TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

VERİ MERKEZİ REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Mart 2019

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Mart 2018	İlk sürüm	TÜBİTAK BİLGEM YTE
Sürüm 2	Mart 2019	Revizyon	TÜBİTAK BİLGEM YTE

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

YÖNETİCİ ÖZETİ

Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan, kurumsal dijital kabiliyetlerini bütüncül bir yapı üzerinden değerlendirmeyi sağlayan **Dijital Olgunluk Değerlendirme Modeli**'nin geliştirilmesi ve bu **Model** ile uyumlu **Rehberlerin** hazırlanması ile dijital kurumsal kapasitenin artırılmasına ihtiyaç bulunmaktadır. Bu ihtiyaç doğrultusunda TÜBİTAK-BİLGEM-YTE tarafından iç destekli olarak **Dijital Olgunluk Modeli ve Rehberlik** (DİJİTAL-OMR) Projesi 2016 yılında başlatılmıştır. Proje kapsamında d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılması ile dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanacaktır.

Modeli ve **Rehberlerin** hazırlanmasına yönelik ulusal politika hedefleri, ülkemizde geliştirilen ve uygulamaya alınan Bilgi Teknolojileri (BT) rehber ve olgunluk modelleri ile 5 uluslararası kuruluş, 12 danışmanlık firması, 6 ülke tarafından geliştirilen standart, rehber ve çerçeve modelleri, uygulama örnekleri ve ilgili akademik çalışma örnekleri incelenmiştir. Farklı dijital kabiliyet alanlarında 34 bilişim uzmanından tecrübe aktarımı sağlanmıştır. Merkezi Yönetim ile yapılan anket üzerinden ilgili kapsama giren konular özelinde anket sonuçları analiz edilmiştir. Elde edilen tespitler doğrultusunda, **Dijital Olgunluk Değerlendirme Modeli**'nin taslağı oluşturulmuş ve seçilen kamu kurumlarında pilot uygulama yapılmıştır. Pilot uygulama sırasında alınan geri bildirimler doğrultusunda **Model** nihai hale getirilmiştir. **Model** ile Stratejik Yönetim, Organizasyon, Yazılım Hizmetleri, Yazılım Yaşam Döngüsü, BT Hizmetleri, İşletim ve Bakım, d-Hizmetler başlıklarında yedi yetkinlik belirlenmiştir. Bu yetkinlikler altında gruplandırılmış dijital kabiliyetler bazında seviyelendirilmiş 2500 soru belirlenmiştir.

Model'in 7 kamu kurum ve kuruluşuna uygulaması yapılarak Dijital Olgunluk Seviyeleri belirlenmiş ve dijital kabiliyetler bazında tespit değerlendirmeleri gerekçelendirilerek Dijital Olgunluk Seviyesini geliştirmeye yönelik kısa, orta ve uzun vadede çözüm önerileri sunulmuştur.

Dijital Olgunluk Değerlendirme Modeli kapsamında yer alan yetkinlikler ve söz konusu yetkinlikler kapsamında yer alan dijital kabiliyetler dikkate alınarak yol gösterici olarak kullanılmak üzere **Rehberler** hazırlanmaktadır. Kurumsal kaynakların büyük bir kısmının işletim ve bakım proje ve faaliyetlerine ayrılmış olduğu tespitinden hareketle, ilk olarak **İşletim ve Bakım Rehberi** hazırlanmış ve 2017 yılında yayımlanmıştır. **Rehber**'de, işletim

ve bakım yetkinliği altında toplanan kabiliyetler bazında tespit edilen seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna yönelik referans, rol, işleyiş, iş akışı ve çıktılar ile ilgili bilgiler sunulmaktadır. Aynı yıl **Model** ile belirlenen tüm dijital kabiliyetler için, yatırım planlanırken dikkate alınması gereken unsurlar ve alternatifleri ile ilgili bilgi ve yönlendirmeleri içeren 32 adet **Dijital Kabiliyet Rehberi** hazırlanmıştır. Söz konusu rehberlerin yetkinlikler altında ve tüm yaşam döngüsü dikkate alınarak genişletilmesine yönelik rehber hazırlama çalışmaları devam etmekte olup bu kapsamda 2018 yılında **BT Hizmetleri** yetkinliği altında yer alan **Veri Merkezi Rehberi**, 2019 yılında aynı yetkinlik altında **Kablosuz Ağların Kullanımı Rehberi** yayımlanmıştır. **Kablosuz Ağların İşletimi Rehberi** hazırlıkları devam etmektedir. 2019 yılı içerisinde bunlara ek olarak **Aktif Dizin Rehberi, Sunucu Rehberi** ve **İstemci Rehberi**'nin hazırlanması planlanmaktadır.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** **www.dijitaldonusum.gov.tr** platformu ile açık erişimi sağlanmakta ve **Rehberlerin** kullanımının yaygınlaşması amacıyla eğitim programları, toplantılar ve çalıştaylar düzenlenmesi ile **Rehberlik Mekanizmaları** hayata geçirilmektedir. Bu sayede d-Devlet ekosisteminde görev alan bilişim uzmanlarının yetkinliklerinin artırılması hedeflenmektedir. Yanı sıra **Dijital Olgunluk Değerlendirme Modeli** ile uyumlu olarak 2017 yılında Türkiye'ye özgü **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiş ve **Model** ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönlerinin belirlenmesi ve eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmıştır. 28 bilişim profesyonel rolü ile bu rollerdeki çalışanların sahip olması hedeflenen 41 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 5 kurumda yaklaşık 1000 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

2019 Yılı Yıllık Programı'nda belirlenen kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilmesinin ihtiyacının karşılanmasında Dijital Devlet ekosistemine katkı sağlayacağını öngördüğümüz Türkiye'ye özgü geliştirilen ilk **Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri** ile **Dijital Kabiliyet Rehberleri'nin** içeriği ile ilgili **epid.yte@tubitak.gov.tr** ve **www.dijitaldonusum.gov.tr** adresleri aracılığıyla ileteceğiniz değerlendirmelerinizle ilgili çalışmaların tüm ekosistemin bilgi ve tecrübesiyle iyileştirilmesini temenni ederiz.

1 GİRİŞ

Veri Merkezi Rehberi 5 bölümden oluşmaktadır:

1. Bölüm'de, dokümanın kapsamı, kullanılan terimler ve yararlanılan kaynaklar,
2. Bölüm'de, Proje'nin amacı ve kapsamı,
3. Bölüm'de Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri ile ilgili bilgiler,
4. Bölüm'de, Veri Merkezi Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Veri Merkezi Rehberi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
Alt Yüklenici	Tedarikçiler tarafından sunulan hizmetlerde bir sözleşme ile katkıda bulunan organizasyondur.
Arıza / Kesinti	Planlı olmayan BT hizmet kesintileri veya hizmet kalitesinin beklenen seviyenin altına düşmesidir.
Anti-Passback	Giriş kontrol sistemlerinde giriş yapmadan çıkış yapamama/çıkış yapmadan giriş yapamama yada aynı geçiş noktasından kartın tekrarlı okutulmama kontrolüdür.
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
Bilgi Güvenliği	Bilginin kullanılabilirlik, bütünlük ve gizlilik niteliklerinin korunmasıdır.
Bilgi Güvenliği İhlal Olayı	Yüksek bir olasılıkla iş fonksiyonlarını kesintiye uğratabilecek bilgi güvenliğini tehdit eden, istenmeyen ya da beklenmeyen bilgi güvenliği olaylarıdır.
Bilinen Hata	Kök nedeni belirlenmiş veya geçici bir çözümü bulunan problemlerdir.
Biyometrik	Kimlik saptamak için bireyin ölçülebilir fiziksel ve/veya davranışsal özellikleridir.
BT	Bilgi Teknolojileri

Terim / Kısaltma	Tanım
By-Pass	Atlamak, pas geçmek.
Çağrı	Kullanıcılardan gelebilecek her türlü bildirim (arıza/kesinti, talep/istek) bu kabiliyet kapsamında çağrı olarak kullanılmaktadır.
d-Devlet	Dijital Devlet
Dual Bus	Çift Veriyolu
Değişiklik Talebi	Hizmet, hizmet bileşeni ya da hizmet yönetim sistemi kapsamlı yapılacak değişiklik önerileridir.
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur. Genel olarak yüzde olarak ifade edilir.
Etkililik	Faaliyetlerin gerçekleşen sonuçlarının planlanan sonuçları oluşturabilme seviyesidir.
Franklin Çubuğu	Yıldırım yakalama çubuğu
Hizmet	Kullanıcı ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (Örnek: Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
Hizmet Bileşeni	Bir hizmetin tam olarak sunulabilmesi bir araya getirilen hizmet birimleridir. Donanım, yazılım, araç, uygulama, doküman, bilgi, süreç ve destek hizmetler örnek olarak verilebilir. Bir hizmet bileşeni bir ya da birden fazla konfigürasyon öğesi içerebilir.
Hizmet Gereksinimi	Hizmet edinen ve hizmet kullanıcılarının ihtiyaçlarıdır.

Terim / Kısaltma	Tanım
Hizmet Kataloğu	Hizmet kataloğu, tüm canlı ve canlıya alınması planlanan BT hizmetlerine ilişkin bilgileri içeren bir doküman / veritabanı / listedir.
Hizmet Sürekliliği	Bir hizmet ya da hizmetlerin üzerinde mutabık kalınmış hizmet seviyelerinde sürekli olarak verilmesine yönelik ciddi etkileri olan olay ve risklerin yönetilmesidir.
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanma durumudur.
Kapasite Planı	Gelecek dönem ihtiyaçları doğrultusunda, alternatif iş senaryolarının göz önünde bulundurularak, gerekli kaynak gereksinimlerinin tespit edildiği ve bu gereksinimlerin karşılanması için gerçekleştirilecek faaliyetlerin yer aldığı plandır.
Konfigürasyon Dayanağı	Hizmet ya da hizmet bileşeninin yaşam döngüsü içerisinde önceden belirlenmiş durumların oluştuğu anlarda kayıt altına alınan konfigürasyon bilgisidir. Onaylanmış değişiklik kayıtları ile mevcut konfigürasyon, konfigürasyon dayanağını oluşturur.
Konfigürasyon Öğesi	Yaşam döngüsü boyunca izlenebilir ve yönetilebilir kılmak amacı ile kontrol altında tutulan varlıklardır.
Konfigürasyon Yönetimi Veri tabanı	Konfigürasyon yönetimi faaliyetlerini yönetebilmek amacı ile BT hizmetleri, bu hizmetleri oluşturan konfigürasyon öğeleri, konfigürasyon öğelerinin temel özellikleri ve diğer konfigürasyon öğeleri ile olan ilişkileri hakkında bilgilerin yönetildiği veri saklama alanıdır.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.
Kuru Kontak	Kaynak üzerinden gerilim gelmeden çalışan kontak

Terim / Kısaltma	Tanım
Modbus	Endüstriyel ürünler için geliştirilmiş bir haberleşme yöntemi
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.
Olgunluk Değerlendirme Modeli	Başlangıç durumundan, önceden tanımlanmış yetkinlik alanlarındaki olgunluk durumuna kadar, öngörülen, arzu edilen ya da tercih edilen yol doğrultusunda, sıralı düzeyler ya da aşamalar içeren modeldir. İlgili alanda referans modele göre mevcut durumun değerlendirilmesi ve referans modele göre iyileştirme alanlarının belirlenmesi için kullanılır.
Önleyici Faaliyet	Olası bir uygunsuzluk ya da istenmeyen durumdan kaçınmak ya da oluşma ihtimalini azaltmak için duruma sebep verdiği belirlenen kök nedenlerin ortadan kaldırılmasına yönelik faaliyetlerdir.
Problem	Bir veya birden fazla arızaya/kesintiye ilişkin kök neden olarak tanımlanan durumdur.
Risk	Olası bir olayın sonuçlarının iş hedefleri üzerinde belirsizlik oluşturma etkisi ve ilişkin olasılığıdır.
Selenoid Valf	Gaz, hava, su, buhar ve yağ gibi akışkanların geçişini kontrol altında tutan elektromekanik vanalardır.
STK	Sivil Toplum Kuruluşu
Sürüm	Bir hizmet üzerinde gerçekleştirilmek üzere birlikte hazırlanacak, test edilecek ve devreye alınacak değişiklikler topluluğudur.
Tedarikçi	Hizmet sağlayan organizasyonun dışında hizmet sağlayan ile bir sözleşme ile muhatap olan hizmet tasarım, sunum ve iyileştirme faaliyetlerinde katkıda bulunan organizasyondur. Tedarikçilerin alt yüklenicileri tedarikçi olarak ele alınmaz.
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

Terim / Kısaltma	Tanım
UPS	Uninterruptible Power Supply – Kesintisiz Güç Kaynağı
Uygunsuzluk	Bir gereksinimin karşılanamaması durumudur.
VFI	Voltage and Frequency Independent – Voltaj ve Frekans Bağımsız
Yangın Bariyeri	Yangın sırasında cephelerde pencere ve kapı boşluklarından yükselen alev ve dumanın, katlar arası yayılımını engelleyen yangın durdurucu sistemlerdir.
Yangın Dayanımı	Bir yapı bileşeninin ya da elemanının; yük taşıma, bütünlük ve yalıtkanlık gibi özelliklerini bir süre boyunca yangına karşı korumasına denir.
Yangın Yükü	Bir binadaki veya sınırlı bir alanda yanıcı madde miktarını ve bunun üretebileceği ısı miktarına denir.
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1.2 REFERANSLAR

Ref 1. TIA (2015) 942-A: Veri Merkezleri İçin Telekomunikasyon Altyapı Standartı

Ref 2. ANSI/BICSI 002 (2014): Veri Merkezi Tasarım ve Uygulama En İyi Pratikleri

Ref 3. Rob Snevely (2012): Enterprise Data Center Design and Methodology

Ref 4. NSA (2018), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri

Ref 5. IT Grundschutz 1.Yayım (2018): Bilgi Teknolojileri Güvenliği Enstitüsü (BSI), Almanya.

Ref 6. ISO (2011). ISO/IEC 20000-1:Information technology -- Service management -- Part 1: Service management system requirements.

Ref 7. ISO (2012). ISO/I”EC 20000-2: 2012: Information technology - Service management - Part 2: Guidance on the application of service management systems.

Ref 8. ISO (2013). ISO/IEC 27001 - Information security management.

Ref 9. ISO (2013). ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security controls

2 DİJİTAL OLGUNLUK MODELİ VE REHBERLİĞİ PROJESİ

Dijital Olgunluk Modeli ve Rehberlik (DİJİTAL-OMR) Projesi, 2016 yılında TÜBİTAK-BİLGEM-YTE tarafından yürütülen iç destekli bir projedir. Projenin amacı, Dijital Devlet (d-Devlet) alanında gelinen düzeyde ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan kurumsal **Dijital Olgunluk Değerlendirme Modeli'nin** geliştirilmesi ve bu yönde kurumsal kapasitenin artırılması için **Model** ile **Rehberlerin** hazırlanmasıdır.

Bu proje ile 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda doğrudan rehberlik mekanizmalarına yönelik tanımlanan aşağıdaki eylemlere de katkı sağlanacaktır:

- "*E1.1.4-e-Devlet Ekosistemi Rehberlerinin Hazırlanması ve Güncellenmesi*" eylemi, e-Devlet ekosisteminin etkin bir şekilde çalışabilmesi ve sürdürülebilirliği için birlikte çalışabilirlik, kamu kurum / kuruluşlarının internet siteleri ve mobil uygulamaları ile kamu kurum / kuruluşlarının resmi sosyal medya hesaplarının kullanımı ve yönetimine dair rehberler başta olmak üzere mevcut rehberlerin güncellenmesi ve ihtiyaç duyulan yeni rehberlerin hazırlanmasına yönelik bir eylemdir.
- *"E1.1.6-Ulusal e-Devlet Olgunluk Seviyesi Ölçümleme Mekanizmasının Oluşturulması"* eylemi, yaşamsal olaylar bütünlüğünde kamu hizmetlerinin e-Devlet olgunluk düzeyi, Kurum seviyesinde e-Devlet olgunluk düzeyi ve Ulusal e-Devlet olgunluk düzeyi kapsamında e-Devlet olgunluk ve olgunluk ölçümleme modellerinin tanımlanması, tanımlanan bu modeller kullanılarak ulusal düzeyde e-Devlet olgunluk düzeyi ölçümleme çalışmaları ile birlikte, seçilen e-Devlet hizmetleri ve kamu kurumları için e-Devlet olgunluk düzeyi ölçümleme çalışmalarının yürütülmesine yönelik bir eylemdir.

Proje kapsamında yapılacak faaliyetler, kurumsal düzeydeki dijital dönüşümü ve 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'ndaki eylemler ile hayata geçirilmesi öngörülen ulusal düzeydeki olgunluk değerlendirme modelini destekleyecektir. Bir başka ifadeyle, Proje kapsamında üretilecek **Model** ve **Rehber** ile kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek adına kurumsal düzeyden başlayan ve ulusal düzeye çıkan ölçümleme çalışmalarına katkı sağlanacaktır. Dolayısıyla mikro seviyede kurum düzeyindeki kurumsal etkinliği artırma odağı ile şekillendirilen proje çıktıları, makro seviyede ulusal olgunluk düzeyine çekilebilecek bir alt yapı oluşturacaktır. Bu alt yapı sayesinde 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda yer alan eylemlerin uygulanabilirliği artırılacaktır.

Dijital Olgunluk Değerlendirme Modeli ile;

- Kamu kurumlarının bilişim proje ve faaliyetlerine sistemli ve bütüncül bakış açısının geliştirilmesi desteklenecektir.
- Kamu kurumları ve sundukları hizmetlerin dijital olgunlukları hakkında bir değerlendirme yapabilmek ve seviye tespit edebilmek mümkün olacaktır.
- Kurumların içinde bulunduğu dijitalleşme sürecinde değişimlere ve yeniliklere uyumu desteklenecektir.

Model kapsamında hazırlanacak **Rehberler** ve **Rehberlik** mekanizması ile;

- Bilişim projeleri ve faaliyetlerinin daha verimli, etkin ve güvenli planlanması, yürütülmesi ve tamamlanması sağlanarak başarı oranının artırılmasına katkı sağlanacaktır.
- Bilişim proje ve faaliyetlerinin verimliliği artırılarak ilgili hizmetlerin kalite ve performansı iyileştirilecektir.
- Bilişim uzmanlarının dijital kabiliyetleri artırılacaktır.
- TÜBİTAK tarafından yürütülen Kamu BT projeleri ile edinilen bilgi ve tecrübenin, özel sektör ve STK ile açık paylaşımı sağlanacak ve ilgili paydaşlar ile karşılıklı bilgi ve tecrübe alışverişi gerçekleştirilecektir.

3 DİJİTAL OLGUNLUK VE YETKİNLİK DEĞERLENDİRME MODELLERİ

Dijital Olgunluk Değerlendirme Modeli, bir organizasyonun önceden tanımlanmış yetkinlik alanlarındaki yetkinlik durumundan hedeflenen ya da gerekli görülen seviyeye kadar, dijital dönüşüm ve/veya dijital hizmet kabiliyetlerindeki seviyelerin değerlendirilmesini ve iyileştirilmesini sağlayan kademeli referans modeldir.

Dijital teknolojilerin yenilikçi fırsatlarıyla iş süreçlerine uyarlanması ve dijital teknolojiler doğrultusunda yeni katma değerli hizmet ve süreçler oluşturulması kurumsal düzeyde dijital dönüşümün en öncelikli amacı olmaktadır. Dünyada özellikle son 10 yıldır dijitalleşmenin ve ülkelerin farklılaşan koşullarına göre geliştirilen birçok dijital olgunluk değerlendirme modeli olmasına karşın, Türkiye'de kamu kurumlarında "e-Kurum" "e-Devlet" ve "dijital" gibi kavramların hiçbirine yönelik olgunluk referans modelinin olmadığı görülmüştür.

Günümüz koşulları değerlendirildiğinde "dijital" kavramı doğrultusunda hazırlanacak ve kurumların dijital dönüşümlerini analiz edip referanslar doğrultusunda yönlendirecek bir modelin ve model uygulama yaşam döngüsünün olması önemli bir ihtiyaçtır. Ancak bilişim ya da bilgi güvenliği standart ve rehberlerine benzer şekilde uluslararası kabul gören bir kurumsal dönüşüm standardı mevcut değildir.

Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır. Ancak ortak alanlar olmakla birlikte kamu kurumlarının ihtiyaçları özel sektör ihtiyaçlarından ayrışmaktadır. Üstelik kamu yönetim anlayışı ve birikimi göz önüne alındığında, ülkemiz diğer ülkeler ile de ayrışmaktadır. Teknoloji odaklı dönüşüm çabası içerisinde olan tüm organizasyonlar için ortak gereksinimler söz konusu iken mevcut koşulları doğrultusunda her organizasyon tipinin kendi içerisinde özelleşmiş ihtiyaçları da olabilmektedir. Bu doğrultuda, kamu kurumlarında dijital dönüşüme yön verilmesi ve uygulamanın başarı ile hayata geçirilebilmesi için öncelikli olarak, kamu kurumlarına yönelik **Dijital Olgunluk Değerlendirme Modeli** oluşturulmuş ve **Modelin** ülke koşullarına uygun yapıya sahip olması sağlanmıştır. Oluşturulan **Model**, aynı zamanda ülkenin mevcut dijital dönüşüm politikalarıyla uyumludur ve uluslararası tecrübeleri dikkate almaktadır.

Model ile bir organizasyonun dijital kabiliyetlerini değerlendirerek, tespit edilen mevcut kabiliyet seviyelerinin iyileşmesi için yol haritası sağlanmaktadır. Böylece, kurumların dijital

dönüşümlerinin yapısal, standart, tutarlı, etkin ve verimli bir şekilde yapılmasına katkı sağlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli gereksinim ağacı 3 basamak olarak oluşturulmuştur:

- Yetkinlik
- Kabiliyet Grubu
- Kabiliyet
    - Alt Kabiliyet

Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

Dijital Olgunluk Değerlendirme Modeli 7 yetkinlik altında tanımlanmış 38 kabiliyet grubu ve bu kabiliyet grupları altında gruplandırılmış çeşitli kabiliyetlerden oluşmaktadır:

- **Yetkinlik**, kendi aralarında ilişki söz konusu olan kabiliyet gruplarından oluşmaktadır. Her bir yetkinlik kendi içerisinde bir bütündür ve organizasyonlarda dijital dönüşüm için müstakil olarak ele alınabilir. Belirlenecek tespitler ve değerlendirmeler doğrultusunda organizasyonun her bir yetkinlik için yetkinlik seviyesi ortaya konmaktadır.
- Birbirlerine yakın olan kabiliyetler **kabiliyet grupları** altında toplanmıştır. Her bir yetkinlik altında tanımlanmış kabiliyet grupları arasında ilişki mevcuttur. Bu ilişki genel olarak bir döngü ya da pratikler üzerinden tarif edilmektedir.

- **Kabiliyetler**, organizasyonun iş ve işlemlerini gerçekleştirebilmek için gerek duyduğu/duyacağı en küçük bileşenlerdir. Kabiliyetler uluslararası normlara ve ulusal gereksinimlere uygun olarak belirlenmiştir.
- **Alt Kabiliyetler,** kabiliyetlerin; amaç, hedef kitle ve operasyonel sorumluluk alanlarına göre özelleşmiş alt bileşenleridir.
- **Seviye**, kurumun varlıklarının, uygulamalarının ve süreçlerinin gerekli çıktıları güvenilir ve sürdürülebilir bir şekilde üreterek olgun bir yapıya ulaşması amacıyla yapılandırılmış düzeylerdir.

Dijital dönüşümü hedefleyen kurumların ihtiyaç duyacağı yetkinlik alanları **Dijital Olgunluk Değerlendirme Modeli** kapsamında aşağıdaki gibi tanımlanmıştır:

Şekil 2. Dijital Olgunluk Değerlendirme Modeli - Genel Görünüm

1. Yetkinlik: STRATEJİK YÖNETİM

Dijital dönüşüm ve dijital hizmet yönetimi kapsamında orta ve uzun vadeli amaçları, temel ilke ve politikaları, hedef ve öncelikleri ve bunlara ulaşmak için izlenecek yol ve yöntemleri içeren strateji belgelerinin; kapsamına ilişkin faaliyetleri amaç, yöntem ve içerik olarak düzenleyen ve gerçekleştirme esaslarının bütününü içeren politika belgelerinin hazırlanmasını, izlenmesini ve güncellenmesini kapsar. Bu strateji ve politikalar doğrultusunda, kurumsal mimari yapısının kurulması, ihtiyaçların tanımlanması, çözümlerin planlanması ve bütçenin yönetilmesi amaçlanmaktadır. Bu yetkinlik, dijital

strateji yönetimi, politika, kurumsal mimari, ihtiyaç tanımlama ve çözüm planlama ve bütçe kabiliyet gruplarını içermektedir.

2. Yetkinlik: ORGANİZASYON

Dijital dönüşüm çalışmalarının (portföy, program vb.) yönetişim mekanizmasından sorumlusu ekip / kişilerin mevcudiyeti, yönetişim mekanizmasının işlerliği, rol, yetenek ve yetkinliklerinin yönetilmesini kapsar. Bu yetkinlik, organizasyon, dijital kültür ve yetkinlik kabiliyet gruplarını içermektedir.

3. Yetkinlik: YAZILIM HİZMETLERİ

Kurum ihtiyaçlarına göre bir yazılımın yaşam döngüsü için yapılan yazılım fizibilitesi, geliştirilmesi, bakımı ve modernizasyonu, hazır paket yazılımların tedariki ile veri üretimi ve sayısallaştırma hizmetlerini kapsar. Bu yetkinlik, yazılım fizibilite, yazılım geliştirme, yazılım modernizasyonu, yazılım tedarik, yazılım bakımı, veri üretimi ve sayısallaştırma kabiliyet gruplarını içermektedir.

4. Yetkinlik: YAZILIM YAŞAM DÖNGÜSÜ

Yazılım projesinin planlamasından başlayarak teslimatına kadar geçirmiş olduğu bütün aşamaları ve bu aşamalardan oluşan döngüyü kapsar. Bu yetkinlik, proje yönetimi, gereksinim mühendisliği, teknik çözüm, doğrulama ve geçerleme, konfigürasyon ve kalite güvence kabiliyet gruplarını içermektedir.

5. Yetkinlik: BT HİZMETLERİ

Kurumun sahip olduğu teknolojiler ile mevcut donanım ve altyapıların yönetilmesini kapsar. Bu yetkinlik, teknoloji sahipliği, donanım/BT altyapı fizibilitesi, donanım/BT altyapı tedariği, yapım işi, hizmet alımı ve BT Altyapısı Bakımı / Modernizasyonu kabiliyet gruplarını içermektedir.

6. Yetkinlik: İŞLETİM VE BAKIM

Kurumsal BT hizmetlerinin planlanması ve yönetişimi, yeni planlanan / değişen BT hizmetlerinin devreye alınması ve kontrolü, BT hizmetlerinin yönetimi, sunulması ve desteği ile BT Hizmet kalitesinin sürekli iyileştirilmesi için gerekli kabiliyetleri kapsar. Bu yetkinlik, planlama ve yönetişim, geçiş ve kontrol, sunum ile izleme ve değerlendirme kabiliyet gruplarını içerir.

7. Yetkinlik: D-HİZMETLER

Kurumun sahip olduğu idari uygulamaların yönetimini, kurum dijital tanıtım kanalları (internet sitesi, sosyal medya hesapları vb.) ve dijital olarak sunulan kamu hizmetlerin tasarımını ve iyileştirilmesini içeren tüm adımları kapsar. Bu yetkinlik, kurumsal uygulamaların kullanımı, kurumsal bilgi yönetimi, d-hizmet yönetişimi, d-hizmet tasarımı, d-hizmet sunumu, d-hizmet iyileştirme, d-hizmet inovasyonu kabiliyet gruplarını içerir.

Kabiliyet grubu altındaki hangi kabiliyetlerin organizasyon için gerekli olduğu ve mevcut durumu dijital olgunluk değerlendirmesi kapsamında belirlenebilmektedir. Bu sayede, bazı kabiliyetler ya da kabiliyet grupları değerlendirme dışında bırakılabilmektedir. Benzer şekilde, kurumsal faaliyetlerin çeşitliliğine göre bazı kabiliyet ya da kabiliyet grupları diğerlerinden daha öncelikli olabilmektedir. Nihai kurumsal dijital olgunluk değerlendirmesi, kurumun faaliyet alanı, iş ve işlemlerini dikkate alarak kuruma uygun olarak özelleştirilebilmektedir. Bu sayede, dijital dönüşüm çalışmaları özelleşmiş ihtiyaçlara göre yönlendirilebilmektedir.

Kurumsal Dijital Olgunluk Seviyesi 4 ana gruba ayrılmıştır:

- Seviye 0 (Eksik): kabiliyet yoktur.
- Seviye 1 (Uygulanan): kabiliyetin temel pratikleri uygulanmaktadır.
- Seviye 2 (Kurumsallaşmış): kabiliyetler tanımlı, olup pratikleri, standart ve tutarlı bir şekilde uygulanmaktadır.
- Seviye 3 (Optimize Edilen): kabiliyet seviyeleri ölçülmekte olup, gerçek ve potansiyel problemlerin kaynağı analiz edilerek sürekli iyileşen kabiliyetler vardır.

Her kabiliyet seviyesinin altında tanımlanan sorular, doküman inceleme, ilgili personelle görüşmeler, yerinde gözlemleme, katılımcı gözlemi, fiziksel bulgular gibi çeşitli veri toplama yöntemleri kullanılarak yanıtlanmaktadır. Elde edilen yanıtların konu uzmanlarının değerlendirmeleri ile kabiliyetin seviyesi tespit edilmektedir.

Dijital Olgunluk değerlendirmesi kapsamında kurumun büyüklüğüne göre değişen ortalama 16 haftalık bir süreçte, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarıyla **Dijital Olgunluk Öz Değerlendirme Anketi** yolu ile bilgi toplanmakta, kurum uzmanları ile 3-4 tam gün değerlendirme mülakatları yapılmakta, bilgi, belge ve dokümanlar incelenmekte ve değerlendirme sonrası kurumun mevcut **Dijital Olgunluk Seviyesi** belirlenmektedir. Dijital Olgunluk Seviyesinin bir üst seviyeye çıkması amacı ile değerlendirme sonucu elde edilen tespitler gerçekleşme etkisi ve gerçekleşme süresi

üzerinden sınıflandırılarak kısa, orta ve uzun vadeli öneriler ilgili uzman görüşleri dijital kabiliyet rehberleri ile desteklenecek şekilde raporlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli ile;

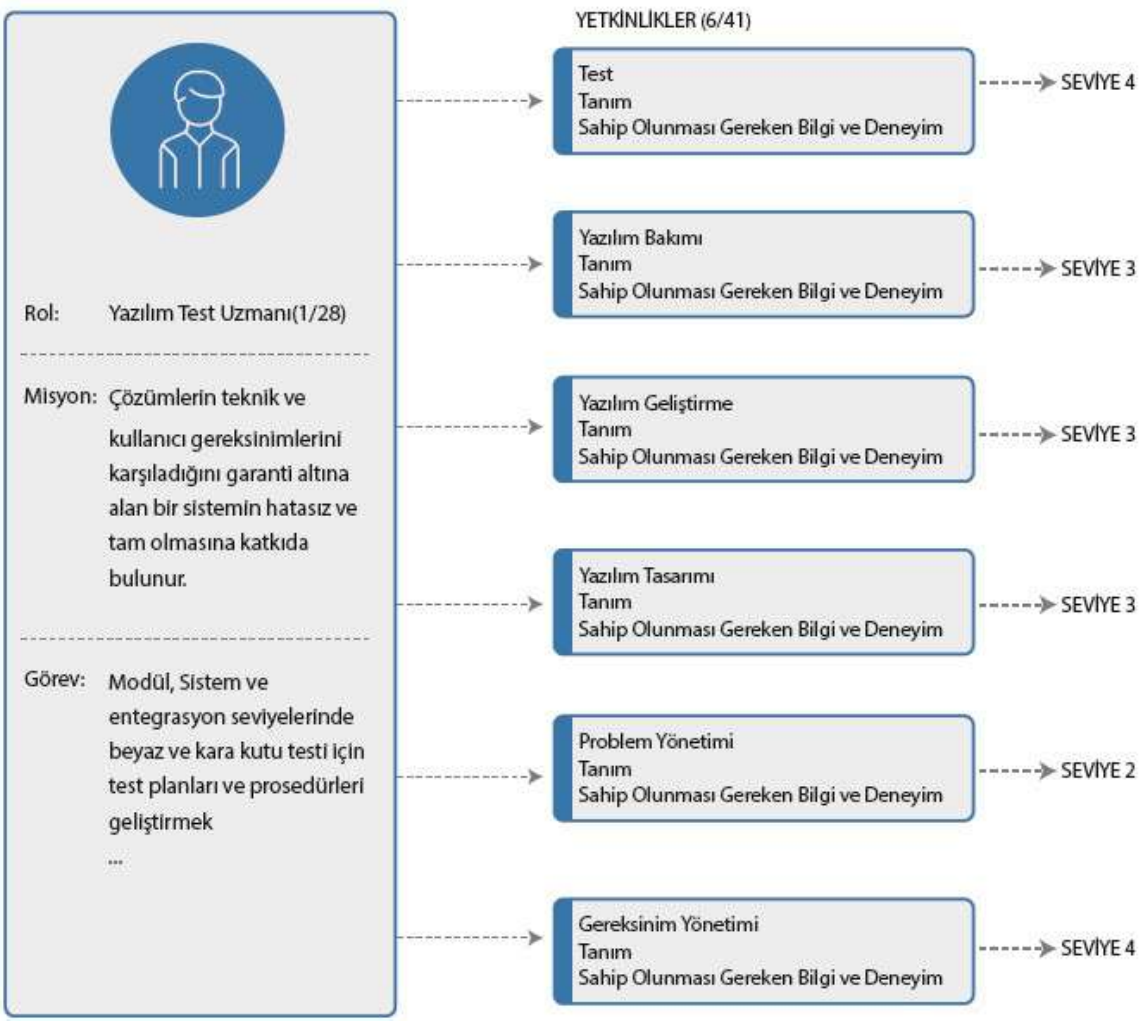
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının belirlenmesi,
- Dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi, çalışan ve vatandaş memnuniyetinin arttırılması

sağlanmaktadır.

Kurum dijital olgunluğunun yetkin insan kaynağı ile iyileştirilmesine yönelik **Dijital Olgunluk Değerlendirme Modeli'nde** yer alan kabiliyetler baz alınarak TÜBİTAK-BİLGEM-YTE tarafından **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Model ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönleri belirlenmekte, eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmaktadır. "SFIA - Skills Framework for the Information Age" ve "European e-Competence Framework" modelleri analiz edilerek Türkiye'ye özgü ihtiyaçlar dikkate alınarak **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Dijital Yetkinlik Değerlendirme Modeli'nde;

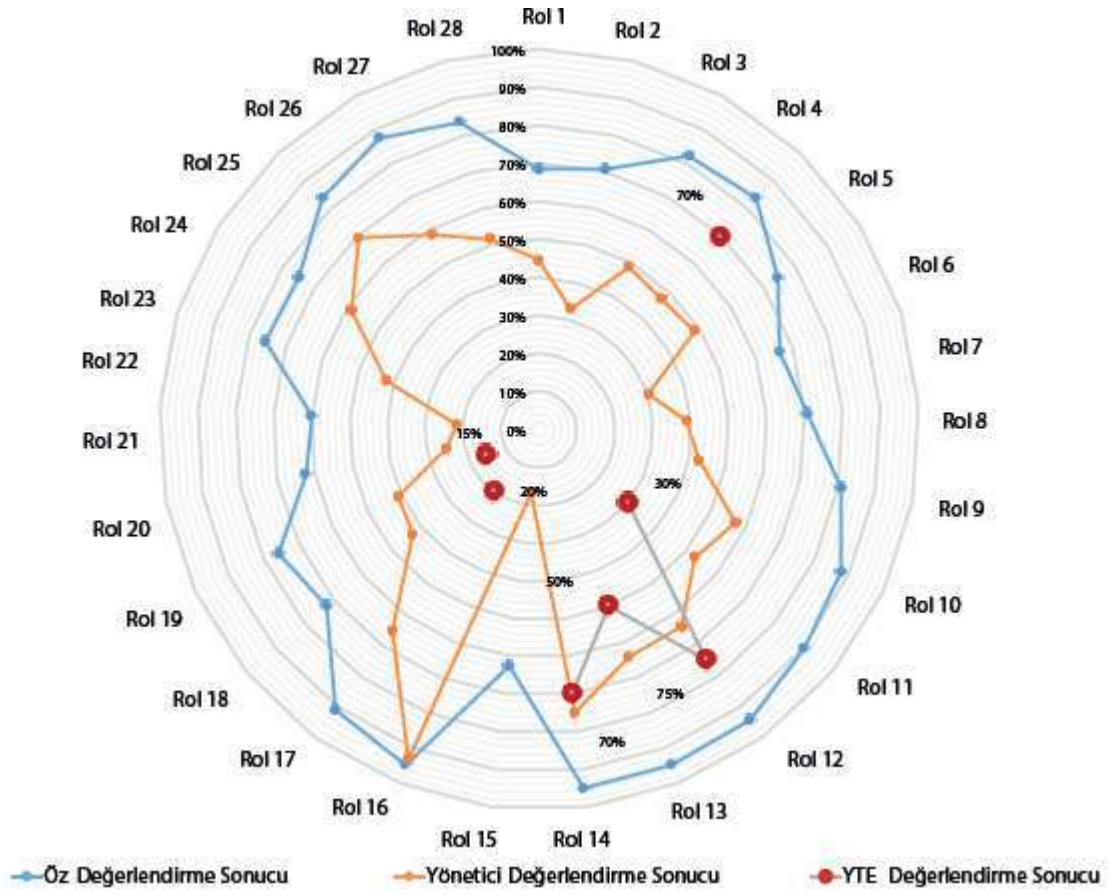
- Bilişim Üst Yönetimi,
- Proje Yönetimi,
- Ağ ve Sistem Yönetimi,
- Bilgi Güvenliği Yönetimi,
- Yazılım Teknolojileri Yönetimi,
- Bütçe ve Tedarik Yönetimi

alanlarında Türkiye'deki organizasyon yapılarına özgü 28 bilişim profesyonel rolü tanımlanmıştır: Ayrıca, bu rollerdeki çalışanların sahip olması hedeflenen 41 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller; yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. Bunun için bir örnek aşağıdaki gibidir:



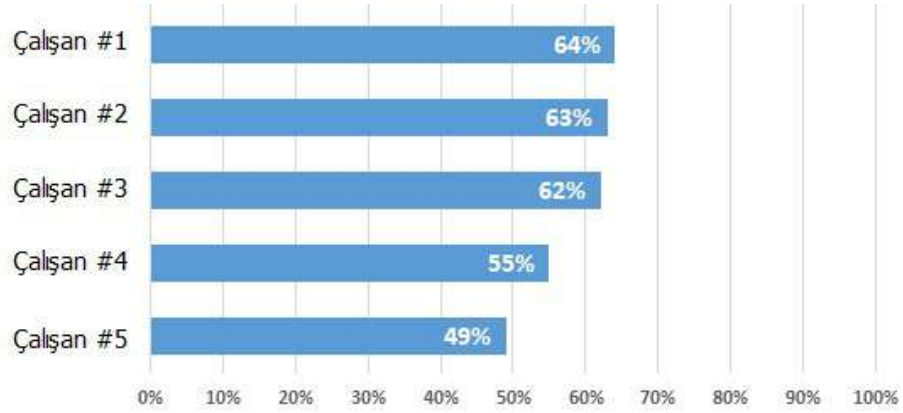
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

Dijital yetkinlik değerlendirmesi kapsamında kurumdaki bilişim uzmanı sayısına bağlı olarak değişen bir sürede, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarının **Dijital Yetkinlik Öz Değerlendirme Anketi** yolu ile kendilerini değerlendirmesinin yanında, çalışanın bağlı olduğu bir üst yöneticisi tarafından **Yönetici Çalışan Değerlendirme Anketi** yoluyla yöneticisinin çalışanı değerlendirmesi sağlanmaktadır. Çalışan sayısına bağlı olarak değişen sürede çalışanlar ile değerlendirme mülakatları gerçekleştirilmektedir. Çalışan öz değerlendirme ve yönetici değerlendirmesi ile YTE değerlendirme sonucu üzerinden 28 rol bazında uygunluğu raporlanmaktadır:



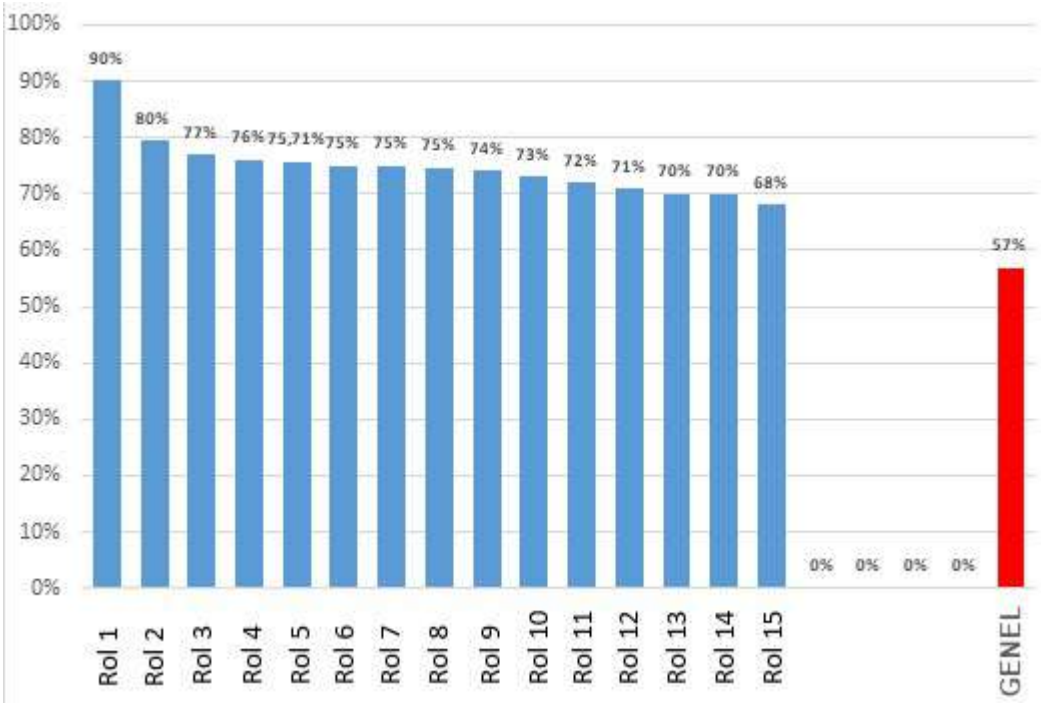
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

Rol bazlı çalışan karşılaştırması yapılarak insan kaynağı kapasitesi değerlendirilmektedir:



Şekil 5. Rol Bazında Dijital Yetkinlik Değerlendirmesi

Bunun yanı sıra kurumdaki roller bazında değerlendirme raporlanmaktadır ve **Kurum Dijital Yetkinlik Haritası** çıkarılmaktadır:



Şekil 6. Kurum Dijital Yetkinlik Haritası

Kurumun büyüklüğü ve bağlı olduğu sektöre göre benzer kategoriye giren dünyadaki en iyi örnekler ile bilişim istihdam dağılımının karşılaştırması yapılarak kurumun istihdam planına rehberlik sağlanmaktadır.

Dijital Yetkinlik Değerlendirme Modeli ile;

- Yetkin bilişim insan kaynağı kapasitesinin arttırılması,
- Bilişim insan kaynağı yetkinliğinin ve kapasitesinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Bilişim uzmanlarının kariyer planı için gerekli yetkinlikleri ve gereken yetkinlik seviyelerini içeren yol haritasının belirlenmesi,
- Bilişim insan kaynağının etkin bir şekilde yönetilmesi

sağlanmaktadır.

4 BT HİZMETLERİ YETKİNLİĞİ

BT Hizmetleri Rehberleri, BT sistemleri için standartlaştırılmış koruma gereksinimlerini ve bu gereksinimleri karşılamak için gerekli uygulama faaliyetlerini açıklar. Bu rehberlerin amacı, kamu kurumlarına BT hizmetleri alanında yol göstermek; "Ağ ve İletişim", "Veri Merkezi", "BT Sistemleri" ve "Uygulamalar" kabiliyetleri bazında tespit edilen seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna ve bu olgunluğu geliştirmeye yönelik bilgiler sunmaktır. Böylece, bu kabiliyet için öncelikli yapılması veya kontrol edilmesi gereken noktalar ve bundan sonra uygulanması gereken faaliyetler sıralı bir şekilde verilmektedir. Bu sayede, bir yol haritası da sunulmaktadır. Bu anlamda bu rehber, kurumun olgunluk seviyesini artırmaya yönelik sürekli kullanılabilecek bir rehber olma özelliği taşımaktadır.

Her konu, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) oluşur.

Bu rehberler, korunma gereksinimlerini basit ve ekonomik bir şekilde oluşturmayı mümkün kılmaktadır. Geleneksel risk analizi yöntemi ilk olarak tehditleri tanımlar ve bunların meydana gelme olasılıkları ile değerlendirir, ardından uygun güvenlik önlemlerini seçer ve sonra kalan riski değerlendirir. Bu adımlar, BT hizmetlerinin her temel bileşen rehberi içerisinde zaten yapılmıştır. Rehberler içerisindeki standartlaştırılmış güvenlik gereksinimleri, BT çalışanları tarafından kendi kurumsal koşullarına uyan koruma önlemlerine kolay bir şekilde dönüştürülebilir. Rehberlerde uygulanan analiz yöntemi, temel bileşenlerde önerilen güvenlik gereksinimleri ile mevcut durumun karşılaştırılmasını mümkün kılmaktadır.

BT hizmetleri rehberlerinde belirtilen gereksinimler, yeterli düzeyde korunma amaçlı uygulanmalıdır. Bu gereksinimler; 1. seviye koruma, 2. seviye koruma ve 3. seviye koruma olarak ayrılmıştır. 1. seviye gereksinimler, sistemlerin korunması için gerekli asgari/temel ihtiyaçları içerir. Başlangıç olarak kullanıcılar, en önemli gereksinimleri öncelikli karşılamak için kendilerini 1. seviye gereksinimlere göre sınırlandırabilirler. Ancak, yeterli korunma yalnız 2. seviye gereksinimlerin uygulanmasıyla sağlanacaktır. 3. seviye korunma gereksinimleri için örnek olarak, uygulamada kendini kanıtlamış ve kurumun daha fazla korunma gereksinimi durumunda, kendini nasıl emniyet altına alabildiğini göstermektedir.

Yüksek gereksinimler, ele alınması gereken 3. seviye güvenlik eksikliklerini gösterir. Yüksek gereksinim hedefleri, bir taraftan sistemlerin en iyi şekilde korunması sağlar, diğer tarafta uygulamada ve bakımda önemli ölçüde maliyetleri artıracaktır. Bundan dolayı yüksek koruma gereksinimleri hedefleniyorsa, maliyet ve etkililik yönleri dikkate alınarak

bireysel bir risk analizi yapılmalıdır. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin uygulanması ve bu yöndeki ihtiyaçların giderilmesi, kurumun veya organizasyonun hedefleri doğrultusunda yeterlidir.

Temel bileşen rehberlerine ek olarak oluşturulan uygulama rehberleri, hedeflenen gereksinimlerin en iyi şekilde nasıl uygulanabileceğine dair ek bilgiler içerir. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin yerine getirilmesi, ISO 27001 sertifikasının alınması sürecine katkı sağlayacaktır.

4.1 YÖNTEM

BT Hizmetleri yetkinliğinde hazırlanan **Veri Merkezi Rehberi** çalışmaları sırasında, uluslararası boyutta hazırlanmış ve bu alanda kabul görmüş çeşitli standartlar ve çerçevelerden faydalanılmıştır.

Faydalanılan kaynaklar şunlardır:

- TIA-942-A [Ref 1]: Veri Merkezleri İçin Telekomunikasyon Altyapı Standartı
- ANSI/BICSI 002-2014 [Ref 2]: Veri Merkezi Tasarım ve Uygulama En İyi Pratikleri
- Enterprise Data Center Design and Methodology [Ref 3], Rob Snevely
- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) [Ref 4], Amerika Birleşik Devletleri
- Bilgi Teknolojileri Güvenliği Enstitüsü (BSI) [Ref 5], Almanya. Uzmanlık alanları:
    - Bilgisayar uygulamaları güvenliği,
    - Kritik bilişim teknolojilerinin altyapı güvenliği,
    - Güvenlik sertifikasyonu ve belgelendirilmesi
- ISO 20000 – 1: ISO 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Standardı [Ref 6], bilgi teknolojileri hizmeti sunan kurumların veya firmaların iç ve dış müşterilerinin beklentilerini karşılayabilmeleri, durumlarını ve performanslarını sürekli iyileştirme ve geliştirmeleri, ilgili operasyonlarını yönetmelerinde ve hizmet vermelerinde hangi yöntemleri nasıl uygulayacakları konularında kılavuzluk eden bir standarttır. Bu standart, hizmet yönetimini “işin gereksinimlerini karşılamak amacıyla hizmetlerin yönetilmesi” şeklinde tanımlamaktadır.
- ISO 20000 – 2 [Ref 7], ISO 20000 – 1’in rehberlik dokümanıdır, gereksinimlerin açılması ve uygulama yöntemleriyle ilgili detaylı bilgileri içermektedir.
- ISO 27001 [Ref 8]: Bilgi Güvenliği Yönetimi Sistemi gereksinimlerini tanımlayan uluslararası denetlenebilir standarttır.
- ISO 27002 [Ref 9]: Bilgi Güvenliği Yönetim Sistemine ait iyi uygulama örneklerini içeren dokümandır.

Özellikle **Rehberde** detaylandırılacak alt kabiliyetlerin belirlenmesi için IT-Grundschutz BSI, ANSI, BICSI, ISO 20000 ve ISO 27001 temel alınmıştır. Türkiye'de Veri Merkezi denilince akla gelecek temel başlıklar modeller örnek alınarak oluşturulup, **Rehberin** temel yapısı kabiliyetler üzerinden belirlenmiştir.

4.2 REHBER YAPISI

Her kabiliyet, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) oluşur.

TEMEL BILEŞEN YAPISI

Temel bileşenler, ilgili konunun prosedürlerini ve açıklamalarını içermekte, risklere ve bileşenin korunmasını sağlamaya yönelik özel gereksinimlere kısa bir genel bakış sunmaktadır. Ayrıca BT bileşenleri, aynı fihrist/dizin yapısında düzenlenmiştir. Temel bileşen yapısı aşağıdaki gibi oluşturulmuştur:

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
  - **1.1 Tanım**: Bileşenin kısa tanımıdır.
  - **1.2 Hedef**: Bu bileşenin uygulanmasıyla ne tür güvenlik kazanımlarının sağlanacağı hedefler verilmektedir.
  - **1.3 Kapsam Dışı**: Bileşende ele alınmayan kapsamın yanı sıra hangi bileşenin konusu olduğu gibi bilgiler yer alır.
- **Bölüm 2 - Risk Kaynakları**
  - Temel bileşene ait özet riskler anlatılmaktadır. Bunlar, sistemlerin kullanımında önlem alınmadığı takdirde ortaya çıkabilecek güvenlik sorunlarının bir resmini çizer. Olası risklerin açıklanması, kullanıcının konu hakkındaki bilinç düzeyini artırır.
- **Bölüm 3 - Gereksinimler**
  - **3.1 1. Seviye Gereksinimler:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir .
  - **3.2 2. Seviye Gereksinimler:** İhtiyaçlar doğrultusunda bu standart gereksinimlerin yerine getirilmesi tavsiye edilir.
  - **3.3 3. Seviye Gereksinimler:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 4 - Detaylı Bilgi için Kaynaklar**
  - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

BT Hizmetleri rehberleri içerdikleri konular itibari ile birbirleri arasındaki ilişkinin kurulması için bir referanslama metodu kullanılmıştır. Bu amaçla her gereksinim maddesi

numaralandırılmıştır. Örneğin, BT Hizmetleri rehberlerinde yer alan VRM.3.G4 kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

Veri merkezi rehberleri için kullanılan kısaltma (Üst Başlık)	Elektrik kablolaması için atanan numara (Alt Başlık)	4.Gereksinim maddesi
VRM	3	G4

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberlerinde ise yalnız "G" harfi yerine "U" harfi kullanılmıştır. Yani, VRM.3.G4 gereksinim maddesinin karşılığı VRM.3.U4 olarak geçmektedir.

Ayrıca madde başlıklarında, köşeli parantez içinde madde konusundan ana sorumlu/önerilen kişiler verilmektedir. Bu şekilde, kurum içerisinde hangi role sahip kişilerin ilgili maddenin uygulamasından sorumlu olduğu açıklanır. Kurumdaki konuyla ilgili uygun kişiler, bu roller yardımıyla tespit edilebilir.

UYGULAMA REHBER YAPISI

BT hizmetlerinin temel bileşenleri için ayrıntılı uygulama talimatları (öneriler ve tecrübe edilmiş pratikler) bu rehberlerde detaylandırılmıştır. Bunlar, gereksinimlerin nasıl uygulanabileceğini ve uygun korunma önlemlerini ayrıntılı olarak açıklar. Korunma konseptleri için bu tür önlemler bir temel olarak kullanılabilir, ancak ilgili kurumun hedef ve koşullarına uyarlanmalıdır.

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
  - **1.1 Tanım:** Bileşenin detaylı tanımıdır.
  - **1.2 Yaşam Döngüsü:** Uygulama rehberleri "Planlama ve Tasarım", "Tedarik", "Uygulama", "Operasyon", "Elden Çıkarma" ve "Acil Durum Hazırlık" gibi aşamalardan oluşan yaşam döngüsüne yönelik önlemlerin genel resmini içerir.
- **Bölüm 2 – Uygulamalar:**
  - **2.1 1.Seviye Uygulamalar:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir.
  - **2.2 2.Seviye Uygulamalar:** İhtiyaçlar doğrultusunda bu standart gereksinimleri yerine getirilmesi tavsiye edilir.

- **2.3 3.Seviye Uygulamalar:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.

- **Bölüm 3 - Detaylı Bilgi için Kaynaklar**
  - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

Uygulama rehberlerinde yer alan gereksinimlere ait hazırlanan kontrol soruları **EK-A**'da verilmektedir.

4.3 KABİLİYET GRUPLARI

BT Hizmetleri yetkinliğinde ele alınan kabiliyet gruplarının açıklaması ve altlarındaki kabiliyetler şu şekildedir:

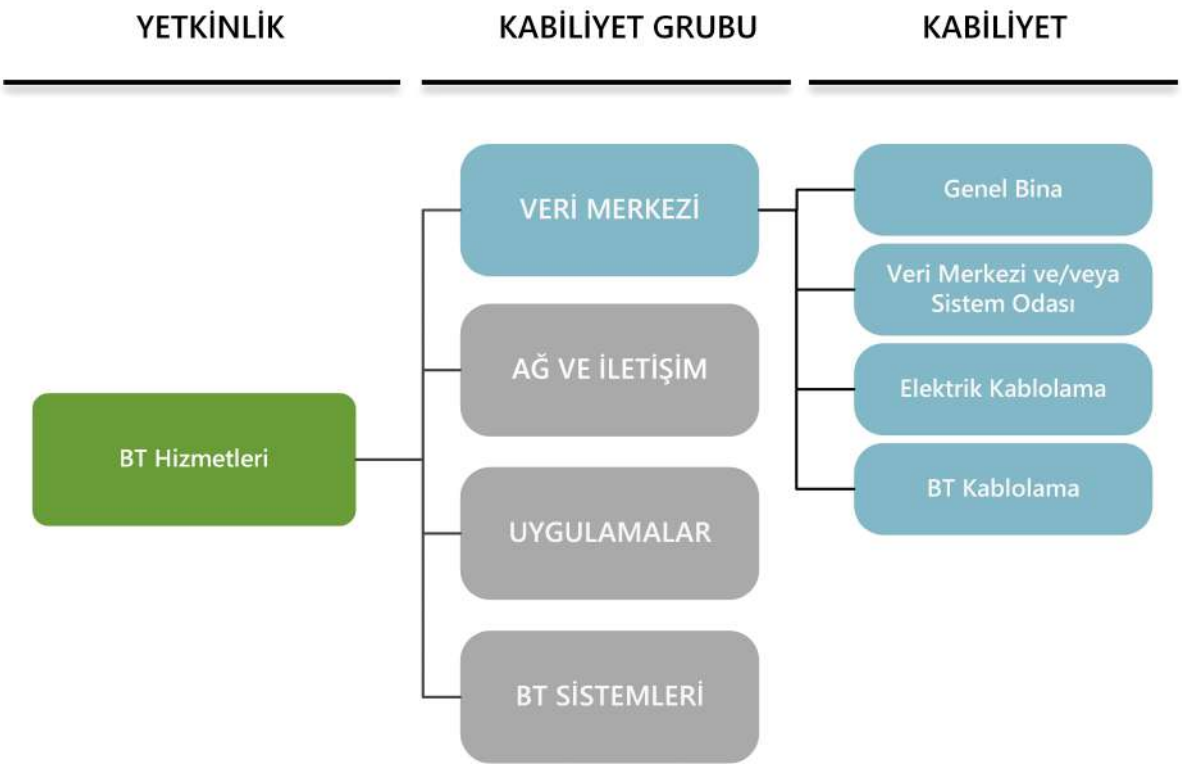
Şekil 7. BT Hizmetleri Yetkinliği Kabiliyet Grupları

- **Veri Merkezi**; Veri merkezi kapsamında, kritik BT bileşenlerini içeren kurumun yapısal-teknik koşullarının yanında, altyapı güvenliği ile ilgili yönlerini de irdeler. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Genel Bina
    - Veri merkezi içerisinde bulunan binalar için, genel bina önlemleri en az bir kere uygulanmalıdır.
  - Veri Merkezi ve/veya Sistem Odası
    - Veri merkezi ve/veya sistem odası modülü, kurumun kritik odaları için uygulanmalıdır.
    - Kurum/organizasyon erişilebilirlik hedeflerine veya organizasyon boyutuna göre bu tür alanlar, rehber içeriğinde kritiklik düzeyine göre özelleştirilerek verilmiştir.
  - Elektrik Kablolama
    - Veri merkezini ve kritik bileşenleri besleyen güç kaynaklarının hedeflenen erişilebilirlik prensipleri doğrultusunda en az bir kere uygulanması gereklidir.

- BT Kablolama
  - Kural olarak bu modül veri merkezinin içerisinde yer alan bina veya yerleşke için en az bir kere uygulanmalıdır. Ayrıca veri merkezi için de kullanılabilir.

- **Ağ ve İletişim**; Ağ ve iletişim sistemleri, belirli BT sistemleri yerine genel ağ bağlantılarına ve iletişimine bakar. Bunlar örneğin; ağ yönetimi, güvenlik duvarı ve WLAN bileşenlerini içerir.
- **Uygulamalar**; Uygulamalar modülü; iletişim, dizin hizmetleri, ağ tabanlı hizmetler ve iş uygulamaları dahil olmak üzere birçok alanı kapsamaktadır. Bu başlığın tipik bileşenleri genel grup yazılımı, ofis ürünleri, web sunucuları ve ilişkisel veri tabanı sistemleridir.
- **BT Sistemleri**; BT sistemleri katmanı içerisinde, kurumun bilişim teknolojilerinde kullanılan sistemleri gruplandırılmış halde sunulmaktadır. Sunucuların, masaüstü sistemlerinin, mobil cihazların ve yazıcılar gibi çevresel BT sistemlerinin güvenlik yönlerini kapsar. Bu modül örneğin, belirli işletim sistemleri, genel akıllı telefonlar ve tabletler, ayrıca yazıcılar, fotokopi makineleri ve çok işlevli cihazlar için bilgileri içerir.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

VRM - VERİ MERKEZİ
TEMEL BİLEŞEN REHBERLERİ

Veri merkezi kapsamında kritik BT bileşenlerini içeren, kurumun yapısal-teknik koşulları ve altyapı güvenliği ile ilgili yönleri aşağıdaki başlıklarda detaylandırılmıştır:

VRM.1.G Genel Bina

VRM.2.G Veri Merkezi ve/veya Sistem Odası

VRM.3.G Elektrik Kablolama

VRM.4.G BT Kablolama

VRM.1.G: GENEL BİNA

1 Açıklama

1.1 TANIM

Binalar, iş süreçlerinin yürütülmesi için gerekli ortamı sağlayan fiziksel yapılardır. Bir bina, iş birimlerini, veriyi, verinin işlenerek elde edilen bilgiyi ve bilgi teknolojilerini barındırır. Ayrıca bu unsurlar için bir koruma sağlar. Gerek iş süreçlerinin ve gerekse BT operasyonlarının yürütülmesinde bina ile birlikte bina altyapısı da oldukça önemlidir. Bu yüzden elinizdeki rehber sadece binaya ilişkin değil, aynı zamanda duvar, tavan, zemin, çatı, pencere ve kapı ile birlikte elektrik, su, gaz, ısıtma ve soğutma gibi unsurlar ile ilgili tüm bina altyapı ve tedarik hizmetlerine ilişkin gereksinimleri içermektedir.

Bina içerisinde yer alan birimlerin birbirinden farklı ihtiyaçları bulunabilir. Bir bina aynı anda farklı taraflarca (ziyaretçiler, müşteriler, tedarikçiler vb.) kullanılabilir. Bu farklı kullanımlar göz önünde bulundurularak, bina tasarımı ve kullanılan altyapı ekipmanları ile bina kullanım konseptinin uyumlu olması sağlanmalıdır. Bina içerisinde teknolojik bileşenlerin etkin ve güvenli bir biçimde kullanılmasıyla, çalışanlar için en uygun ortamın sağlanması hedeflenmelidir.

1.2 HEDEF

Genel bina temel bileşen rehberi, bir binanın kurum ihtiyaçları doğrultusunda en uygun şekilde kullanılması için hangi gereksinimlerin karşılanması gerektiğini açıklamaktadır. Gereksinimleri karşılamak için uygulanacak önlemler ve çözümler, kurumun türüne ve boyutuna bağlı olarak değişebilir. Bu önlemler ve çözümler genel bina uygulama rehberi içerisinde yer almaktadır. Elinizdeki rehber bir bina içerisinde bulunan kurumlar tarafından kullanılabileceği gibi, birkaç bina veya kampüse/yerleşkeye yayılmış kurumlar tarafından da kullanılabilir.

1.3 KAPSAM DIŞI

Bu modül, içerisinde veri merkezi veya sistem odası yer alan, kurum ve şirket binalarının planlama ve kullanılmasında teknik ve teknik olmayan gereksinimleri ve bu gereksinimlere yönelik yararlanılabilecek uygulamaların kısa bir özetini içerir.

Kurumların belirli bir yaşam döngüsünü takip ederek, önerileri uygulamaları beklenmektedir. Örneğin sırasıyla şu adımlar yerine getirilebilir:

- Gereksinimlerin belirlenmesi,
- Uygun önlemlerin/çözümlerin seçilmesi,
- Yapılandırma ve kurulum,

- Uygulama ve işletme.

Bu rehber içerisinde belirli konu detaylarına (örneğin kablolama gibi) özellikle girilmemektedir. Bu tür detaylar ayrıntılı olarak diğer veri merkezi rehberlerinde ele alınmaktadır.

2 RİSK KAYNAKLARI

Aşağıdaki riskler ve eksiklikler genel bina güvenliği açısından özellikle önemlidir:

2.1 YANGIN

Bina ve içerisinde bulunan kişiler yangın esnasında ciddi hasar görebilir. Yangın nedeniyle meydana gelebilecek doğrudan hasarın yanında, dolaylı hasar oluşabilir. Bir yangında en büyük tehlike kaynağı toksik yangın dumanıdır ve kişisel yaralanmaların çoğu, duman zehirlenmesi ile meydana gelir. Cihazlar, altyapı ekipmanları ve BT bileşenleri üzerinde de yangın dumanı ciddi hasarlara neden olabilir.

Örneğin PVC yandığında, nem ve söndürücü su ile birlikte hidroklorik asit oluşturan klor gazı üretir. Hidroklorik asit buharlarının iklimlendirme sistemi aracılığıyla dağıtılması, binanın yangından uzak bir yerinde bulunan hassas elektronik ekipmanların zarar görmesine neden olabilir.

2.2 YILDIRIM

Yıldırımlar, bina ve içerisinde yer alan veri merkezileri için tehlike oluşturur. Yıldırım, bulut ile yer arasında meydana gelen yüksek gerilimli bir elektrik boşalmasıdır. Bina yakınında meydana gelebilecek bir yıldırım yüksek akım, aşırı gerilim ve güç dalgalanmalarına yol açabilir. Bu durum binada elektrik ile beslenen cihazların hasar görmesine, tahrip olmasına neden olur.

Yıldırım bir binaya doğrudan vurursa, onun dinamik enerjisi bina üzerinde ciddi hasarlar oluşturabilir. Yıldırım binaya (çatı ve cephe) zarar verebilir, oluşabilecek yangınlar veya aşırı gerilim nedeniyle de altyapı ekipmanları ve BT bileşenleri zarar görebilir.

2.3 SU

Bina içerisinde, su taşkınları, borulardaki çatlaklar, hatalı yangın söndürme sistemleri, kanalizasyon hasarı ve klima arızaları nedeniyle iç kaynaklı veya yağmur, sel ve taşkın gibi dış kaynaklı su sızıntıları oluşabilir. Bu durum bina ve içerisinde yer alan tesisatın hasar görmesine ve çalışamamasına; olası bir kısa devre nedeniyle veri merkezi elektrik sisteminin kesintiye uğramasına ve hatta yangına neden olabilir.

2.4 DOĞAL TEHLİKE VE FELAKETLER

Bina, bulunduğu yere bağlı olarak farklı derecede doğal tehlike ve felaketlere maruz kalabilir. Sismik, iklimsel veya volkanik kaynaklı doğal felaketler binaya zarar verebilir. Sel felaketi, deprem, heyelan, tsunami, çığ, volkanik patlamalar doğal felaketlere örnek olarak gösterilebilir.

2.5 ÇEVRESEL TEHLİKELER

Binalar, yakın çevrede yaşanabilecek olaylardan zarar görebilir. Örneğin yakında yer alan bir üretim tesisinden zehirli maddelerin yayılması, havaalanları, demiryolları, çevrede bulunan tehlikeli fabrikalar, terörist ataklar bina ve içerisinde yer alan tesisatın hasar görmesine neden olabilir.

2.6 İZİNSİZ GİRİŞ

Bina çevresinde giriş kontrollerinin bulunmaması veya yetersiz olması, yetkisiz ve kötü niyetli kişilerin bina ve içerisinde bulunan veri merkezine zarar verme riskini artırır, onarılması güç hasarlara neden olabilir. Yetkisiz erişim, verilerin ve BT bileşenlerinin erişilebilirliği, gizliliği ve bütünlüğü üzerinde oldukça önemli bir etkiye sahiptir. Yetkisiz erişim nedeniyle, kurum için kritik ve hassas veriler ve BT bileşenleri çalınabilir, değiştirilebilir, farklı şekilde yapılandırılabilir veya zarar görebilir.

Açıkça görülemeyen değişiklikler ve farklı yapılandırmalar, doğrudan tahribata kıyasla çok daha fazla hasara neden olabilir.

2.7 YASA VE YÖNETMELİKLERE UYULMAMASI

Binaların planlanması, inşa edilmesi, işletilmesi sırasında uyulması gereken birçok farklı yasa ve yönetmelik bulunmaktadır. Yasal düzenlemeler ile gerek binanın, gerekse bina içerisinde bulunan kişilerin etkinliği, verimliliği ve güvenliği güvence altına alınır. Tabi olunan yasal düzenlemelere uyulmaması, bina veya insan güvenliğini tehlikeye atabileceği gibi kurum için cezai yaptırımlar uygulanmasına da neden olabilir.

2.8 YETERSİZ YANGIN DAYANIMI

Veri merkezi ve/veya sistem odası barındıran bina, birçok tesisat hattı ve kablo taşıma kanalları barındırır (örn. kanalizasyon boruları, ısıtma boruları, enerji iletimi ve veri iletimi için kullanılan kablolar). Bu gibi yerlerde yangına dayanıklı yapı malzemelerinin kullanılmaması, yangın ve duman kontrolünü olumsuz olarak etkileyebilir. Bu risk unsurları kontrol altına alınmaz ise, bitişik odadaki bir yangın veri merkezine sıçrayabilir, ayrıca veri merkezi içerisinde kolaylıkla yayılabilir. Diğer taraftan, veri merkezi içerisinde başlayan bir yangın tüm binaya yayılabilir.

2.9 ELEKTRİK İLETİMİNİN ARIZALANMASI

Bina içerisinde yaşanabilecek bir elektrik kesintisi veri merkezinde bulunan BT bileşenlerinin ve dolayısıyla kurumun çalışmasında önemli aksaklıklara neden olabilir. BT hizmetleri aniden ulaşılamaz hale gelebilir, kritik veriler kaybolabilir. Yaşanan elektrik kesintisinin BT bileşenlerine ve altyapı ekipmanlarına (aydınlatma elemanları, asansörler, iklimlendirme sistemleri, güvenlik sistemleri, güvenlik kilitleri, otomatik kapı kilitleme sistemleri, yağmurlama sistemleri, telefon uzatma sistemleri gibi) zarar vermesi de mümkündür.

3 GEREKSİNİMLER

Genel binaya ilişkin, karşılanması beklenen gereksinimler bu başlıkta açıklanmaktadır. Kurumdan kuruma değişiklik gösterebilmekle birlikte, genel olarak bina gereksinimlerinin karşılanmasından bina/kampüs hizmetleri yöneticisi sorumludur. Her bir gereksinim içerisinde, ilgili diğer sorumlu kişiler de tanımlanmıştır. Kurumların son zamanlarda bilgi güvenliği (ve özellikle ISO 27001) çalışmaları gerçekleştirmekte olduğu göz önünde bulundurularak, bilgi güvenliği sorumlusunun stratejik kararlara dahil edilmesi de sağlanabilir. Bilgi güvenliği görevlisi ayrıca, gereksinim maddelerinin uygulanması sırasında kurum için oluşturulan güvenlik politikalarına uyumluluğun kontrolünden de sorumludur.

Rehber içerisinde gereksinimler, üç ana başlık içerisinde toplanmıştır. Kurumların öncelikli olarak “1.Seviye Gereksinimler” başlığı altında yer alan maddeleri zorunlu olarak değerlendirmeleri, sonra ihtiyaçları doğrultusunda “2.Seviye Gereksinimler” ve “3.Seviye Gereksinimler” başlıklarını ele almaları önerilmektedir.

Tablo 2. Genel Bina Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Yöneticisi
Diğer Sorumlular	Bina Hizmetleri Yöneticisi, Bilgi Güvenliği Sorumlusu, Teknisyen, Proje Yöneticisi, Personel, Planlama Sorumlusu

3.1 1.SEVİYE GEREKSİNİMLER

Kurumlar ve organizasyonlar aşağıda yer alan gereksinimleri öncelikli olarak uygulamalıdırlar.

VRM.1.G1 Bina güvenliği planlaması [Planlama Sorumlusu, Bilgi Güvenliği Sorumlusu]

Bina güvenliğine ilişkin herhangi bir planlama yapılmış mı?

Bina içerisinde işletilen iş süreçlerine ve veri merkezinin koruma gereksinimlerine bağlı olarak bina güvenliği planlanmalıdır. Planlama sırasında, binada çalışacak kişilerin ve kritik varlıkların korunmasına yönelik gereksinimler, farklı birimlerin güvenlik gereksinimleri, bina içerisinde yer alacak BT bileşenlerine ilişkin ihtiyaç duyulan erişilebilirlik seviyeleri, olası çevresel tehlikeler, iç ve dış tehdit unsurları dikkate alınmalıdır.

VRM.1.G2 Elektrik yük dağılımının ayarlanması/yapılandırılması

Elektrik tesisatı, ihtiyaçlara uygun bir şekilde tasarlanmış mı? Güncel ihtiyaçları karşılayıp karşılamadığı kontrol ediliyor mu?

Bina tasarımı sırasında, bina içerisinde yer alacak birimlerin, altyapı ekipmanlarının ve veri merkezinde yer alacak BT bileşenlerinin kullanım gereksinimleri göz önünde bulundurularak elektrik tesisatı tasarlanmalı ve kullanıma hazır hale getirilmelidir. Kurulu elektrik tesisatının, güncel ihtiyaçları karşılama durumu düzenli olarak kontrol edilmelidir.

VRM.1.G3 Yangın güvenliği yönetmeliklerine uyulması

Yangın güvenliği yönetmeliklerine uyuluyor mu?

Bakanlar Kurulu tarafından kararlaştırılan, Resmi Gazete'de yayımlanan, bina yangın korunma yönetmeliği gereksinimlerine uyulmalıdır. Bina içerisinde yer alan kaçış yolları, yönetmeliklere uygun olarak işaretlenmeli ve açık tutulmalıdır. Yerel itfaiyenin, yangın güvenliği planlamasına dahil edilmesi önerilmektedir. Bina içerisinde yer alan veri merkezi/sistem odası ile ilgili detaylı bir yangın koruma yaklaşımı oluşturulmalı ve uygulanmalıdır.

Bina içerisinde yangın oluşturabilecek gereksiz materyal ve cihazlardan kaçınılmalı, atık kağıtların ve ambalaj atıklarının düzenli bir şekilde imha edilmesi sağlanmalıdır.

Yangın güvenliğine ilişkin tüm çalışmaların, yangın güvenliği konusunda eğitimli personel ya da yangın acil durum sorumlusu koordinasyonunda yürütülmesi tavsiye edilmektedir.

VRM.1.G4 Binalarda yangın algılama [Planlama Sorumlusu]

Yangının zamanında algılanabilmesi için bir yangın alarm sistemi bulunuyor mu?

Yangının zamanında algılanabilmesi için bina içerisine yeterli sayıda duman dedektörü yerleştirilmelidir. Büyük binalarda tüm dedektörlerin bağlı olduğu bir yangın alarm paneli kullanılması önerilir. Dedektörler tarafından duman algılanması durumunda, bina

içerisinde bulunan herkesin duyabileceği ölçüde alarm tetiklenmesi sağlanmalıdır. Tehlikeli ve acil bir durumda, bina içerisinde bulunan kişilerin, hızlı bir şekilde binayı tahliye edebilmeleri için gerekli önlemler alınmalıdır.

Bina içerisine yerleştirilmiş tüm duman dedektörlerinin ve kurulu yangın alarm sisteminin işlevselliği düzenli olarak test edilmelidir. Ayrıca acil durumda tahliye için kullanılacak kaçış yollarının kullanılabilir ve engelsiz olduğu düzenli olarak kontrol edilmelidir.

VRM.1.G5 Taşınabilir yangın söndürücüler

Taşınabilir yangın söndürücüler kullanılıyor mu?

Yangın durumunda, bina içerisinde yangının hızlı bir şekilde söndürülebilmesi için yeterli sayıda ve boyutta taşınabilir yangın söndürücüleri (TS 862-3, DIN/EN 3-3 standartlarına uygun) bulundurulmalıdır. Yangın durumunda, yangın söndürücülerin kolayca erişilebilir bir yerde tutulması sağlanmalı ve yangın söndürücüler düzenli olarak kontrol edilmelidir. İlgili personele taşınabilir yangın söndürücülerin kullanımı konusunda eğitimlerin verilmesi ve talimatların hazırlanması önerilmektedir.

VRM.1.G6 Kapalı pencereler ve kapılar [Personel]

(Özellikle dışarıya bakan) Pencerelerin ve kapıların kapalı tutulmasına ilişkin bir talimat/politika bulunuyor mu?

Bina içerisinde yer alan odaların mesai saatleri dışında, dışa bakan pencereleri ve dış ortama açılan kapıları (balkonlar, teraslar) kapalı tutulmalıdır. Bina içerisinde çalışacak tüm personelin buna uygun hareket etmesini sağlamak için bir talimat hazırlanması tavsiye edilir. Odayı terk eden son kişi, pencerelerin ve kapıların kapalı olup olmadığını kontrol etmelidir. Ayrıca kritik odaların (örneğin veri merkezi / sistem odası) pencereleri ve kapıları belirli aralıklar ile kontrol edilmelidir. Özellikle yangına ve dumana karşı yalıtımlı koruma kapılarının açık tutulmasına izin verilmemelidir.

VRM.1.G7 Güvenlik ve Erişim Kontrolü [Organizasyon Yöneticisi]

Bina içerisinde koruma gerektiren alanlara erişimi kontrol eden herhangi bir mekanizma oluşturuldu mu?

Bina içerisinde koruma gerektiren bölümleri ve odaları yetkisiz erişime karşı koruyabilmek için bir erişim kontrol mekanizması kurulmalıdır. Bu amaçla, erişim yönetmeliği/prosedürü/politikası hazırlanması, bütün alanlara erişim hakkına sahip kişilerin sayısının asgari düzeyde tutulması, sadece görev tanımları gereği ilgili alanlara erişimlerin sağlanması önerilir.

Bina içerisinde farklı alanlara girmesi gereken ziyaretçilerin ve harici personelin, ancak gerekliliğin incelenmesinden sonra ilgili alana girmesine izin verilmelidir. Tüm girişlerin ve çıkışların kayıt altına alınması ve denetlenmesi önerilir. Ayrıca binaya tüm girişlerin ve çıkışların izlenmesi sağlanmalıdır. Güvenlik ihtiyacı farklı olan odalar için ne detayda bir izleme kontrolünün yapılması gerektiği önceden hesaba katılmalıdır.

Belirli aralıklar ile erişim kontrolünün kullanımına ilişkin düzenlemelere uyulup uyulmadığı ve erişim kontrol önlemlerinin etkinliği kontrol edilmelidir.

3.2 2.SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, binaların durumlarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

VRM.1.G8 Binanın fiziksel güvenlik çerçevesi [Bina Hizmetleri Yöneticisi, Planlama Sorumlusu, Bilgi Güvenliği Sorumlusu]

Bina kullanımına ilişkin bir güvenlik modeli oluşturulmuş mu?

Kurum ihtiyaçlarına uygun şekilde, bina kullanımı için bir güvenlik modeli oluşturulması önerilir. Bu kapsam içerisinde genel koruma hedefleri, kurumun değerli varlıkları, kritik odaların ve alanların, personelin güvenliğine yönelik önlemler ile birlikte erişim kontrolü, yangından korunma ve altyapı güvenliğini sağlama gibi unsurlar yer almalıdır.

Oluşturulan bina güvenlik sistemi belirli aralıklarla gözden geçirilmeli, gerekli durumlarda (bina kullanımının değişimi, kurum için önceliklerin ve güvenlik ihtiyaçlarının değişimi, vb.) güncellenmelidir.

VRM.1.G9 Uygulanabilir standartlara ve düzenlemelere uyum [Yüklenici, Bina Hizmetleri Yöneticisi]

Tabi olunan standartlara ve düzenlemelere uyum sağlanıyor mu?

Binaların planlanması, inşa edilmesi, işletilmesi ve yenilenmesi sırasında, BT bileşenlerinin ve altyapı ekipmanlarının kurulumunda ilgili tüm standartların ve düzenlemelerin dikkate alınması önerilir.

VRM.1.G10 Kapıların kilitlenmesi [Personel]

(Özellikle mesai saatleri dışında) Belgelerin ve BT bileşenlerinin güvenli ortamlarda saklanmalarına ilişkin bir yaklaşım var mı?

Bina içerisinde çalışanlar, mesai saatleri dışında ofis kapılarını kapatmaları ve masalarındaki belgeleri güvenli olarak saklamaları hususunda bilgilendirilmelidirler. Çalışanların bu uygulamaya uyumlulukları belirli aralıklarla kontrol edilmelidir.

VRM.1.G11 Anahtar/kilit yönetimi

Odalara giriş/çıkış için kullanılan anahtarlar ve kartlar merkezi olarak yönetiliyor mu?

Bina içerisinde kullanılan tüm anahtarlar için (katlar, koridorlar ve odalar) bir kilitleme planı oluşturulmalıdır. Anahtarların üretimi, depolanması, yönetimi ve dağıtılması merkezi olarak yönetilmelidir. Yedek anahtarlar güvenli bir biçimde saklanmalı, bununla birlikte yedek anahtarların acil durumlar için ulaşılabilir olması (yetkili kişiler aracılığı ile) sağlanmalıdır. Kullanım için yetkili personele verilen anahtarlar kayıt altına alınmalıdır. Belirli aralıklarla anahtarların yerinde (veya verilen kişilerde) olup olmadığı kontrol edilmelidir.

VRM.1.G12 Dağıtım panolarına erişimle ilgili düzenlemeler

Enerji ve ağ dağıtım panolarına kimler erişebilir?

Binadaki dağıtım panoları (elektrik, ağ, telefon vb.), acil durumlarda erişilebilecek şekilde konumlandırılmalıdır. Dağıtım panolarının kilitli tutulması ve erişimin sınırlı sayıda yetkiliye verilmesi önerilmektedir.

VRM.1.G13 Yıldırımdan korunma cihazları

Bina içinde ve dışında yıldırımdan korunma sistemleri kullanılmakta mı?

Yıldırımın fiziksel etkilerinden korunma amaçlı, standartlara uygun bir yıldırımdan korunma sistemi kurulmalıdır. Sistem, iç ve dış kaynaklı aşırı yüksek gerilimlerinin sebep olacağı tüm olumsuz etkilere karşı elektrik tesisatını ve tesisata bağlı teçhizatı korumalıdır. Bu tür cihazlar ile ilgili çeşitli standartlar bulunmaktadır. ISO 62305, IEC 61643-11, IEC 60634, UL 1449 bunlardan bir kısmıdır. Türkiye'de TS EN 62305-1/2/3/4 standardı yıldırıma karşı koruma oluşturmanın genel kurallarını açıklar. Kapsamlı bilişim donanımına sahip binalar için yıldırım koruma cihazları, en azından ISO / DIN EN 62305 standardı koruma sınıfı II'ye uyacak şekilde yapılandırılmalıdır. Ayrıca yıldırımdan korunma sisteminin düzenli olarak kontrol edilmesi ve sadece yetkili kişilerin bu sisteme erişebilmeleri sağlanmalıdır.

VRM.1.G14 Altyapı tesisat hatlarının yerleşim planları

Bina içerisinde kullanılan tesisatlara ilişkin detaylı planlar bulunuyor mu?

Bina içerisinde (ve çevresinde) yer alan tesisat hatlarına ilişkin detaylı bilgileri içeren planlar hazırlanmalıdır. Tesisat planlarını güncelleyecek kişiler/ekipler önceden belirlenmeli ve herhangi bir değişiklik/yenilik sonrası bu planların güncellenmesi sağlanmalıdır. Planlar, yalnızca yetkili kişilerin erişebileceği şekilde muhafaza edilmeli ve ihtiyaç duyulduğunda hızlı bir şekilde kullanılabilir halde tutulmalıdır.

VRM.1.G15 Korunma gerektiren bina bölümlerine ilişkin konum/tabela bilgilendirilmelerinden kaçınma

Bina içerisinde özel korunma gerektiren bölümlere ilişkin gösterge/tabelalar kaldırılmış mıdır?

Binanın özel koruma gerektiren bölümlerinde (veri merkezi, sunucu odası, vb.), bu bölümleri açığa çıkaracak bir biçimde gösterge/tabela kullanılmasından kaçınılmalıdır. Ayrıca bu bölümlerin gerek içeriden gerekse dışarıdan kolay bir biçimde görülmemesi sağlanmalıdır.

VRM.1.G16 Dumandan korunma [Planlama Sorumlusu]

Yangın anında dumandan korunma önlemleri alınmış mı?

Yangında meydana gelen can ve mal kayıplarının önemli sebeplerinden biri de dumandır. Duman içeriğindeki zehirli maddeler ve gazlar doğrudan hayatı tehdit etmekte, bünyesindeki diğer katı ve sıvı tanecikler de BT bileşenleri üzerinde çeşitli hasarlara yol açmaktadır. Bu nedenle, bina içerisinde kapsamlı duman korumasına önem verilmelidir.

Binanın dumandan korunma önlemleri, her türlü kurulum ve dönüştürme çalışması sonrası gözden geçirilmelidir. Belirli aralıklar ile düzenlenen testler/tatbikatlar aracılığıyla duman koruma bileşenlerinin işlevselliği kontrol edilmelidir.

VRM.1.G17 Yangın güvenlik kontrolleri

Yangın güvenlik kontrolleri gerçekleştirildi mi?

Bina bünyesinde alınmış yangın önlemlerinin kontrolünü sağlamak amacıyla, düzenli aralıklarla (yılda en az bir veya iki kez olmak üzere) yangın önleme sistemlerinin düzgün çalıştığının test edilmesi önerilir. Bu testler sırasında tespit edilen aksaklıkların hızlı bir biçimde giderilmesi için gerekli iyileştirme planları gerçekleştirilmelidir.

VRM.1.G18 Acil durum sorumlusunun zamanında bilgilendirilmesi

Kurum bünyesinde yangın önlemlerinden sorumlu bir acil durum sorumlusu atanmış mı? Bu kişiye gerekli konularda bilgilendirmeler yapılmış mı?

Kurum içerisinde yangın önlemleri ile ilgili en yetkili kişi olan acil durum sorumlusu, tesisat hattı güzergâhları, koridorlar, kaçış ve kurtarma güzergâhları üzerinde gerçekleştirilecek çalışmalara ilişkin detaylı bilginin aktarılması gereklidir. Yangın konularında ki acil durum sorumlusunun koordinasyonunda, yangın önleme tedbirlerinin alınması, düzgün bir biçimde işletilmesi, gerektiğinde güncellenmesi ve kontrol edilmesi sağlanmalıdır.

VRM.1.G19 Acil durum planı ve yangın tatbikatları

Bina için hazırlanmış bir yangın planı bulunuyor mu? Yangın tatbikatları gerçekleştiriliyor mu?

Yangın durumunda alınacak önlemler bir acil durum eylem planı içerisinde yazılı hale getirilmelidir. Kurum çalışanlarının katılımıyla, belirli aralıklarla yangın tatbikatlarının gerçekleştirilmesi önerilir. Tatbikat sırasında yazılı plana uygun bir biçimde yetkili ekiplerin görevleri yerine getirdiği, planda yer alan tedbirlerin doğru, güncel ve pratik olup olmadığı kontrol edilmelidir. Gerekli durumlarda planın güncellenmesi sağlanmalıdır. Ayrıca alarm planı belirli aralıklarla gözden geçirilmeli ve gerekli durumlarda güncellenmelidir.

3.3 3.SEVİYE GEREKSİNİMLER

1. ve 2. seviye gereksinimler sonrasında, binalar için artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilmektedir. Gereksinim tarafından öncelikli koruma sağlanan prensip parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.1.G20 Bağımsız elektrik hatları üzerinden beslenme (E)

Bina içerisinde elektrik iletimi için birbirinden farklı iki elektrik hattından yararlanılıyor mu?

Binanın, özellikle içerisinde yer alan veri merkezi / sistem odasının, birbirinden bağımsız en az iki elektrik hattı aracılığıyla beslenmesi sağlanmalıdır.

VRM.1.G21 Güvenli Kapılar ve Pencereler (GBE)

Korunması gereken odalar için (özel) güvenli kapılar ve pencereler kullanılmış mı?

Güvenli kapılar ve pencereler için birçok farklı standart bulunmaktadır. Bina içerisinde korunacak alanın ve kurumun, güvenlik ihtiyaçlarına uygun standardın belirlenmesi ve belirlenen standarda uygun kapı ve pencere seçilmesi gerekmektedir. Güvenlik önlemlerinin yer aldığı, korunması gereken tüm odaların kapıları ve pencereleri hırsızlık, yangın ve dumana karşı güvenli hale getirilmelidir. Kapılar ve pencereler için alınan güvenlik tedbirlerinin işlevselliği düzenli kontrollerle takip edilmelidir.

VRM.1.G22 Güvenlik bölgelerinin oluşturulması [Planlama Sorumlusu] (B)

Bina içerisinde farklı koruma ihtiyaçları için farklı güvenlik bölgeleri oluşturulmuş mu?

Bina içerisinde farklı güvenlik bölgeleri oluşturulmalıdır. Benzer koruma ihtiyaçlarına sahip olan farklı odalar, ortak riskler ile karşı karşıya kalabilir. Söz konusu aynı risklere yönelik ortak önlemlerin alınabilmesi gerekli güvenlik önlemlerinin toplam maliyetini düşürecektir. Benzer koruma ihtiyaçlarına sahip odalar aynı güvenlik bölgesi içerisine konumlandırılarak ortak güvenlik önlemlerinden faydalanmalıdır. Bina ve yerleşke için oluşturulan güvenlik bölgeleri tanımlanarak yazılı hale getirilmeli ve yetkili kişiler ile paylaşılmalıdır.

VRM.1.G23 Otomatik drenaj (E)

Su tahliyesi için otomatik drenaj uygulanmış mı?

Bina içerisinde tüm su tehlikesi oluşturan alanlar, gerekli durumlarda istenmeyen ve binaya zarar verebilecek suyun uzaklaştırılabilmesi için otomatik drenaj ile donatılmalıdır. Ayrıca bina bünyesinde oluşturulan aktif ve pasif drenaj tesislerinin işlevselliği düzenli olarak kontrol edilmelidir.

VRM.1.G24 Uygun yer seçimi [Kurum Yöneticisi] (E)

Binanın yer seçimi sırasında çevre koşulları göz önünde bulundurulmuş mu?

Bina/yerleşke için yer belirlerken ve binayı/yerleşkeyi planlarken, özellikle bina içerisinde yer alacak veri merkezini/sistem odasını etkileyebilecek çevre koşulları incelenmelidir. Belirlenen yerler ile ilgili riskler analiz edilmelidir. Bu riskleri kontrol altına alabilmek için gerekli önlemler planlanmalıdır.

VRM.1.G25 Güvenlik görevlileri ve bina güvenlik hizmeti (GBE)

Bina/kampüs girişinde yetkin güvenlik görevlileri yer alıyor mu?

Bina girişinde görev yapacak güvenlik görevlilerinin sorumlulukları, açık ve net bir şekilde tanımlanmalı ve yazılı hale getirilmelidir. Güvenlik görevlileri, kapıdaki ve diğer tüm girişlerdeki hareketleri gözlemlemeli ve kontrol etmelidir. Tüm çalışanların ve ziyaretçilerin, geçerli bir kimlik doğrulama sonrasında binaya giriş yapabilmesi sağlanmalıdır. Ziyaretçilerin bina içerisine giriş nedeni/ihtiyacı sorgulanmalı, gerekli onay alınması durumunda giriş izni verilmelidir. Güvenlik görevlileri veya yetkili çalışanlar, ziyaretleri süresince ziyaretçilere refakat etmelidirler. Çalışanlara veya ziyaretçilere ilişkin erişim izinlerinin değişmesi durumunda güvenlik görevlileri zamanında bilgilendirilmelidir. Çeşitli eğitim ve bilgilendirme çalışmaları ile güvenlik görevlilerinin BT yetkinlikleri artırılmalıdır.

VRM.1.G26 Hırsızlığa Karşı Koruma (GBE)

Bina içerisinde hırsızlığa karşı koruma önlemleri alınmış mı?

Bina içerisinde hırsızlığa ve saldırıya karşı gerekli önlemler uygulanmalıdır. Planlama, uygulama ve işletme aşamalarında hırsızlığa karşı uygulanan güvenlik önlemlerinin yeterliliği ve işlerliği yetkili bir kişi tarafından düzenli olarak kontrol edilmelidir. Hırsızlığa karşı korunma önlemleri konusunda çalışanların dikkat etmesi gereken hususlar tanımlanmalı, yazılı hale getirilmeli ve tüm çalışanlar ile paylaşılmalıdır.

VRM.1.G27 İklimlendirme (Klima) Sistemleri (BE)

Bina içerisinde uygun iklim koşulları oluşturuluyor mu?

Binalarda havalandırma, çalışanların uygun ortamlarda çalışabilmesini sağlayacak biçimde, havalandırma/iklimlendirme sistemleri ile sağlanır. İklimlendirme sistemleri bina kullanımına ve insan sağlığına uygun bir şekilde tasarlanmalıdır. Ayrıca kullanılan sistemlerin periyodik bakımları planlanmalı ve gerçekleştirilmelidir.

VRM.1.G28 Bina temizliği için prosedürler (GBE)

Bina içi temizlik çalışmaları kontrol ediliyor mu?

Bina içi temizliğin sağlanmasından sorumlu temizlik görevlilerinin veya bina temizliği için görevlendirilen temizlik şirketi çalışanlarının, binadaki odalara erişim için kendilerine verilen anahtarları veya kimlikleri uygun bir biçimde kullanıp kullanmadıkları kontrol edilmelidir. Temizlik personeli, BT bileşenleri ve kurum içi bilgi yönetimi hakkında yeterince bilgilendirilmelidir. Özellikle veri merkezi / sistem odası gibi kritik alanlarda, temizlik personelinin yetkili bir kişi gözetiminde ve denetiminde temizlik çalışmalarını gerçekleştirmesi sağlanmalıdır.

VRM.1.G29 Uygun bina seçimi (GBE)

Bina seçimi sırasında bina içi koşullar göz önünde bulundurulmuş mu?

Uygun yer seçimine ek olarak, belirlenen binaya ilişkin iç koşulların kurum gereksinimlerine uygunluğu kontrol edilmelidir. Bina içi mevcut riskler ve tehlikeler belirlenmeli, gerekli hasar önleme veya azaltma tedbirleri planlanmalıdır.

VRM.1.G30 Bina tahliyesi [Teknisyen] (B)

Binanın tahliye öncesi, kritik varlıkların envanteri hazırlandı mı?

Binanın belirli bir bölümünün veya tamamının taşınması öncesinde BT bileşenlerini ve kurum için kritik bilgi varlıklarını (donanım, yazılım, medya, klasörler, belgeler vb.) içeren bir envanter hazırlanması önerilmektedir. Taşınma sonrasında hazırlanan envanter kullanılarak, BT bileşenlerinin ve kritik bilgi varlıklarının düzgün ve eksiksiz bir biçimde taşınıp taşınmadığı kontrol edilmelidir.

VRM.1.G31 Korunması gereken alanların düzenlenmesi (GBE)

Bina içerisinde yer alan kritik odalar hangi bölümlerde yer alıyor? Nasıl korunuyor?

Korunması gereken odaların dışarıdan görülebilen, dış tehditlere açık ve tehlikeli olabilecek alanlarda konumlandırılmaması gerekir. Korunması gereken odaların bu tarz alanlarda bulunması durumunda, olası tehditlerin belirlenerek yazılı hale getirilmesi, söz konusu tehditlere yönelik önlemlerin alınması sağlanmalıdır.

VRM.1.G32 İkaz ve Alarm Sistemi (E)

Bina içi yaşanan acil durumların ve olayların ilgili kişilere zamanında duyurulabilmesi için bir ikaz ve alarm sistemi yer alıyor mu?

Bina içerisinde, belirlenmiş risklere uygun bir ikaz ve alarm sistemi kurulmalıdır. Alarm sistemi düzenli olarak kontrol edilmeli, uygun bir biçimde çalışması güvence altına alınmalıdır.

4 DETAYLI BİLGİ İÇİN KAYNAKLAR

Genel bina ile ilgili detaylı konulara aşağıdaki referans ve kaynaklardan ulaşılabilir:

- ISO/IEC 27001:2013 - Annex A.11 Physical and enviornmental security
  ISO, Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.11 Physical and environmental security, 2013
- https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en The Standard of Good Practice - AREA CF19 Physical and Environmental Security
  AREA CF19 Physical and Environmental Security, ISF, 06.2014
- NIST Special Publication 800-53 Revision 4 - APPENDIX PAGE F-213
  Assesing Security and Privacy Controls for Federal Information Systems and Organizations, insbesondere APPENDIX F-PS PAGE F-213, FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION, NIST, 2013
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- BSI - Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_1_Allgemeines_Geb%C3%A4ude.html
- TS EN 62305-1/2/3/4

VRM.2.G: VERİ MERKEZİ VE/VEYA SİSTEM ODASI

1 AÇIKLAMA

1.1 GİRİŞ

Günümüzde hemen hemen tüm stratejik ve operasyonel görevler, bilgi teknolojisi (BT) tarafından önemli ölçüde desteklenmekte ve BT olmadan yürütülememektedir. Bu yüzden, BT sistemlerinin performans, erişilebilirlik ve ağ bağlantı gereksinimleri giderek artmaktadır. Bu gereksinimleri karşılamak, kaynakları korumak ve BT sistemlerini ekonomik olarak işletebilmek için kurumlar ve şirketler BT birimlerine yoğunlaşmaktadır.

Veri merkezleri; sunucular, depolama, ağ (network) ve haberleşme cihazları ile benzeri BT donanımlarının güvenli bir şekilde çalışmalarının sağlandığı, verilerin saklandığı, korunduğu, bununla birlikte kullanıcıların kesintisiz ve hızlı bir şekilde verilere ulaşması için gerekli tüm teknik altyapının yer aldığı odalardan oluşur. Veri merkezleri; kullanıldığı kurumun faaliyet alanı büyüklüğü, kritiklik seviyesi ve kapasitesi gibi unsurlara göre tasarlanmaktadır.

Veri merkezi içerisinde, BT bileşenleri ile destek altyapısını oluşturan ekipmanlar (elektrik güç kaynağı, klima teknolojisi vb.) genellikle farklı odalarda bulunurlar. Fakat birçok kurum, içinde bulundukları koşullar nedeniyle tüm gerekli ekipmanları tek bir oda içerisinde barındırmayı tercih etmektedir. Elinizdeki rehber içerisinde bu tip odalar, sistem odası olarak adlandırılmaktadır.

Veri merkezi işleten veya veri merkezi hizmetinden yararlanan kurumların elinizdeki rehber içerisinde yer alan gereksinim maddelerini incelemeleri, öncelikle temel gereksinimlerden başlayarak ihtiyaçları doğrultusunda bu maddeler içerisinde yer alan uygulamaları gerçekleştirmeleri önerilmektedir.

Diğer yandan, sistem odasına sahip kurumların, sahip oldukları imkanlar doğrultusunda, bu rehberde yer alan gereksinim maddelerini dikkate almaları ve en azından **temel gereksinimleri** yerine getirmeleri beklenmektedir.

1.2 HEDEF

Veri merkezi rehberi ile veri merkezi/sistem odası bulunan kurumların karşı karşıya oldukları tehditleri anlayabilmeleri, gerekli tedbirleri belirleyerek uygulayabilmeleri, uygun önlemlerin alınıp alınmadığını kontrol edebilmeleri hedeflenmektedir. Rehber içerisinde yer alan gereksinimlerin nihai amacı, özellikle küçük ve orta ölçekli kurumların sahip oldukları veri merkezlerinin/sistem odalarının etkin, verimli ve güvenli bir biçimde çalışabilmelerinin sağlanmasıdır.

1.3 KAPSAM DIŞI

Veri merkezi rehberi içerisinde yer alan gereksinimler (örneğin bankacılık sektöründe kullanılan), yüksek güvenlikli veri merkezlerini korumak için yeterli değildir. Bu tür bir veri merkezi, yüksek performans, yüksek erişilebilirlik, afet toleransı, yedeklilik, enerji verimliliği gibi bir çok farklı unsur göz önünde bulundurularak tasarlanır ve rehbere konu veri merkezlerinden bu noktalarda ayrışır.

Ayrıca, bünyesinde sadece bir veya bir kaç sunucu barındıran BT birimlerinin "Sunucu Odası Rehberi" içerisinde yer alan gereksinimleri göz önünde bulundurmaları önerilir.

2 RİSK KAYNAKLARI

Aşağıdaki tehditler ve risk unsurları veri merkezleri için özel önem taşımaktadır:

2.1 YANLIŞ/EKSİK PLANLAMA

Temel ihtiyaçlar ve tehdit unsurları göz önünde bulundurulmaksızın kurulan ve işletilen veri merkezleri yüksek kesinti riskleri taşırlar. Örneğin; depremler, sel baskınları veya yanlış yapılandırılmış BT bileşenleri (hatta politik konular), operasyonel güvenliği ve BT sistemlerinin kullanılabilirliğini tehlikeye atabilir. Veri merkezinin dış dünya ile bağlantısının kurulması için gerekli mevcut bant genişliğinin gereksinimlere cevap verememesi veya veri merkezinin bulunduğu bölgede enerji kaynağının yetersiz olması gibi durumlar, bir veri merkezinin sağlıklı işletilebilmesini ciddi biçimde engelleyebilir.

2.2 YETKİSİZ ERİŞİM

Erişim kontrollerinin bulunmaması veya yetersiz olması, yetkisiz ve kötü niyetli kişilerin veri merkezine zarar verme riskini artırır ve onarılması güç hasarlara neden olabilir. Yetkisiz erişim, verilerin ve BT sistemlerinin erişilebilirliği, gizliliği ve bütünlüğü üzerinde oldukça önemli bir etkiye sahiptir. Kurum için kritik ve hassas veriler, BT bileşenlerinin yetkisiz erişimi nedeniyle çalınabilir veya zarar görebilir.

2.3 YETERSİZ İZLEME

Veri merkezinde bulunan BT bileşenlerinin ve altyapı ekipmanlarının yeterince izlenmemesi ve kontrol edilmemesi, önemli olabilecek sorunların zamanında tespit edilmemesine neden olabilir. Bu durum, veri merkezinin kullanılabilirliğini ve BT bileşenlerinin erişilebilirliğini ciddi şekilde etkileyebilir.

Genellikle veri merkezinde yaşanabilecek kesintilere ilişkin bulgular zaman içerisinde, yavaş yavaş ortaya çıkar. Aktif izleme olmaksızın bunları fark etmek oldukça zordur. Böyle bir durumda çoğu zaman önlem almak mümkün değildir.

2.4 VERİ MERKEZİ YETERSİZ İKLİMLENDİRME

Veri merkezi içerisinde çalışmakta olan BT bileşenleri tarafından harcanan enerji nedeniyle ısı açığa çıkar. Bu durum veri merkezi ortam sıcaklığının artmasına neden olur. BT bileşenlerinin etkin ve verimli bir biçimde çalışabilmesi için ortam sıcaklığının belirli bir aralıkta olması gereklidir. Ortamın istenilenden daha soğuk veya daha sıcak olması, gerekli iklim koşullarının sağlanamaması, BT bileşenlerinin arızalanmasına veya hasar görmesine neden olabilir.

Veri merkezi ve sistem odası rehberi içerisinde, bilinçli olarak teknik ayrıntılardan ve planlama parametreleri kullanımından kaçınılmıştır. Konu ile ilgili daha detaylı bilgi için ilgili standartlardan (örn. ANSI/BICSI 002-2014, DIN EN 50600) destek alınabilir.

2.5 YANGIN

Veri merkezinde yangın korumasının olmaması veya yetersiz olması durumunda, olası bir yangının yayılması engellenemeyebilir. Yangının hızla gelişip tüm veri merkezine yayılma riski ortaya çıkar. Veri merkezi içerisinde ateş ve duman son derece büyük hasarlara neden olabilir.

2.6 SU SIZINTILARI

Veri merkezinde; sel, borulardaki çatlaklar, hatalı yangın söndürme sistemleri, kanalizasyon hasarı veya klima arızaları nedeniyle su sızıntıları oluşabilir. Bu durum, BT sistemlerinin hasar görmesine ve çalışamamasına; olası bir kısa devre nedeniyle veri merkezi elektrik sisteminin kesintiye uğramasına ve hatta yangına neden olabilir.

2.7 EKSİK VEYA YETERSİZ HIRSIZLIK KORUMASI

Veri merkezi giriş/çıkışlarında ve çevresinde fiziksel güvenlik önlemlerinin yetersiz olması, yetkisiz kişilerin veri merkezine kolayca girmelerine neden olur. Kötü niyetli kişiler tarafından, veriler ve BT bileşenleri çalınabilir, değiştirilebilir ve hatta yok edilebilir. Ayrıca kurum içi gizli bilgilere erişilebilir veya direk olarak veri merkezine zarar verilebilir.

2.8 ELEKTRİK İLETİMİNİN ARIZALANMASI

Veri merkezi bünyesinde yedek/alternatif bir güç kaynağı olmaması durumunda, yaşanacak olası bir elektrik kesintisi veri merkezinde bulunan BT bileşenlerinin ve dolayısıyla kurumun çalışmasında önemli aksaklıklara neden olabilir. BT hizmetleri aniden ulaşılamaz hale gelebilir, kritik veriler kaybolabilir. Elektrik kesintisinin BT bileşenlerine ve altyapı ekipmanlarına zarar vermesi de mümkündür.

2.9 TEMİZLİK/KİRLENME

Veri merkezi içerisinde oluşan kir, toz, ve benzeri unsurlar, BT bileşenlerinin ve altyapı ekipmanlarının çalışmamasına neden olabilir. Kirlenme nedeniyle, altyapı ekipmanları daha sık arıza yaşayabilir ve BT bileşenlerinin yaşam ömrü azalır.

2.10YETERSİZ KABLO TAŞIMA KANALLARI

Veri merkezi içerisinde gerek enerji, gerekse veri iletimi kablolar aracılığı ile sağlanır. Enerji ve veri iletimi için kullanılan kablolar farklı kanallardan taşınmıyorsa ve kablo minimum bükülme çaplarına dikkat edilmiyorsa, enerji ve veri kalitesi düşebilir, veri merkezi içerisinde kesintiler oluşabilir. Eğer kablolar, yangın duvarlarından geçiyorsa, kablo geçirme deliklerinin enine kesitinin %60'ının kablolarla kaplanması, kalan % 40'ının ise yangın geçirmez harç veya yangın söndürme için onaylanmış bir başka malzeme ile doldurulması önerilir. Bu gereksinim gözetilmez ise, bitişik odadaki bir yangın veri merkezine sıçrayabilir, veri merkezi içerisinde kolaylıkla yayılabilir.

3 GEREKSİNİMLER

Veri merkezine ilişkin, karşılanılması beklenen gereksinimler bu başlıkta listelenmektedir. Prensipte kurum içerisinde yetkili BT Yöneticisi aşağıda yer alan gereksinimlerin karşılanılmasından sorumludur. Her bir gereksinim içerisinde, ilgili diğer sorumlu kişiler de tanımlanmıştır. Kurumların son zamanlarda bilgi güvenliği (ve özellikle ISO 27001) çalışmaları gerçekleştirmekte olduğu göz önünde bulundurularak, Bilgi Güvenliği Sorumlusunun stratejik kararlara dahil edilmesi sağlanabilir.

Rehber içerisinde gereksinimler, üç ana başlık içerisinde toplanmıştır. Kurumların öncelikli olarak "1. Seviye Gereksinimler" başlığı altında yer alan maddeleri değerlendirmeleri, sonra ihtiyaçları doğrultusunda "2. Seviye Gereksinimler" ve "3. Seviye Gereksinimler" başlıklarını ele almaları önerilmektedir.

Tablo 3. Veri Merkezi Rol Listesi

Varlık Sorumlusu/Sahibi	BT Yöneticisi
Diğer Sorumlular	Veri Koruma Görevlisi, Bina Hizmetleri, BT Operasyon Uzmanı, Bilgi Güvenliği Sorumlusu, çalışanlar, Planlama Sorumlusu, Bakım Personeli

3.1 1. SEVİYE GEREKSİNİMLER

Kurumlar öncelikli olarak aşağıda yer alan gereksinimleri göz önünde bulundurarak gerçekleştirecekleri faaliyetleri planlayabilirler.

VRM.2.G1 İhtiyaçların Tanımlanması [Planlama Sorumlusu, BT Operasyon Uzmanı, Bina Hizmetleri, Bilgi Güvenliği Sorumlusu]

Kurum bünyesinde veri merkezi ihtiyaçları tanımlanmış mı?

Hangi boyutta olursa olsun, bir veri merkezi için öncelikle ihtiyaçların belirlenmesi, teknik ve kurumsal gereksinimlerin tanımlanması gereklidir. Bu esnada veri merkezi içerisinde yer alacak BT bileşenlerine ilişkin ihtiyaç duyulan erişilebilirlik seviyeleri, olası çevresel tehlikeler, iç ve dış tehdit unsurları dikkate alınmalıdır.

Veri merkezi kapalı bir güvenlik bölgesi olarak tasarlanmalı, mümkünse veri merkezi içerisinde farklı güvenlik alanları oluşturulmalıdır. Bu amaçla; öncelikle idari, lojistik, teknik ve BT için ayrı alanlar ayrılmalıdır.

Kurum tarafından, tek bir oda (sistem odası) içerisinde BT bileşenlerinin barındırılması durumunda, farklı güvenlik bölgelerinin uygulanabilir olup olmadığı kontrol edilebilir.

Ayrıca, (örn. su veya gaz için) tedarik hatlarının veri merkezinin hemen yakınında bulunmamasına dikkat edilmeli, mevcut ikmal hatlarının, en azından kritik noktalarda düzenli olarak kontrol edilmesi sağlanmalıdır.

VRM.2.G2 Yangın bölgelerinin oluşturulması [Planlama Sorumlusu]

Veri merkezinde yangın bölgeleri oluşturulmuş mu?

Veri merkezi dışında oluşabilecek bir yangının veri merkezini etkilememesini, veri merkezi içerisinde oluşabilecek bir yangının dışarıya yansımamasını sağlamak ve yangının genişlemesini önlemek amacı ile yangın bölgeleri oluşturulmalıdır. Personel ve bina ile birlikte BT bileşenlerinin yangından korunması göz önünde bulundurulmalıdır. Yangın bölgeleri ile ısı ve duman yayılmasının önlenmesi de sağlanmalıdır.

Kurum tarafından, tek bir oda (sunucu odası) içerisinde BT bileşenlerinin barındırılması durumunda, uygun yangın bölmelerinin uygulanabilir olup olmadığı kontrol edilebilir.

VRM.2.G3 Kesintisiz güç kaynağı (UPS) kullanımı [Bina Hizmetleri]

Veri merkezinde kesintisiz güç kaynağı (UPS) kullanılıyor mu?

Veri merkezinde yer alan kritik BT bileşenlerinin elektrik kesintilerinden etkilenmemelerini sağlamak amacı ile kesintisiz güç kaynağı (UPS) sistemi kurulmalıdır. Altyapı ekipmanlarının (örn. klima sistemleri) güç gereksinimleri genellikle yüksek olduğundan,

öncelikli olarak sadece bu ekipmanları kontrol edecek BT bileşenlerinin UPS sistemine bağlanması sağlanmalıdır. Küçük ölçekli sunucu odalarında, BT bileşenlerine ilişkin erişilebilirlik gereksinimlerine bağlı olarak bir UPS sisteminin gerekli olup olmadığı değerlendirilebilir.

UPS sisteminin, şebeke elektriğinin kesilmesi durumunda, herhangi bir veri kaybı yaşanmaması için, bağlı tüm BT bileşenlerine gerekli enerjiyi sağlayabileceği biçimde boyutlandırılmış (yetiyor) olması gereklidir. UPS sistemi içinde kaç adet UPS'in kullanılacağı, bunların birbirlerine nasıl bağlanacağı, şebeke kesintisi durumunda yedek/alternatif enerjinin nasıl sağlanacağı önceden planlanmalıdır. UPS sisteminin doğru bir biçimde planlanması ve yapılandırılması, elektrik sistemi üzerinde gerçekleştirilecek bakım/onarım çalışmalarının veya değişikliklerin veri merkezini olumsuz bir biçimde etkilememesini sağlar.

Şebeke elektriğinin kesilmesi durumunda, UPS sistemi tarafından yedek/alternatif enerji kaynağı devreye girene kadar gerekli enerjiyi sağlamak amacı ile kullanılacak olan aküler, gerekli sıcaklık aralığında tutulmalı ve tercihen farklı, iklim kontrollü bir oda içerisinde barındırılmalıdır.

UPS sisteminin düzenli olarak bakımları yapılmalı ve sistem belirli aralıklar ile işlevsellik açısından test edilmelidir. Bu amaçla üretici tarafından önerilen bakım aralıklarına uyulmalıdır. (VRM.2.G10 Altyapı Denetimi ve Bakımı'na bkz.)

VRM.2.G4 Acil durumlarda elektrik iletiminin kapatılması [Bina Hizmetleri]

Veri merkezinde acil durumlarda elektrik iletiminin kapatılması için bir mekanizma bulunuyor mu?

Acil bir durumda, veri merkezinin elektrik bağlantısını hızlı bir biçimde kesebilmek için gerekli mekanizma oluşturulmalıdır. Örneğin bir acil durum durdurma (emergency power off – EPO) anahtarı kurulması düşünülebilir. Bu tarz bir mekanizma yardımı ile gerekli bir durumda harici elektrik kaynağının bağlantısının yanı sıra tüm UPS sisteminin kapatılması sağlanmalıdır. Veri merkezi içerisinde kullanılan tüm acil durum durdurma anahtarları, yanlışlıkla çalıştırılmaması için kilitli tutulmalı ve yetkisiz kullanıma karşı fiziksel olarak korunmalıdır.

VRM.2.G5 Hava sıcaklığı ve nem ile uyumluluk [Bina Hizmetleri]

Veri merkezinde uygun iklim koşulları sağlanıyor mu?

BT bileşenlerinin, istenilen performans ve erişilebilirlik ihtiyaçlarına uygun, güvenilir bir şekilde çalışabilmeleri için, üretici firmaların önerileri doğrultusunda, çalışma ortamında

uygun iklim koşullarının sağlanması (hava sıcaklığı ve nemin belirtilen sınırlar dahilinde tutulması) gerekmektedir.

Bu amaçla, veri merkezi içerisinde iklimlendirme sistemlerinden yararlanılarak uygun iklim koşulları oluşturulmalıdır. Veri merkezi içerisinde soğutulan alanlardaki gerçek ısı yükü, düzenli aralıklarla (veya veri merkezi içerisinde kapsamlı, büyük değişiklikler yapıldıktan sonra) kontrol edilmeli, ortam sıcaklığının ve nemin sürekli izlenmesi ve kayıt altına alınması sağlanmalıdır.

Ayrıca kullanılan iklimlendirme sisteminin bakımları düzenli olarak yapılmalıdır.

VRM.2.G6 Erişim kontrolleri [Bina Hizmetleri, BT Operasyon Uzmanı, Bilgi Güvenliği Sorumlusu]

Veri merkezinde yetkisiz erişime karşı bir erişim kontrol mekanizması kurulmuş mu?

Veri merkezini, yetkisiz erişime karşı koruyabilmek için bir erişim kontrol mekanizmasının kurulması gereklidir. Bir erişim yönetmeliği/prosedürü/politikası yardımı ile veri merkezine, sadece görev tanımları gereği o alanda çalışma gerçekleştirmesi gereken kişilerin erişebilmeleri sağlanmalıdır. Yetkili kişilerin (kurum içerisinden veya dışarısından), ne kadar bir süre boyunca, veri merkezi içerisinde hangi alanlara erişmeleri gerektiği belirlenmeli, kişilere gereksiz veya çok geniş erişim haklarının verilmesi engellenmelidir.

Veri merkezinde çalışma yapması gereken ziyaretçilerin ve harici personelin, gerçekten ihtiyaç duyulması halinde, bir yetkili kurum çalışanı nezaretinde veri merkezine giriş yapması, çalışmalarını gerçekleştirmesi; tüm girişlerin ve çıkışların ayrı ayrı kayıt altına alınması ve denetlenmesi sağlanmalıdır.

Ayrıca veri merkezine tüm girişler ve çıkışlar ve veri merkezi içerisinde gerçekleştirilen tüm faaliyetler izlenmelidir. Küçük ölçekli sunucu odaları için daha basit (sadece giriş/çıkış) bir izleme gerçekleştirilebilir.

VRM.2.G7 Kilitleme ve koruma [Çalışanlar, Bina Hizmetleri]

Veri merkezinde yer alan kapılar ve pencereler kilitli tutuluyor mu?

Veri merkezinde bulunan tüm kapılar daima kilitli tutulmalıdır. Planlama sırasında, mümkün olduğunca veri merkezinde pencerelerin bulunmasından kaçınılmalıdır. Pencerelerin bulunması durumunda, pencerelerin de kapılar gibi kilitli tutulması sağlanmalıdır. Kapılar ve pencereler için saldırı ve çevresel etkilere (örneğin, yangın ve duman) karşı yeterli koruma sağlayacak malzemeler kullanılmalıdır.

VRM.2.G8 Yangın alarm sisteminin kullanımı [Planlama sorumlusu]

Veri merkezinde bir yangın alarm sistemi bulunuyor mu?

Veri merkezinde bir yangın alarm sistemi bulunması gereklidir. Bu sistem aracılığıyla tüm veri merkezi izlenmeli, şüpheli bir durumda gerekli mesajlar üretilerek, uygun ekiplere iletilmelidir (Ayrıca VRM.2.G13 Alarm Sistemlerinin Planlanması ve Kurumu bkz.). Yangın alarm sisteminin bakımları belirli aralıklarla, üretici firma tarafından belirtilen biçimde gerçekleştirilmelidir. Ayrıca düzenli aralıklarla veri merkezi içerisinde yangına sebebiyet verecek materyallerin bulunup bulunmadığı kontrol edilmelidir.

VRM.2.G9 Yangın önleme veya yangın söndürme sistemi kullanımı [Planlama sorumlusu]

Veri merkezinde bir yangın önleme/söndürme sistemi yer alıyor mu?

Veri merkezinde güncel yöntemler ve teknoloji kullanılarak bir yangın önleme ve söndürme sistemi kurulması gerekir.

Sınırlı sayıda BT bileşenin bulunduğu sistem odalarında yeterli sayıda ve boyutta yangın söndürücülerin kullanılması yeterli olabilir. Yangın durumunda yangın söndürücülerin kolayca erişilebilir bir yerde tutulması gerekmektedir. Her yangın söndürücü, acil bir durumda tam olarak çalışmayı güvence altına alabilmek amacı ile düzenli olarak kontrol edilmelidir. Başta veri merkezinde görev alacak çalışanlar olmak üzere, ilgili herkese yangın söndürücülerin kullanımı konusunda eğitimler verilebilir, bu konuda talimatlar hazırlanabilir.

VRM.2.G10 Altyapı kontrol ve bakım çalışmaları [Bina Hizmetleri, BT Operasyon Uzmanı, Bakım Personeli]

Veri merkezi altyapı ekipmanları gözden geçiriliyor mu?

Veri merkezi altyapı ekipmanları üzerinde, üretici firma tarafından tavsiye edilen bir biçimde, düzenli aralıklar ile bakım faaliyetleri gerçekleştirilmelidir. Veri merkezi içerisinde bulunan yangın duvarları, kablo ve boru girişleri, bölmelerin uyumlu ve sağlam olduğundan emin olmak için düzenli olarak kontrol edilmelidir. Gerçekleştirilen çalışmalar, zaman, kişi, görev, vb. bilgiler ile denetim ve bakım günlükleri içerisinde kayıt altına alınmalıdır.

VRM.2.G11 Altyapı ortam izleme [Bina Hizmetleri, BT Operasyon Uzmanı]

Veri merkezinde altyapı ekipmanları izleniyor mu?

Altyapı ekipmanları (ve bu ekipmanları yönetmek için kullanılan sistemler) tarafından üretilen tüm arıza mesajları kayıt altına alınmalı, ilgili kişilere iletilmelidir. Özellikle iklimlendirme, elektrik ve UPS sistemleri (bir izleme sistemi vasıtasıyla) otomatik olarak

izlenmeli ve gerekli durumlarda ilgili ekiplerin mümkün olduğunca çabuk faaliyete geçmesi sağlanmalıdır.

Küçük ölçekli sistem odası içerisinde yer alan, genellikle az sayıda kişi tarafından işletilen BT ve destek ekipmanlarının uzaktan izlenmeleri, gerekli durumlarda sorumlu çalışanların vakitli olarak uyarılması önerilir.

3.2 2. SEVİYE GEREKSİNİMLER

Temel gereksinimler sonrasında, veri merkezlerinin durumunu daha iyi bir seviyeye getirmeyi düşünen kurumlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini planlayabilirler.

VRM.2.G12 Veri merkezi için çevre koruma tasarımı ve uygulanması [Planlama sorumlusu, Bina Hizmetleri]

Olası dış tehditler için veri merkezi çevresinde gerekli önlemler alınmış mı?

Veri merkezinin içerisinde bulunduğu bina/yerleşke güvenliği ile birlikte, çevrenin korunması için gerekli önlemlerin alınması önerilir. Veri merkezinin yer aldığı bölge, koruma gereksinimleri ve çevresel etkenler (veri merkezinin şehir merkezine, karakola, hastaneye, vb. yakınlığı gibi) göz önünde bulundurularak, çevre koruma önlemleri oluşturulabilir. Çevre koruma önlemleri arasında:

- Bina/yerleşke dış muhafazası,
- Bina/yerleşke sınırının kasıtsız olarak geçilmesine karşı ihtiyati tedbirler,
- Bina/yerleşke sınırının kasıtlı aşılmasına karşı güvenceler,
- Bina/yerleşke sınırının kasıtlı olarak şiddet yoluyla aşılmasına karşı alınacak tedbirler
- Açık hava güvenliği (dış güvenlik) önlemleri,
- Bina/yerleşke giriş/çıkış kontrolü,
- Harici yolcu ve araç tanımlaması yer alır.

VRM.2.G13 Alarm sistemlerinin planlanması ve kurulumu [Planlama sorumlusu]

Veri merkezinde alarm sistemleri kullanılıyor mu?

Bina/yerleşke ve veri merkezi için tasarlanmış güvenlik konseptine uygun alarm sistemleri kullanılması gerekir. Bu amaçla kullanılacak alarm sisteminin türü belirlenmeli, alarm sisteminin kullanılacağı alanlar planlanmalı, alarm sistemleri kurulmalı ve oluşan alarm mesajlarının ne şekilde yönetileceği kurgulanımalıdır. Bina/yerleşke alanı ve/veya veri merkezi üzerinde gerçekleştirilen değişiklikler sonrası, alarm sistemi üzerinde gerekli uyarlamalar gerçekleştirilmelidir.

Kurulan alarm sistemi tarafından üretilen mesajların, bir merkezi operasyon birimine (alarm alma istasyonu) aktarılması önerilmektedir. Merkezi operasyon biriminin her zaman erişilebilir olması, bildirilen mesajlara teknik olarak uygun yanıt vermesi ve gerekirse çözüm üretebilmesi sağlanmalıdır. Alarm sistemi tarafından üretilen mesajların, merkezi operasyon birimine aktarılması için kullanılan iletim yolunun (ağ bağlantısı) yedekli tasarlanması ve düzenli olarak test edilmesi önerilir.

VRM.2.G14 Jeneratör kullanımı [Planlama sorumlusu, Bina Hizmetleri]

Veri merkezinde jeneratör bulunuyor mu?

Veri merkezi bünyesinde yedek/alternatif bir enerji kaynağı olarak jeneratör kullanılması önerilmektedir. Veri merkezinde yer alan BT bileşenlerinin ve altyapı ekipmanlarının enerji kullanımlarına göre gerekli jeneratör kapasitesi planlanmalıdır. Jeneratör düzenli olarak kontrol edilmeli, üretici firma tarafından önerilen biçimde bakımları gerçekleştirilmelidir (VRM.2.G10 Altyapının denetimi ve bakımı'na bkz.). Bakımlar sırasında, yük ve fonksiyon testleri gerçekleştirilerek jeneratörün gerektiğinde istenilen şekilde çalışması güvence altına alınmalıdır.

VRM.2.G15 Aşırı gerilimden korunma sistemleri [Planlama sorumlusu, Bina Hizmetleri]

Veri merkezinde aşırı gerilim koruma cihazlarından yararlanılıyor mu?

Standartlara uygun cihazlar seçilerek, veri merkezine uygun bir yıldırım ve aşırı gerilim korunma yaklaşımının oluşturulması ve uygulanması önerilmektedir.

Yıldırım ve aşırı gerilim korunma sistemi, belirli aralıklar ile kontrol edilmeli ve gerekirse değiştirilmelidir. Cihazları etkileyebilecek olaylar sonrası kontrol tekrarlanmalıdır.

Veri merkezi içerisinde yer alan cihazlar için farklı topraklama sistemlerinin kullanılması, elektriksel potansiyel farkının oluşmasına neden olabilmektedir. Bu çok istenmeyen bir durumdur. Bu durumu engellemek amacı ile veri merkezi içerisinde tüm cihazların topraklanması için kullanılabilecek bir sinyal referans şebekesi - SRG (Signal Reference Grid) - oluşturulması önerilir.

VRM.2.G16 Veri merkezi iklimlendirme [Bina Hizmetleri]

Veri merkezinde uygun iklim koşullarının sağlanması için iklimlendirme sistemleri kullanılıyor mu?

Veri merkezinde hava sıcaklığı ve nem için uygun iklim koşullarının sağlanması (VRM.2.G5 Hava sıcaklığı ve nemi ile uyumluluğuna bkz.), temiz havanın korunması ve muhafaza edilmesi gerekmektedir. Veri merkezi planlaması aşamasında, iklimlendirme

gereksinimleri belirlenerek, iklimlendirme sisteminin veri merkezine uygun biçimde boyutlandırılması sağlanmalıdır. Gerek hava sıcaklığı, gerekse nem ve iklimlendirme ile ilgili tüm değerler sürekli izlenmeli, belirlenen standart değerlerden sapmalar olması durumunda, alarm sistemleri aracılığı ile otomatik uyarı mesajları üretilerek ilgili ekiplere gerekli bildirimler gerçekleştirilmelidir.

Veri merkezinde genellikle ayrı bir odada bulunan iklimlendirme sistemlerinin, sunucu odasında en azından yetkisiz kişilerin müdahele edemeyecekleri, güvenli bir biçimde konumlandırılmaları gerekir.

VRM.2.G17 Erken yangın algılama [Planlama sorumlusu, Bina Hizmetleri]

Veri merkezinde yangın algılama sistemi bulunuyor mu?

Veri merkezlerindeki yangınları çok erken bir aşamada saptamak için hassas alıcılar kullanılarak oluşturulan erken yangın algılama sistemi kurulması önerilmektedir. Yangının olabildiğince erken bir biçimde algılanmasını ve gerekli faaliyetlerin başlatılmasını sağlayacak bu tür sistemler sayesinde yangının yayılmasını önlemek, otomatik olarak enerjiyi devre dışı bırakmak mümkün hale gelir.

Erken yangın algılama sistemi, veri merkezi içerisinde farklı izleme alanlarını (veya BT bileşenlerini) izleyebilecek biçimde kurgulanmalıdır. Yangın durumunda hangi alanların (veya BT bileşenlerinin) etkilendiği hızlı biçimde belirlenerek, daha etkin ve verimli bir yangın koruması sağlanması hedeflenir.

Veri merkezinde kullanılacak erken yangın algılama sisteminin, güncel teknolojiye uygun olması gerekir. Erken yangın alarm sistemi üretici firmanın önerilerine uygun bir biçimde çalıştırılmalı ve düzenli olarak bakımdan geçirilmelidir.

VRM.2.G18 Su sızıntısına karşı koruma [Bina Hizmetleri]

Veri merkezini su sızıntısına karşı korumak için gerekli önlemler alınmış mı?

BT bileşenlerinin bulunduğu alanlarda, mümkün oldukça su taşıyan borulardan kaçınılmalıdır. Örnek olarak, veri merkezlerinde radyatör yer almamalıdır.

Bazı veri merkezlerinde (örneğin iklimlendirme sistemlerinde veri merkezinin soğutulması için) su (veya benzeri sıvılar) kullanımına rastlanmaktadır. Su taşıyıcı hatların engellenemediği bu gibi durumlarda, uygun algılayıcılar kullanılarak su sızıntılarının olabildiğince erken tespit edilmesi ve etkilerin en aza indirgenmesi gerekir. Algılama sistemi tarafından üretilen mesajlar yetkili çalışanlara bildirilmeli, hızlı bir şekilde müdahale edilmesi sağlanmalıdır (VRM.2.G13 Alarm sistemlerinin planlanması ve montajı'na bkz.).

Belirli aralıklar ile yetkili çalışanların, var olan su borularını görsel olarak kontrol ederek, olası sorunları erken evrelerde tespit etmeleri önerilmektedir.

VRM.2.G19 Teknik altyapı fonksiyonel testler [Bina Hizmetleri]

Veri merkezinde kullanılan altyapı ekipmanları test ediliyor mu?

Veri merkezinde kullanılan teknik altyapı ekipmanlarının (özellikle herhangi bir arıza durumunda yedek ekipmanların düzgün çalışıp çalışmadığının belirlenmesi amacı ile) düzenli olarak test edilmesi gereklidir. Test sonuçları değerlendirilerek gerekli ekipman ve yapılandırma değişiklikleri gerçekleştirilmeli, onarımlar yapılmalıdır. Gerçekleştirilen tüm testler ve test sonuçları kayıt altına alınmalıdır. Özellikle gerçek hayatta ortaya çıkabilecek durumlar göz önünde bulundurularak gerekli testlerin hazırlanması ve testlerin yılda en az bir kez gerçekleştirilmesi önerilir.

VRM.2.G20 Altyapı ve inşaat planlarının düzenli güncellemeleri [Planlama Sorumlusu]

Veri merkezinde gerekli durumlarda altyapı ve inşaat planları güncelleniyor mu?

Veri merkezinin içerisinde bulunduğu bina/yerleşke inşaat planları, yerleşim planları, veri merkezi altyapı planları, yangın çıkış güzergah planları, elektrik devre şemaları, itfaiye yolları vb. planlar ve dökümanlar her değişiklik ve/veya yeni kurulum sonrası güncellenmelidir. Konu ile ilgili çalışanlar güncellemeler ile ilgili olarak bilgilendirilmeli, herhangi bir yenilik, değişiklik olmaması durumunda dahi tüm ilgili planların güncelliği ve doğruluğu belirli aralıklar ile kontrol edilmelidir.

3.3 3. SEVİYE GEREKSİNİMLER

Temel ve standart gereksinimler sonrasında, veri merkezlerinde artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda, risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilir. Parantez içinde bulunan harfler ile gereksinim tarafından öncelikli koruma sağlanan prensip belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.2.G21 Felaket Kurtarma Merkezi (E)

Kurum tarafından kullanılmakta olan bir Felaket Kurtarma Merkezi bulunuyor mu?

Herhangi bir felaket durumunda BT hizmetlerinin devamlılığını sağlamak isteyen kurumların, mevcut veri merkezinden coğrafi olarak ayrılmış bir felaket kurtarma merkezi (FKM) kurması ve kullanması önerilir. FKM, kurum için kritik iş süreçlerini destekleyecek BT hizmetlerinin felaket durumunda çalışabilmesini sağlayacak biçimde

boyutlandırılmalıdır. Gerektiğinde kullanıma hazır olmasını sağlamak amacı ile gerekli planlar hazırlanmalı, kurum tarafından kritik tüm verilerin düzenli olarak FKM'ye aktarılması sağlanmalıdır.

VRM.2.G22 Veri merkezi operasyonu sırasında inşaat projeleri (B)

İnşaat projelerinde gerekli önlemler alınıyor mu?

Ekonomik nedenlerden ötürü, genellikle veri merkezini/sistem odasını yeniden inşa etmek yerine, bitişik alanları birleştirerek mevcut veri merkezinin/sistem odasının genişletilmesi tercih edilir. Bu durum ciddi miktarda iş yükünü beraberinde getirir.

Kurum işleyişinin aksamaması için, inşaat çalışmaları sırasında, mevcut BT bileşenlerinin çalışmaya devam etmesi gereklidir. Aynı zamanda devam etmekte olan BT operasyonu, inşaat işlerini mümkün olduğunca kısıtlamamalı veya proje maliyetlerini gerekli seviyenin üzerine çıkaracak gereksinimler sunmamalıdır.

Güç kaynağı, iklimlendirme sistemleri, izleme ve alarm teknolojisi gibi veri merkezinin destekleyen altyapı unusurlarının, inşaat çalışmalarından etkilenmemeleri ve işlevselliklerini sürdürebilmeleri için gerekli planlamalar ve hazırlıklar gerçekleştirilmelidir. Ayrıca BT bileşenlerinin barındırıldığı alan toza, kire ve yetkisiz erişime karşı korunmalıdır. Aynı zamanda inşaat sahasına gereksiz yere giriş/çıkış engellenmemelidir.

VRM.2.G23 Güvenli veri merkezi kabloları [Bina Hizmetleri] (E)

Veri merkezi içerisinde kablo kanalları kullanılıyor mu?

Sistem odaları ve veri merkezlerinde, TS EN 50173-1 "Bilgi teknolojisi - Jenerik kablolama sistemleri - Bölüm 1: Genel kurallar" standardı içerisinde tanımlanmış, kablolama sistemlerine ilişkin temel ilkeler takip edilmelidir. Veri merkezi içerisinde kablo taşımak için kullanılacak kanallar dikkatle planlanmalı ve hazırlanmalıdır. Tüm kablolar, kazayla oluşabilecek hatalara, yetkisiz kişilerin neden olabileceği sorunlara ve yangınlara karşı korunmalıdır.

VRM.2.G24 Video gözetim sistemlerinin kullanımı [Plan sorumlusu, Bina Hizmetleri, veri koruma sorumlusu] (BE)

Veri merkezinde video gözetim sistemleri kullanılıyor mu?

Veri merkezini, yetkisiz erişime karşı koruyabilmek için kullanılan erişim kontrol mekanizmasının video gözetim sistemleri ile desteklenmesi gereklidir. Bu amaçla öncelikle sürekli olarak izlenmesi gereken alanlar belirlenmeli, bu alanları eksiksiz bir biçimde takip edecek şekilde kamera sistemi seçilmelidir.

Video gözetim sistemi için merkezi bir ortam/oda belirlenmeli, merkezde yer alacak teknoloji bileşenleri kurulmalıdır. Kameralar tarafından alınan görüntülerin bu merkezde kayıt altına alınması, bir görevli tarafından izlenmesi sağlanmalı, belirli aralıklarla video gözetim sisteminin düzgün bir şekilde çalışıp çalışmadığı kontrol edilmelidir.

VRM.2.G25 Kesintisiz güç kaynaklarının (UPS) yedekli tasarımı [Plan sorumlusu]

Veri merkezinde kesintisiz güç kaynaklarının (UPS) yedekliliği düşünülmüş mü?

Veri merkezinin erişilebilirliğini daha üst seviyelere çıkarabilmek için, UPS sistemlerinin yedekli olması gerekmektedir. Veri merkezine enerji sağlayan elektrik şebekesinde yaşanabilecek olası bir kesinti durumunda, alternatif güç kaynağı devreye girene kadar, veri merkezinin sorunsuz bir biçimde çalışabilmesi için gerekli olan tüm bileşenlere enerji UPS sistemleri tarafından sağlanır. Özellikle en ufak kesintiye tahammülü olmayan kurumlarda UPS sisteminin yedekli bir biçimde tasarımın gerçekleştirilmesi önerilmektedir.

UPS sisteminin düzenli olarak bakımları yapılmalı ve sistemin belirli aralıklar ile işlevsellik açısından test edilmesi sağlanmalıdır. Bu amaçla üretici tarafından önerilen bakım aralıklarına uyulması tavsiye edilmektedir. (VRM.2.G10 Altyapı kontrol ve bakım çalışmalarına bkz.)

VRM.2.G26 ′Yedekli jeneratör (E)

′Veri merkezinde jeneratör yedekliliği düşünülmüş mü?

Yüksek koruma gereksinimleri kapsamında, alternatif güç kaynağı olarak kullanılacak sistemlerin yedekli tasarlanması önerilmektedir. Yedekli jeneratör sisteminin düzenli olarak bakımları yapılmalı ve sistemin belirli aralıklar ile işlevsellik açısından test edilmesi sağlanmalıdır. Bu amaçla üretici tarafından önerilen bakım aralıklarına uyulması tavsiye edilmektedir. (VRM.2.G10 Altyapı kontrol ve bakım çalışmalarına bkz.)

VRM.2.G27 Felaket kurtarma ve yangın tatbikatları (GE)

Veri merkezinde felaket kurtarma ve yangın tatbikatları gerçekleştiriliyor mu?

Kurum çalışanlarının katılımıyla, belirli aralıklarla felaket kurtarma ve yangın tatbikatlarının gerçekleştirilmesi önerilmektedir. Bu tatbikatlar, alınacak önlemlerin yazılı hale getirildiği bir plana (felaket kurtarma planı, yangın önleme planı vb.) dayanmalıdır. Tatbikat sırasında yazılı plana uygun bir biçimde yetkili ekiplerin görevleri yerine getirmesi sağlanmalı, planda yer alan tedbirlerin doğru, güncel ve pratik olup olmadığı kontrol edilmelidir.

VRM.2.G28 Teknik altyapıda yedeklilik, modülerlik ve ölçeklenebilirlik (BA)

Veri merkezinin seviyesi ne olarak konumlandırılmaktadır?

BT bileşenlerinin erişilebilirliğini sağlamak için en iyi yöntem, yedekliliktir. Bu, belirli bir görevi gerçekleştirmek için aslında gerekli olandan daha fazlasına sahip olmak demektir (Latince'den: "redundare", taşma, fazla olma). Bilgi Teknolojileri endüstrisinde yedeklilik, bir teknik sistemin işlevsel olarak eşdeğer kaynaklarının varlığı anlamına gelir. Bu nedenle yedeklilik ile ilgili asıl soru: “Yedekliğe sahip olmak için ihtiyaçtan fazla kapasiteler oluşturmak gerekli midir?” sorusudur.

Modülerlik ise istenilen hizmetin bir veya daha fazla modül tarafından sağlanıp sağlanamadığını açıklar. Başarılı şekilde oluşturulan modül tasarımları sayesinde, gereken yedeklilikler ortadan kalkabilir. Değişen teknik gereksinimlere karşın en iyi planlanan modeller bile bir süre sonra yeniden ölçeklendirilmeye (boyutlandırılma) muhtaç kalabilir.

4 DETAYLI BİLGİ İÇİN KAYNAKLAR

- TIA-942-A: Veri Merkezleri İçin Telekomunikasyon Altyapı Standartı
- ANSI/BICSI 002-2014: Veri Merkezi Tasarım ve Uygulama En İyi Pratikleri
- Enterprise Data Center Design and Methodology, Rob Snevely
- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri
- Bilgi Teknolojileri güvenliği enstitüsü (BSI) Almanya, IT Grundschutz Rechenzentrum
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_2_Rechenzentrum_sowie_Serverraum.html

VRM.3.G: ELEKTRİK KABLOLAMA

1 AÇIKLAMA

1.1 TANIM

BT sistemlerinin ve diğer cihazların elektrik kablolaması, elektrik dağıtım sistemi operatörünün binaya giriş noktasından son kullanıcı kablo bağlantılarına kadar olan tüm kablolamayı içerir.

Düzgün ve standarda uyumlu elektrik kabloları, BT erişilebilirliğini ve bütünlüğünü sağlamak için temel teşkil eder.

1.2 HEDEF

Bu modülün amacı, tüm elektrik kablolarının arıza ve elektrik kesintilerine karşı korunmasıdır.

1.3 KAPSAM DIŞI

Bilişim sistemlerinin iletişimi için gerekli BT kablolama, ayrı bir modülde ele alınmaktadır (bkz. VRM.4 BT Kablolama).

2 RİSK KAYNAKLARI

Aşağıdaki riskler ve eksiklikler elektrik kablolamanın güvenliği açısından özellikle önemlidir:

2.1 KABLOLARIN YANGIN YÜKÜ

Kablo üreticileri elektrik kablolarının imalatında plastik içerikli kılıflar veya izolasyon malzemeleri kullanmaktadırlar. Bunlar içinde;

- PVC polvinyl chloride,
- PE Polyethylene,
- PP Polypropylene,
- Sentetik lastik,

en çok kullanılanlarıdır.

Tüm bu plastikler yanabilir malzemelerdir. Dolayısı ile elektrik nedenli çıkan bir yangının (kısa devre, aşırı yük gibi) ortaya çıkan alevler bu kablolar üzerinde çok hızlı bir şekilde yürür ve yayılır. Yatay olarak serilen PVC kablo demeti üzerinde yangının ilerleme hızı 20 m/dk'dır. PE ve PP malzemeleri içeren kablolar çok daha kolay yanabildikleri gibi ayrıca eriyen damlaların oluşturduğu sıcaklık ile diğer komşu malzemeleri de kolayca yakabilirler.

Kablo yangınları genellikle gelişme aşamasında, sıcaklıkta hafif bir artışa neden olur. Böylece, tavandaki duman dedektörleri algılamadan önce önemli miktarda duman oluşması gibi ek bir risk söz konusudur.

2.2 ELEKTRİK KABLOLAMANIN EKSİK ÖLÇEKLENDİRİLMESİ

İşyerleri, sistem odaları veya veri merkezleri genellikle mevcut ihtiyaçlar dikkate alınarak planlanır. Eksik planlamadan dolayı zamanla hatalar ortaya çıkar. Mevcut elektrik kapasitenin genişleyeceği (ek sunucu/depolama cihazlarının bağlanması vb.) göz ardı edilmektedir. Bununla birlikte, elektrik kablolamanın boyutlandırılması ancak mevcut kablolama altyapısı veya alanların izin verdiği sürece mümkündür. Planlama sonrası mecburi değişiklikler, normalden daha masraflı olarak ortaya çıkmaktadır.

2.3 KABLOLAMANIN YETERSİZ DOKÜMANTASYONU

Kablolama dokümantasyonundaki bilgi eksikliği (tesisat konumları, ölçekler vb.), bir bina dışında veya içerisinde yapılan inşaat çalışmaları sırasında tesisatlara zarar verebilir. Bütün kablolama altyapısının geçerli standartlara göre döşendiği ise varsayılamaz. Belgelemenin yetersiz olması, tesisatlardaki test, bakım ve onarım çalışmalarını zorlaştırır.

2.4 YETERSİZ KORUNAN ELEKTRİK PANOLARI

Elektrik şebekesi ana/tali dağıtım panoları genellikle koridorlarda veya merdivenlerde, erişilebilir ve kilidi açılabilir halde tutulabilmektedir. Bu durum herkesin panolara erişmesine, manipüle etmesine veya elektrik kesintilerine neden olabilir. Ayrıca pano sigorta ve prizlerinin sökülmesi sonrası, yüksek akımlara maruz kalınması gibi ciddi tehlikeler ile karşı karşıya kalınabilir.

2.5 KABLO HATTI HASARLARI

Kablolar ne kadar korumasız bırakılırsa, bu durum hasar riskini o oranda artırır. Hasarın elektrik kesintilerine sebebiyet vermesinin yanında, kablo izolasyonunun ve kılıflarının aşınması veya yırtılması gibi durumlar, istenmeyen etkileşimlerin (aşınan kablonun, su veya oradan geçen insanlarla teması gibi) ortaya çıkmasına neden olur.

2.6 GERİLİM DALGALANMALARI / YÜKSEK GERİLİM VEYA DÜŞÜK GERİLİM

Elektrik iletimi geriliminde ki dalgalanmalar, arızalara ve bilişim sistemlerine zarar verebilir. Bunlar, düşük etkili veya BT'ye etkisi olmayan dalgalanmalardan, son derece yıkıcı ve zarar etkisi yüksek dalgalanmalara kadar uzanır. Bunun nedeni cihazların bağlı olduğu hatlardan, elektrik şebekesi santrallerine kadar uzanan hatlar da olabilir.

2.7 YETERSİZ GRUP PRİZLERİ

Çalıştırılacak cihazlar için, sabit priz sayısı çoğu zaman yeterli değildir. Bu eksikliği telafi etmek için genellikle taşınabilir grup prizleri kullanılır. Yetersiz kalitede elektrik prizleri, tehlikeli bir yangın kaynağı ve dolayısıyla yangın tehlikesi oluşturur. Ek olarak grup prizleri arka arkaya seri halde takılmış ise, bu aşırı yüklenme riskine sebebiyet verir.

3 GEREKSİNİMLER

Elektrik kablolamaya ilişkin, karşılanması beklenen gereksinimler bu başlıkta açıklanmaktadır. Kurumdan kuruma değişiklik göstermekle birlikte, genel olarak bina gereksinimlerinin karşılanmasından bina/kampüs hizmetleri yöneticisi sorumludur. Her bir gereksinim içerisinde, ilgili diğer sorumlu kişiler de tanımlanmıştır. Kurumların son zamanlarda bilgi güvenliği (ve özellikle ISO 27001) çalışmaları gerçekleştirmekte olduğu göz önünde bulundurularak, bilgi güvenliği görevlisinin stratejik kararlara dahil edilmesi de sağlanabilir. Bilgi güvenliği görevlisi ayrıca, gereksinim maddelerinin uygulanması sırasında kurum için oluşturulan güvenlik politikalarına uyumluluğun sağlanmasından sorumludur.

Rehber içerisinde gereksinimler, üç ana başlık içerisinde toplanmıştır. Kurumların öncelikli olarak “1.Seviye Gereksinimler” başlığı altında yer alan maddeleri zorunlu olarak değerlendirmeleri, sonra ihtiyaçları doğrultusunda “2.Seviye Gereksinimler” ve “3.Seviye Gereksinimler” başlıklarını ele almaları önerilmektedir.

Tablo 4. Elektrik Kablolama Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	Bina hizmetleri yöneticisi
Diğer Sorumlular	BT yöneticisi

3.1 1.SEVİYE GEREKSİNİMLER

Kurumlar ve organizasyonlar aşağıda yer alan gereksinimleri öncelikli olarak göz önüne alarak uygulamalıdırlar.

VRM.3.G1 Uygun kablo tiplerinin seçimi

Kablo seçilirken, iletim gereksinimleri yanında ortam koşulları da irdelendi mi?

Kablo seçiminde, teknik gereksinimlerin yanında kablo çekimi sırasındaki ortam koşulları ve işletilmesine de önem verilmelidir. Elektrik kablolarını seçerken, ilgili standartlara ve düzenlemelere uyulmalıdır. Çevresel koşullarla ilgili olarak, sıcaklık, kablo güzergâhı, gerilim kuvveti, tesisat çeşitleri ve arıza kaynakları gibi unsurlar dikkate alınmalıdır.

VRM.3.G2 Kablo yönetimi

Kablo taşıma kanalları, olası genişletme veya minimum mesafeler bakımından yeterince boyutlandırılmış mı?

Kablolar, kablo güzergahları ve kablo taşıma kanalları, kurulmadan önce işlevsel ve fiziksel açıdan yeterince boyutlandırılmış olmalıdır. Bu süreçte, gelecekteki elektrik ihtiyaçlarının yanı sıra kablo kanalı ve yollarında olası teknik genişlemeler için de yeterli alan dikkate alınmalıdır. BT ve elektrik kabloları ortak kablo taşıma kanalında yönlendiriliyorsa, kablo türlerinin karışmaması için özen gösterilmelidir. Genel olarak, BT kablolarının elektrik kablolarından ayrı tutulması önerilmektedir. Saptanabilir tehlikelerden kaçınmaya özen gösterilmelidir.

VRM.3.G3 Profesyonel kurulum

Elektrik kablolaması, geçerli standartlara ve üreticinin özelliklerine uygun bir şekilde kuruldu mu?

Elektrik kablolama kurulum çalışmaları dikkatli ve ustalıkla yapılmalıdır. Aynı zamanda, ilgili tüm standartlara uyulmalıdır. Elektrik kablolamanın profesyonel şekilde uygulanma kriterleri, işveren tarafından her aşamada kontrol edilmelidir. Elektrik kabloları ve kablo taşıma sistemleri döşenirken, kurulumun herhangi bir hasara neden olmadığına ve binanın normal kullanımını etkilemeyecek şekilde olduğuna dikkat edilmelidir. Ek olarak, BT-Kabloları ve elektrik kabloları ayrı yönlendirilmelidir.

3.2 2.SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, binaların durumlarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

VRM.3.G4 Elektrik kablolama ihtiyaç analizi

Erişilebilirlik, bütünlük ve gizlilik sorunlarını ele alan bir BT kablolama ihtiyaç analizi uygulanıyor mu?

Kapsamlı kablolama çalışmaları öncesinde, geleceğe yönelik, ihtiyaçlara dayalı ve uygun maliyetli elektrik kablolama gereksinimlerinin oluşturulması önerilir. Bir gereksinim analizinde öncelikle kurum kullanıcılarının kısa vadede ne kadar elektrik tüketebileceği ve bu kullanımın daha uzun vadede nasıl gelişebileceği tahmin edilmelidir.

VRM.3.G5 Elektrik kablolamanın iş kabulü

İş kabul belgeleri, giderilen eksiklikler, kalan işler, garanti süreleri için son tarihler hakkında bilgileri içeriyor mu?

Elektrik kablolama onay sürecine/iş kabulüne tabi tutulması önerilir. Kabul, çalışmanın tüm görevleri tamamlanmış, yüklenici kabul aşamasına gelindiğini bildirmiş ve de işveren tarafından yapılan kontrollerde kabul edilemez eksiklikler bulunmadığında verilmelidir. Kontroller için yeterli süre bırakılan bir kabul tarihi seçilmelidir. Ayrıca farklı standartlara uyum iş kabul aşamasında değerlendirilmelidir.

Kabul protokolü için bir kontrol listesi hazırlanmalıdır. Kontrol listesi, işletme alanları için genel gereksinimleri de içermelidir. Kabul protokolü, katılımcılar ve sorumlu kişiler tarafından yasal olarak bağlayıcı bir şekilde imzalanmalıdır. Protokol, kablolama dokümanlarının bir parçası olmalıdır.

VRM.3.G6 Aşırı gerilimden korunma

Kurum veya organizasyonda, aşırı gerilim koruma konsepti oluşturuldu mu?

Elektrik hatları yüksek voltaja karşı korunmalıdır. Bunun için geçerli standartlara uygun aşırı gerilim koruma konsepti oluşturulmalıdır. Jeneratör ve kesintisiz güç kaynakları tasarıma dahil edilmelidir.

VRM.3.G7 Gereksiz kabloların çıkarılması ve devre dışı bırakılması

Yangın yüklerini önlemek için gerekli olmayan kablolar kaldırılıyor mu, belgelere ekleniyor mu?

İşlevini yitiren elektrik kabloları ve hatları tamamen kaldırılmalıdır. Kablolar sökülürken ve çıkarıldıktan sonra yangın bariyerlerinin düzgün kapatılmış olduğundan emin olunması gerekir. Mevcut teknoloji ile rezerv olarak kullanılabilecek kablolar, uygun bir ortamda muhafaza edilebilir. Bu tür kabloların en azından uç noktalarından etiketlenmesi önerilir. İşletme belgelerinde, tüm değişiklikler denetlenebilir bir şekilde belgelendirilmelidir.

VRM.3.G8 Kablo taşıma sistemlerinin yangından korunması

Yangından korunma gereksinimleri ve yönetmelikleri, elektrik kablolama kurulumları sırasında yerine getiriliyor mu?

Kablo yangınlarından kaçınmak için, kablo taşıma kanal mesafeleri yeterince boyutlandırılmış olmalıdır. Ek olarak, montaj çalışmalarının tamamlanmasından sonra kablo sıkılığı (boşluk ve aralıklar) makul aralıklarla kontrol edilmelidir.

VRM.3.G9 Elektrik kablolamanın dokümantasyonu ve etiketlenmesi

Elektrik kablolamanın etiketleme ve dokümantasyonu ile ilgili düzenlemeler mevcut mu?

Kurumun elektrik kablolama kapsamında, iç ve dış dokümantasyona sahip olmalıdır. İç dokümantasyon, kablolarının kurulumu ve işletilmesi ile ilgili tüm kayıtları (mevcut ve

ilerdeki genişleme planlarını) içermelidir. Kablolamanın harici belgelendirmesi ise olabildiğince tarafsız tutulmalıdır.

VRM.3.G10 Elektrik tesisatlarının ve bağlantılarının kontrolü

Elektrik panoları ve prizleri, kablolama açısından düzenli olarak kontrol ediliyor mu?

Tüm elektrik tesisatları ve panolar görsel ve işlevsel olarak denetlenmelidir. Görsel veya işlevsel kontroller sırasında saptanan herhangi bir bulgu belgelenmeli ve ilgili organizasyon birimlerine rapor edilmelidir. Sorumlu birimler, ortaya çıkan eksiklikleri gözden geçirip düzeltmelidir.

VRM.3.G11 Elektrikli cihazların ve elektrik altyapısının yangın çıkarma riski

Elektrikli cihazlarının ve elektrik altyapısının, yangın çıkarma risklerinden kaçınılıyor mu?

Bir kurum içinde kişisel elektrikli ev aletlerinin kullanımı açıkça düzenlenmelidir. Tüm elektrikli ev aletleri, yetkili bir elektrikçi tarafından kontrol edilmeli ve kullanılmadan önce güvenli bulunmalıdır. Grup prizlerinin kullanımından mümkün olduğunca kaçınılmalıdır. Elektrik teknisyeni tarafından eksik prizler mevcut kanal sistemlerine monte edilmelidir.

3.3 3.SEVİYE GEREKSİNİMLER

1. ve 2. seviye gereksinimler sonrasında, binalar için artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda, risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilmektedir. Gereksinim tarafından öncelikli koruma sağlanan prensip parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.3.G12 İkincil güç kaynağı (E)

Kritik alanların yedekli beslenmeleri amaçlı güç kaynakları oluşturuldu mu, bakım, yük ve fonksiyonel testleri uygulanıyor mu?

Elektrik şebekesinden beslenen veri merkezi ve sistem odaları, artan erişilebilirlik gereksinimleri ve acil durum önlemleri gibi nedenlerden dolayı, yedekli yapı olarak ikincil bir güç kaynağı ile desteklenmelidir. Bu amaçla, korunacak alanlar için yeterince boyutlandırılmış bir merkezi UPS ve jeneratör kurulmalıdır. UPS ve jeneratörün, ana güç kaynağı (Şebeke elektriği) ile yedekli bir yapıda olduğu test edilmelidir. İkincil güç kaynakları doğru ve sorunsuz çalışmasını sağlamak için düzenli olarak bakıma tabi tutulmalıdırlar.

VRM.3.G13 A-B (“Dual bus”) yedekli sistem (E)

Kritik BT bileşenleri tamamen iki farklı kanaldan besleniyor mu?

Kritik BT bileşenleri, tek kaynaklı güç kaynağı yerine iki farklı kanaldan beslenmelidir. Bu işlevsellik yetkili kişiler ve uygun ekipman ile belli periyotlarda izlenmelidir.

VRM.3.G14 Elektrik kablolamanın malzeme güvenliği (E)

Kurulu kabloların serbestçe erişilebildiği yerlerin sayısı minimuma (hasar, sabotaja vb.) indirildi mi?

Ziyaretçilerinde çoğunlukla kullandığı veya binanın izlenemeyen alanlarında, kablo taşıma sistemlerinin ve panoların yetkisiz erişime karşı korunması önerilir. Her koşulda, yetkisiz kişilerin kablolara erişebileceği yerlerin sayısının en aza indirilmesi tavsiye edilir.

VRM.3.G15 Kabin sistemlerinin kullanımı (E)

Kabin sistemleri, içinde barındığı BT bileşenlerinin güvenliğini sağlayacak özelliklere sahip midir? Kabin seçimi için genel bir prosedür var mı?

Elektrik bağlantılarının ve ağ cihazlarının operasyonel güvenliğini artırmak için bunlar kabin sistemlerine monte edilmeli veya orada kurulmalıdır.

BT donanımı mümkün olduğunca kabin sistemlerine yerleştirilerek, muhafaza edilmelidir. Kabinler derinlik ve genişlik olarak gereksinimleri karşılamalıdır.

4 DETAYLI BİLGİ İÇİN KAYNAKLAR

Elektrik kablolama ile ilgili detaylı konulara aşağıdaki referans ve kaynaklardan ulaşılabilir:

- DIN 4102:2016-05
- IEC 60364 Electrical Installations for Buildings
- ANSI - Das American National Standards Institute
- BICSI - Building Industry Consulting Service International
- IEC 62305 – Lightning protection standard
- DIN VDE 0100 – Voltage electrical installation

VRM.4.G: BT KABLOLAMA

1 AÇIKLAMA

1.1 TANIM

BT kablolaması, kurum tarafından veri iletimi için kullanılan tüm iletişim kablolarından ve pasif bileşenlerden (bağlantı kutuları, dağıtım panoları (patch panel), vb.) oluşur. Aynı zamanda kurum iletişim ağının fiziksel temelidir. BT kablolaması, harici ağların bağlantı noktalarından (örneğin bir telekomünikasyon sağlayıcının ISDN bağlantısı, bir internet sağlayıcısının DSL bağlantısı), ağ terminal noktalarına (son kullanıcı cihazlarının, sunucuların, vb. ağ bağlantılarına) kadar uzanır.

1.2 HEDEF

BT Kablolama Rehber'i içerisinde, BT bileşenlerinin veri iletimi gerçekleştirmesi amacı ile ağa bağlanabilmelerini sağlayan BT kablolarının, ne tür gereksinimleri karşılamaları gerektiği açıklanmaktadır. Gereksinimleri karşılamak için uygulanacak önlemler ve çözümler, kurumun türüne ve boyutuna bağlı olarak değişebilir. Bu önlemler ve çözümler farklı bir rehber içerisinde yer almaktadır.

Bu **Rehberin** amacı, BT kablolama altyapısı ve ilgili unsurların, kötüye kullanma, izinsiz dinleme, kurulum ve sonrası oluşan arızalara yönelik eksikliklerin giderilmesini sağlamaktır.

1.3 KAPSAM DIŞI

Aktif ağ bileşenleri (yönlendiriciler (router), anahtarlar (switch), vb.) bu rehber kapsamında yer almamaktadır. Benzer şekilde, kablosuz ağlar (WLAN) konusu da rehber içerisinde bulunmamaktadır. Bu konular diğer sistem rehberlerinde ele alınmaktadır. BT kablolaması, üretici firma ve kullanılan uygulamalardan bağımsız bir biçimde iletişim ağına ilişkin fiziksel unsurları içermektedir. Ayrıca BT Kablolaması Rehberi içerisinde, veri aktarımı için kullanılan BT kabloları ile telekomünikasyon hizmetlerinde haberleşme için kullanılan kablolama arasında herhangi bir ayrım gözetilmemektedir.

2 RİSK KAYNAKLARI

Aşağıdaki tehditler ve eksiklikler BT kablolamanın korunması ve güvenliği açısından özellikle önemlidir:

2.1 KABLOLARIN YANGIN YÜKÜ

Kablo yangınları ciddi hasarlara neden olabilir. Kablo yangınları sebebiyle kısa devre, koruyucu iletkenlerin tahribi, tehlikeli gaz oluşumları ve alevler meydana gelebilir. Yanan kablolar genellikle ortam sıcaklığının çok az miktarda artmasına yol açar. Bu durum,

dedektörlerin yangın durumunu algılaması öncesi ortamda önemli miktarda duman oluşması riskini beraberinde getirir.

2.2 BT KABLOLAMANIN YETERSİZ BOYUTLANDIRILMASI

Kurumlarda kullanılacak odaların (iş alanları), sistem odalarının veya veri merkezlerinin tasarımları sırasında genellikle sadece mevcut ihtiyaçların dikkate alındığı gözlenmektedir. Bu durum çeşitli sorunları beraberinde getirmektedir. Örneğin kullanıcı sayısının artması veya yeni hizmetler için yeni donanımların edinilmesi (yeni kullanıcı bilgisayarları, ek sunucu/depolama cihazlarının bağlanması, vb.) ile birlikte kullanılan BT bileşenleri artacak, bu da ek BT kablolama ihtiyacını beraberinde getirecektir. Bununla birlikte yeni bileşenlere, gerekli BT kabloların eklenmesi, ancak mevcut kablolama altyapısı veya alanlar izin verdiği sürece mümkündür.

Birçok kurumda, gelecek ihtiyaçları düşünülmeden kurulan BT kablolama altyapısının yetersiz kalması nedeniyle, sonradan mecburi bir takım değişiklikler gerçekleştirilmekte ve bu değişiklikler çoğu zaman çok daha masraflı olmaktadır.

2.3 KABLOLAMA DOKÜMANTASYONUNUN YETERSİZLİĞİ

Kablolama dokümantasyonundaki bilgi eksiklikleri (tesisat konumları, ölçüler vb.) ve mevcut dokümanların güncel durumu yansıtmaması, bir bina dışında veya içerisinde yapılan inşaat çalışmaları sırasında kablolama tesisatının zarar görmesine neden olabilir. Dokümanların yetersiz olması (veya güncel olmaması), BT kablo tesisatlarında gerçekleştirilecek test, bakım ve onarım çalışmalarını zorlaştırır.

2.4 İZİNSİZ KABLO BAĞLANTILARI

BT bileşenleri veya diğer teknik bileşenler arasında yer alan izinsiz kablo bağlantıları, güvenlik sorunlarına veya arızalara neden olabilir. İzinsiz kablo bağlantıları nedeniyle, ağlara, sistemlere, dolayısıyla bilgilere veya uygulamalara yetkisi olmayan kötü niyetli kişilerin izinsiz erişimleri mümkün hale gelebilir. İzinsiz kablo bağlantıları yoluyla, bilgiler yanlış kişilere iletilebilir. Ayrıca bu nedenle, normal kablo bağlantıları aracılığı ile gerçekleştirilecek veri iletimi de kesintiye uğrayabilir.

2.5 KABLO HATTI HASARLARI

Kablolar ne kadar korunmasız bırakılırsa, bu durum kablo üzerinde yaşanabilecek hasar riskini o oranda artırır. Hasarın ağ kesintilerine sebebiyet vermesinin yanında, kablo izolasyonunun ve kılıflarının aşınması veya yırtılması gibi durumlar, istenmeyen etkileşimlerin (aşınan kablonun, su veya oradan geçen insanlarla teması gibi) ortaya çıkmasına neden olabilir.

2.6 KABLO PERFORMANSININ OLUMSUZ ETKİLENMESİ

Elektrik sinyalleri ileten BT kabloları, çevrelerinde oluşan elektriksel ve manyetik alanlardan olumsuz olarak etkilenebilir. Kablo tipine; elektriksel ve manyetik alanların frekans aralığına, gücüne, süresine, veri iletimi için kullanılan önlemlere (hata düzeltme, artıklık, vb.) bağlı olarak elektriksel ve manyetik alanlar nedeniyle kesintiler meydana gelebilir ve sinyal bozuklukları yaşanabilir. Örneğin parazitlenme, sinyal bozukluğunun özel bir şeklidir. Genellikle yakın veya bitişik bir hattan iletilen sinyaller, yüksek gerilim taşıyan elektrik kabloları nedeniyle oluşan manyetik alan, uydu, radyo, kablosuz ağlar, telekomünikasyon ekipmanları tarafından oluşturulan elektromanyetik alanlar bu tür sinyal bozulmalarına neden olur.

Elektriksel ve manyetik alan dışında, yüksek ısı ve fiziksel mekanik basınç gibi etmenler de kablo performansını olumsuz olarak etkileyebilir.

2.7 DİNLEME VE HATLARIN MANİPÜLASYONU

Hatların dinlenilmesi, ihmal edilmemesi gereken bir bilgi güvenliği tehdididir. Hiç bir kablo türünün, dinlemeye karşı tamamen güvenli olduğu söylenemez. Kullanılan kablo türüne göre, kablo dinleme teknikleri, dinleme için gerek duyulan cihazlar ve kablo dinleme zorluğu farklılıklar gösterir. Bazı hatlar, sadece ağa bağlı bir bilgisayar yardımı ile oldukça kolay bir şekilde dinlenebilir iken, bazı hatları dinlemek için pahalı cihazlara ihtiyaç duyulabilir. Kötü niyetli bir kişi açısından kablo dinleme kararı genellikle, kablo dinlemek için harcanacak eforun karşılığında, dinleme aracılığı ile elde edilecek bilginin değerine ve yakalanma riskine bağlı olarak verilir.

Bir hattın gerçekte dinlenip dinlenmediği kapsamlı bir çalışma ve çabayla saptanabilir. Hatları dinlemenin yanı sıra, kötü niyetli kişiler BT veri hatlarını kasıtlı olarak kendi işlerine yarayacak şekilde değiştirebilirler, hatta veri hatlarını kullanılamaz hale getirebilirler. Böylelikle BT işleyişinin aksamasına, durmasına, kurumun maddi anlamda zarar görmesine neden olabilirler.

3 GEREKSİNİMLER

BT kablolamaya ilişkin, karşılanması beklenen gereksinimler bu başlıkta açıklanmaktadır. Kurumdan kuruma değişiklik gösterebilmekle birlikte, genel olarak BT kablolamaya ilişkin gereksinimlerin karşılanmasından BT Yöneticisi sorumludur. Ayrıca bina ile ilgili fiziksel unsurlar için Bina Hizmetleri Yöneticisi'ne danışılması gerekebilir.

Her bir gereksinim içerisinde, ilgili diğer sorumlu kişiler de tanımlanmıştır. Kurumların son zamanlarda bilgi güvenliği (ve özellikle ISO 27001) çalışmaları gerçekleştirmekte olduğu göz önünde bulundurularak, Bilgi Güvenliği Yöneticisi'nin stratejik kararlara dahil edilmesi

düşünülmelidir. Bilgi Güvenliği Yöneticisi ayrıca, gereksinim maddelerinin uygulanması sırasında, uygulamaların kurum için oluşturulan güvenlik politikalarına uyumluluğunun sağlanmasından sorumludur.

Rehber içerisinde gereksinimler, üç ana başlık içerisinde toplanmıştır. Kurumların öncelikli olarak "1.Seviye Gereksinimler" başlığı altında yer alan maddeleri zorunlu olarak değerlendirmeleri, sonra ihtiyaçları doğrultusunda "2.Seviye Gereksinimler" ve "3.Seviye Gereksinimler" başlıklarını ele almaları önerilmektedir.

Tablo 5. BT Kablolama Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Yöneticisi
Diğer Sorumlular	Bina hizmetleri yöneticisi

3.1 1.SEVİYE GEREKSİNİMLER

Kurumlar ve organizasyonlar aşağıda yer alan gereksinimleri öncelikli olarak uygulamalıdırlar.

VRM.4.G1 Uygun kablo tiplerinin seçimi

Kablo seçilirken, iletim gereksinimleri yanında ortam koşulları da irdelendi mi?

Kablo seçiminde, teknik gereksinimlerin yanında kabloların yer alacağı ve işletileceği çevresel koşullar da dikkate alınmalıdır. Kurumun veri iletişim ve haberleşme ihtiyaçlarını karşılayacak bir altyapı, uygun tip ve mesafede kablolar kullanılarak oluşturulmalıdır. Kabloların bulunacağı ortamların sıcaklıkları, kablo güzergâhları, kurulum sırasında kablolara uygulanacak gerilim kuvveti, kurulum biçimi ve parazit/gürültü kaynakları gibi çevresel faktörlere dikkat edilmelidir. Ayrıca, BT kablolarının seçimi sırasında, geçerli standartlar ve düzenlemeler göz önünde bulundurulmalıdır.

VRM.4.G2 Kablo yönetimi

Kablo taşıma kanalları, olası genişletme ihtiyaçları veya minimum mesafeler bakımından yeterince boyutlandırılmış mı?

Kabloların bina içerisinde hangi güzergahlardan geçeceği ve ne tür taşıma sistemleri (kablo tavaları, kablo kanalları, vb.) aracılığı ile taşınacağı kurulum öncesinde planlanmalıdır. Bu süreçte, mevcut koşullar, gelecekte oluşabilecek ihtiyaçlar ve olası teknik genişlemeler dikkate alınmalıdır. Genel olarak, BT kablolarının, elektrik kablolarından ayrı tutulması sağlanmalı; BT ve elektrik kablolarının ortak kablo taşıma

kanalından taşınması durumunda kablo türlerinin karışmaması için olası tehlikelerden kaçınmaya özen gösterilmelidir.

VRM.4.G3 Profesyonel kurulum

BT kablolaması, geçerli standartlara ve üreticinin tavsiye ettiği özelliklere uygun bir şekilde yapıldı mı?

BT kablolama kurulum çalışmaları, ilgili tüm standartlara uyularak, dikkatli ve ustalıkla yapılmalıdır. BT kablolamanın profesyonel bir şekilde gerçekleştirildiği, malzeme teslimi sırasında doğru kabloların ve bağlantı bileşenlerinin tedarik edilip edilmediği kurum tarafından her aşamada kontrol edilmelidir. BT kabloları ve kablo taşıma sistemleri döşenirken, kurulumun binanın normal kullanımını etkilememesine, bina içerisinde herhangi bir hasara neden olmamasına dikkat edilmelidir. Kurulum sırasında, BT kabloları ile elektrik kablolarının ayrı yönlendirilmesi sağlanmalıdır.

3.2 2.SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, BT kablolama altyapısını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

VRM.4.G4 BT kablolama ihtiyaç analizi

BT kablolama ihtiyaç analizi yapılırken gizlilik, bütünlük, erişilebilirlik hususları ele alındı mı?

Kapsamlı BT kablolama çalışmaları öncesinde, mevcut ve geleceğe yönelik ihtiyaçlar göz önünde bulundurularak, uygun maliyetli BT kablolama gereksinimlerinin oluşturulması önerilmektedir. Bir gereksinim analizinde öncelikle BT bileşenlerinin, bilgisayar (veya iş istasyonu) kullanacak kurum kullanıcılarının sayıları belirlenmeli ve belirlenen sayıların uzun vadede nasıl gelişebileceği tahmin edilmelidir. Ayrıca, BT kablolama ihtiyaç analizi yapılırken, yaşanabilecek arızalara rağmen veri iletiminin kesintisiz olması (erişilebilirlik), taşınan verinin bütünlüğü açısından dış etkenlere karşı koruma (bütünlük) ve taşınan verilerin gizliliğinin sağlanması (gizlilik) hususları göz önüne alınmalıdır.

VRM.4.G5 BT kablolama muayene (kabul)

İş kabul belgeleri, giderilen eksiklikler, kalan işler, garanti süreleri için son tarihler hakkında bilgileri içeriyor mu?

BT kablolamanın, kurulumun tamamlanması sonrasında bir muayene ve kabul sürecine tabi tutulması önerilmektedir. Kabul, BT kablolama çalışmasına ilişkin tüm görevler tamamlandıktan, işi icra eden/yüklenici kabul aşamasına gelindiğini bildirdikten sonra ve

işveren (kurum) tarafından yapılan kontrollerde kabul edilemez eksiklikler bulunmadığında verilmelidir. Kurulum sonrasında gerekli kontroller için yeterli süre ön görülerek bir kabul tarihi belirlenmeli, ayrıca farklı standartlara uyumluluk da kabul aşamasında değerlendirilmelidir.

Kabul sürecinde kullanılmak üzere, kabul sırasında kontrol edilecek unsurları ve kontrol biçimini içeren bir kontrol listesi hazırlanması önerilir. Kontrol listesi, işletme alanları için genel gereksinimleri de içermelidir. Kabul sırasında bir kabul tutanağı oluşturulmalı, bu tutanağın katılımcılar ve sorumlu kişiler tarafından yasal olarak bağlayıcı bir şekilde imzalanması sağlanmalıdır. Tutanak, BT kablolama dokümanlarının bir parçası olmalıdır.

VRM.4.G6 Ağ dokümanlarının gözden geçirilmesi ve güncellenmesi

BT kabloma dokümantasyonu, ağda yapılan değişiklikler sonrası güncelleniyor mu?

İhtiyaçlar doğrultusunda, ağlar ve BT kablolama altyapısı üzerinde değişiklikler gerekebilir. BT kablolamaya ait dokümantasyon, ağ ve kablolamaya ilişkin herhangi bir değişikliğin ayrılmaz bir parçası olarak kabul edilmeli ve dikkate alınmalıdır. Değişiklikler yapılmadan önce bu dokümantasyondan yararlanılmalı, değişiklik sonrası dokümantasyondaki ilgili alanlarının kolayca güncellenebilmesi sağlanmalıdır. Ayrıca, ağ ve BT kablolama dokümantasyonun güncel tutulması için kurumun mevcut doküman yönetim sistemi kullanılabilir. Böylelikle yapılan değişikliklerin geçmişi takip edilebilecektir.

VRM.4.G7 Kablo taşıma sistemlerinin yangından korunması

Kablo kanallarında ve taşıma güzergahlarında yangına dayanıklı malzemeler kullanıldı mı?

Bina içerisinde kullanılan tüm elektrik ve BT kabloları, başta yangın bölgelerinden, duvarlardan, tavanlardan geçirilen veya trafik güzergahlarına döşenen tüm kablolar olmak üzere, yangın güvenlik yönetmeliklerine tabi olmalıdır. Bu nedenle, kablo kanalları ve taşıma güzergahları planlanırken, yangın güvenlik görevlisine (acil durum sorumlusu) danışılması önerilmektedir. Kablo kanallarının yangına dayanıklı malzemeler kullanılarak yalıtılması ve düzgün bir biçimde kilitlenmesi gibi önlemler yardımıyla, kanalların gerek yangına, gerekse sabotaja karşı korunması sağlanmalıdır. Buna ek olarak, kurulum/yenileme çalışmaları sonrası, yangın koruma önlemleri düzenli aralıklarla kontrol edilmelidir.

VRM.4.G8 BT kablolamanın dokümantasyonu ve etiketleme

BT kablolamanın etiketleme ve dokümantasyonu ile ilgili düzenlemeler mevcut mu?

Kurum bünyesinde, BT kablolamasına ilişkin iyi bir dokümantasyon oluşturulmalıdır. Dokümantasyon içerisinde BT kablolama ile ilgili tüm bileşenler, kabloların kurulumu ve işletilmesi ile ilgili tüm kayıtlar (mevcut durum ve ilerdeki genişleme planları dahil olmak üzere) yer almalıdır. Bu tür bir dokümantasyon, bakım, onarım, sorun giderme ve kontrol için oldukça önemlidir. Hazırlanan dokümantasyona uygun bir biçimde, kullanılan kablolar (her iki uçlarından) etiketlenmeli, herhangi bir değişiklik durumunda ilgili dokümanın (ve gerekli durumlarda etiketlerin) güncellenmesi sağlanmalıdır.

VRM.4.G9 Mevcut bağlantıların kontrolü

Pano ve kablo çıkışları (priz vb.) düzenli olarak kontrol ediliyor mu?

Tüm BT kablolama altyapısı, bağlantıları ve kullanılan dağıtım panoları, düzenli aralıklarla, görsel ve işlevsel olarak denetlenmelidir. Görsel veya işlevsel kontroller sırasında tespit edilen bulgular dokümante edilerek kayıt altına alınmalı ve ilgili birimlere raporlanmalıdır. Sorumlu birimlerin, ortaya çıkan eksiklikleri gözden geçirip düzeltmeleri sağlanmalıdır.

3.3 3.SEVİYE GEREKSİNİMLER

1. ve 2. seviye gereksinimler sonrasında, BT kablolama için artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilmektedir. Gereksinim tarafından öncelikli koruma sağlanan prensip, parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.4.G10 Ağ yedekliliği

Yüksek erişilebilirlik kapsamında, farklı hatlar üzerinden yedekli kablo taşıma sistemleri (birincil, ikincil, üçüncül vs.) kullanılıyor mu?

Binaların kritik alanlarına (özellikle sunucu odası veya veri merkezi) kesintisiz hizmet verebilmek için, farklı hatlar üzerinden yedekli kablo taşıma sistemleri aracılığı ile veri iletiminin sağlanması önerilmektedir. Ayrıca, BT veya telekomünikasyon sağlayıcılarıyla olan bağlantıların yedekli tasarlanıp tasarlanmadığı kontrol edilmelidir. Gerçek bir yedeklilik için, fiziksel olarak farklı kablo yolları aracılığı ile ağ bağlantılarının oluşturulması sağlanmalıdır.

VRM.4.G11 BT kablolamanın fiziksel güvenliği

Kablola geçiş güzergahlarında yetkisiz erişimlerden kaynaklı (hasar, sabotaja vb.) olaylara karşı fiziksel güvenlik önlemleri alındı mı?

Ziyaretçilerin kullandığı odalarda veya binanın izlenemeyen alanlarında yer alan kabloların, kablo taşıma sistemlerinin ve dağıtım panolarının yetkisiz erişime karşı korunmaları sağlanmalıdır. Kabloların yetkisiz kişilerin erişebileceği yerlerden geçirilmemesi ve korunması gerekli kablo uzunluğunun mümkün olduğunca kısa tutulması önerilir. Kablo güvenliğinin sağlanabilmesi için kablo kanal güzergâhı boyunca, karşılaşılabilecek tehdit unsurları da göz önünde bulundurulmalı ve alınması gereken önlemler planlanmalıdır. Koridor veya yeraltı otoparkı gibi ulaşım yolları olarak kullanılan alanlarda yer alan kablolar, kazara meydana gelebilecek mekanik hasarlara, gerekli durumlarda sabotaja karşı korunacak şekilde sağlam bir biçimde kapatılmalıdır.

VRM.4.G12 Korumalı (shielded) kablo kullanımı ile elektromanyetik alandan korunma

Kablo iletim yollarının elektromanyetik alanlardan etkilenmemesi için korumalı kablolar kullanılıyor mu?

Binalar ve veri merkezlerinde bulunan kablo iletim yollarının, elektromanyetik alanlardan etkilenmeyecek şekilde tasarlanmalarına dikkat edilmelidir. Aksi takdirde, elektromanyetik girişimler (EMI), kablo üzerinden iletilen sinyallerin bozulmasına, gürültü ve parazit oluşmasına neden olabilir. Elektromanyetik girişimleri engellemek için genellikle korumalı (shielded) kablolardan yararlanılır. Korumalı kablolar ile kabloların fiziksel dayanımı artırılır, elektromanyetik girişimlerin kablo üzerinden iletilen sinyalleri bozması engellenir, kablo üzerinden veri iletişiminin güvenli ve kaliteli biçimde gerçekleşmesi sağlanır.

VRM.4.G13 Kabin sistemlerinin kullanımı

Kabin sistemlerinin seçimi ve ekipmanı ile ilgili bir düzenleme (tek tip kabin sistem özellikler gibi) var mı?

Aktif ve pasif ağ bileşenlerinin operasyonel güvenliğini artırmak için, bu cihazların kabin sistemlerine monte edilmeleri veya kurulmaları sağlanmalıdır.

Kurum içerisinde kullanılacak kabin sistemlerine ilişkin özelliklerin belirlenmesi ve bu özelliklere uygun tek tip kabinlerin seçilmesi önerilmektedir. Kabin sistemlerinin kullanımı ve yönetimi için gerekli yönergeler hazırlanmalı ve ilgili kişiler ile paylaşılmalıdır.

4 DETAYLI BİLGİ İÇİN KAYNAKLAR

BT kablolama ile ilgili detaylı konulara aşağıdaki referans ve kaynaklardan ulaşılabilir:

- [EN50173] EN 50173:2007
- [EN50174] EN 50174:2009
- [EN50310] EN 50310:2017-02
- [EN50346] EN 50346:2010-02
- [IEC60364] IEC60364
- [IEEE8023] IEEE8023
- [ISO11801] ISO/IEC 11801:2002-09
- [VDE100] DIN VDE 0100

VRM - VERİ MERKEZİ UYGULAMA REHBERLERİ

Veri merkezi temel bileşenlerinin ayrıntılı uygulama talimatları aşağıdaki başlıklarda sunulmaktadır:

VRM.1.U Genel Bina

VRM.2.U Veri Merkezi ve/veya Sistem Odası

VRM.3.U Elektrik Kablolama

VRM.4.U BT Kablolama

VRM.1.U: GENEL BİNA

1 AÇIKLAMA

1.1 TANIM

Binalar, iş süreçlerinin yürütülmesi için gerekli ortamı sağlayan fiziksel yapılardır. Bir bina iş birimlerini, veriyi, veri işlenerek elde edilen bilgiyi ve bilgi teknolojilerini barındırır, bu unsurlar için bir koruma sağlar. Gerek iş süreçlerinin ve gerekse BT operasyonlarının yürütülmesinde bina ile birlikte bina altyapısı da oldukça önemlidir. Elinizdeki rehber sadece binaya ilişkin değil, aynı zamanda duvar, tavan, zemin, çatı, pencere ve kapı ile birlikte elektrik, su, gaz, ısıtma ve soğutma gibi unsurlar ile ilgili tüm bina altyapı ve tedarik hizmetlerine ilişkin uygulama maddelerini içermektedir.

Bina birden fazla kurum tarafından kullanılıyor olabilir, bina içerisinde yer alan birimlerin birbirinden farklı ihtiyaçları bulunabilir. Bununla birlikte binanın farklı taraflarca (vatandaşlar, müşteriler, tedarikçiler) kullanımı ön görülüyor olabilir. Bu farklı kullanımlar göz önünde bulundurularak, bina tasarımı ve kullanılan altyapı ekipmanları ile bina kullanım konseptinin uyumlu olması sağlanmalıdır. Bina içerisinde teknolojik bileşenlerin etkin ve güvenli bir biçimde kullanılmasıyla, çalışanlar için en uygun ortamın sağlanması hedeflenmelidir.

1.2 YAŞAM DÖNGÜSÜ

Elinizdeki rehber, içerisinde veri merkezi (veya sistem odası) bulunduran kurum ve şirket binalarının planlanmasında ve kullanılmasında göz önünde bulundurulması gereken teknik ve teknik olmayan unsurlar göz önünde bulundurularak hazırlanmıştır. Rehber içerisinde yer alan uygulama maddeleri, kurum ihtiyaçları doğrultusunda gereksinimlerin belirlenmesinden başlayarak, planlama ve tasarım, tedarik, kurulum ve kullanıma hazırlık, kullanım ve taşınma/sonlandırma adımlarını içerecek biçimde, bir yaşam döngüsüne uygun olarak bir araya getirilmiştir.

Bina içerisinde yer alabilecek kablolama, veri merkezi, vb. temel bileşenlerin her biri farklı rehberlerde ele alınmaktadır.

Kurumların veya şirketlerin yeni bir bina kullanmaları durumunda, rehber içerisinde yer alan uygulamaları, planlama aşamasından başlayarak ele alınmaları önerilmektedir. Diğer taraftan mevcut bir binanın kullanılması söz konusu olduğunda çoğu zaman yenilik, değişiklik, dönüşüm, genişletme gündeme gelecek, rehberde yer alan uygulamaları gerçekleştirme olanakları daha sınırlı olacaktır. Elinizdeki rehber bir bina içerisinde bulunan kurumlar tarafından kullanılabileceği gibi, birkaç bina veya kampüse/yerleşkeye

yayılmış kurumlar tarafından da kullanılabilir. Kurumların rehberden yararlanırken içinde bulundukları koşullara göre hareket etmeleri tavsiye edilmektedir.

Planlama ve Tasarım

Bir binanın kullanım amacı ve bina içerisinde gerçekleştirilecek iş süreçlerine ait koruma gereksinimleri, bina tasarımı ve kullanılacak ekipmanların seçimi açısından belirleyicidir. Binanın yeri ve türünün değerlendirmesiyle başlayarak, binanın kullanım amacına uygunluğu veya kullanım amacına uygun bir hale getirmek için gereken şekilde tasarlanıp tasarlanamayacağı tetkik edilmelidir.

Mevcut bir binanın kullanım amacı göz önünde bulundurularak binanın kullanımına yönelik koruma yönelimli bir planlama yapılabilir (***bkz. VRM.1.U1 Bina güvenliği planlanması***). Bununla birlikte ihtiyaçlar doğrultusunda bina içerisinde farklı güvenlik bölgeleri oluşturulabilir (***bkz. VRM.1.U22 Güvenlik bölgelerinin oluşturulması***). Ayrıca sadece yetkili kişilerin bu bölgelere girişleri sağlanmalı (***bkz. VRM.1.U7 Güvenlik ve erişim kontrolü***) ve yetkisiz kişilerin erişimi engellenmelidir (***bkz. VRM.1.U21 Güvenli Kapılar ve Pencereler***).

Bina kullanıma hazır hale getirilirken mevcut yönetmeliklere uyulması, (**örn. *VRM.1.U3 Yangın koruma yönetmeliklerine uyulması***) ve eğer mevcut bir bina kullanılacak ise bina içerisindeki bölümlerin ihtiyaçlara uygun hale getirilmesi (***bkz. VRM.1.U 31 Korunması gereken alanların düzenlenmesi)*** gereklidir. Ayrıca bina (ve içerisinde bulunan farklı odaların/alanların) amaçlanan kullanımına göre beklenen elektrik tesisatının hazırlanması (***bkz. VRM.1.U 2 Elektrik yük dağılımının ayarlanması/yapılandırılması)*** önemlidir.

Tedarik

Gerek yeni bir bina için yer seçimi, gerekse var olan bir binanın ihtiyaçlara uygunluğunun değerlendirilmesi sırasında ***VRM.1.U24 Uygun yer seçimi*** ve ***VRM.1.U29 Uygun bina seçimi*** uygulama maddeleri göz önünde bulundurulmalıdır.

İnşaat aşaması ve kullanıma hazırlık

Planlama aşamasında gerekli olduğu düşünülen uygulamalar yanı sıra, inşaat aşamasında, ***VRM.1.U9 Uygulanabilir standartlara ve düzenlemelere uyum*** ve ***VRM.1.U3 Yangın güvenliği yönetmeliklerine uyulması*** uygulama maddelerine dikkat edilmesi önerilir. ***VRM.1.U12 Dağıtım panolarına erişimle ilgili düzenlemeler, VRM.1.U7 Güvenlik ve erişim kontrolü*** ve ***VRM.1.U12 Anahtar/kilit yönetimi*** gibi maddelerin, en geç binaya taşınırken tamamlanması gereklidir.

Bina kullanımı

Binanın kullanımı sırasında devreye alınan tüm uygulamaların işletilmesi gerekmektedir. Örneğin ***VRM.1.U17 yangın güvenlik kontrollerin***in gerçekleştirilmesi ile yangın güvenlik yönetmeliklerine uyumluluk izlenebilecektir, ***VRM.1.U6 Kapalı pencereler ve kapılar*** uygulaması sayesinde, bina içerisinde en azından hırsızlığa karşı temel korunma sağlanabilecektir.

Acil durum hazırlığı

İşletim esnasında bina içerisinde, BT bileşenleri ve altyapı ekipmanları üzerinde ne olup bittiğini takip etmek, gerektiğinde alarmlar üreterek yetkili kişilerin hızlı bir şekilde devreye girmelerini sağlamak oldukça önemlidir. Ayrıca acil durumlar esnasında hazırlıklı olunması için bir uyarı planı hazırlanmalı ve bu planın gerektiğinde uygulanabilirliğine ilişkin tatbikatlar düzenli aralıklarla gerçekleştirilmelidir (**bkz. VRM.1.U19 Acil durum planı ve yangın tatbikatları**). Aksi halde acil durumlarda yanlış kararların alınması veya gerçekleştirilen faaliyetlerin belirsizlikler nedeniyle gecikmesi söz konusu olabilir.

2 UYGULAMALAR

Aşağıda yer alan maddeler, "Genel Bina" bölümüne özel uygulama maddeleridir.

2.1 1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

VRM.1.U1 Bina güvenliği planlaması [Planlama Sorumlusu, Bilgi Güvenliği Sorumlusu]

İçerisinde veri merkezi/sistem odası barındıran bir binanın mevcut ve planlanan kullanımı, bina içerisinde işletilen iş süreçlerinin, operasyonun ve veri merkezinin koruma gereksinimlerine bağlı olarak bina güvenliği planlanmalıdır. Planlama sırasında, binada çalışacak kişilerin ve kritik varlıkların korunmasına yönelik gereksinimler, farklı birimlerin güvenlik gereksinimleri, bina içerisinde yer alacak BT bileşenlerine ilişkin ihtiyaç duyulan erişilebilirlik seviyeleri, olası çevresel tehlikeler, iç ve dış tehdit unsurları dikkate alınmalıdır. BT bileşenlerine ek olarak, (örneğin elektrik iletimi, iklimlendirme, vb.) tüm altyapı ekipmanları kapsam içerisinde yer almalıdır.

Binaya yönelik, yangın, yıldırım, su sızıntıları, çevresel tehlikeler, yetkisiz erişim gibi birçok farklı tehdit unsuru bulunabilir. Kurumun ve söz konusu binanın büyüklüğüne, kurum yapılanmasına bağlı olarak farklı tehdit unsurlarını yönetmek amacı ile farklı kişiler yetkilendirilmiş olabilir. Bu durumda gerekli güvenlik önlemlerinin alınabilmesi için yetkili kişilerin koordineli biçimde çalışmaları sağlanmalıdır.

Mevcut binanın yerleşim düzeninin, binanın amaçlanan kullanımı ile uyumlu olması son derece önemlidir (**bkz. VRM.1.U1.8 Binanın fiziksel güvenlik çerçevesi**). Planlama sırasında öncelikle bina içerisinde yer alan güvenlik bölgeleri üzerinde durulması gerekir (**bkz. VRM.1.U23 Güvenlik bölgelerinin oluşturulması**). Özellikle düşük güvenlikli bir bölge ile yüksek güvenlikli bir bölge arasında fiziksel bir ayrım bulunması ve farklı bölgeler arası geçişin gerekli kontroller sonrası gerçekleşmesi sağlanmalıdır. Yetkisi olmayan kişilerin bölgeler arası geçişleri engellenmeli, özellikle bölgeler yetkisiz erişime karşı korunmalıdır. Örneğin, yüksek güvenlikli bölgelerin kaçış kapıları, dışarıdan içeriye açılmayacak şekilde korunabilir. Benzer biçimde pencerelerin ve kapıların koruma gereksinimlerine göre korunması önerilir (**bkz. VRM.1.U21 Güvenli kapı ve pencereler**).

VRM.1.U2 Elektrik yük dağılımının ayarlanması/yapılandırılması

İçerisinde veri merkezi yer alan binalarda, ekonomik bir şekilde elektrik iletimini sağlayabilmek ve güçlü yüklerin akımını karşılayabilmek için üç fazlı elektrik iletiminin sağlanması gerekir. Fakat fazlar arasında yük dağılımının dengesiz olması çeşitli sorunlara yol açabilir. Bu nedenle bina tasarımı sırasında, bina içerisinde yer alacak birimlerin, altyapı ekipmanlarının ve veri merkezinde yer alacak BT bileşenlerinin kullanım gereksinimleri göz önünde bulundurularak elektrik tesisatı tasarlanmalı ve kurulum sırasında fazlar arasında yük dağılımına dikkat edilmelidir.

Özellikle elektrik tesisatının ilk kurulması aşamasında yanlışlıkla, üç fazdan birine daha fazla yüklenildiği durumlar ortaya çıkabilmektedir. Ayrıca odaların doluluk oranları ve elektrik kullanım değerleri, tasarım sırasında öngörülen değerler ile uyuşmayabilir. Kurulu elektrik tesisatının, güncel ihtiyaçları karşılama durumu, fazlar üzerinde yüklerin dengeli olup olmadığı düzenli olarak kontrol edilmeli, gerekli düzenlemelerin ve iyileştirmelerin yapılması sağlanmalıdır.

Düzenleme ve iyileştirme için odaların kullanımında değişikliklere gidilebileceği gibi gerekli durumlarda hatlar yeniden düzenlenerek, BT bileşenlerinin veya altyapı ekipmanlarının farklı fazlardan beslenmelerini sağlamak da düşünülebilir. Bununla birlikte, bazı durumlarda mevcut tesisata ekler yapmak veya tamamen yeni bir tesisat oluşturmak da gerekli olabilir.

Bu konuyla ilgili, ağ kablolama ve elektrik kablolama rehberleri içerisinde daha fazla bilgi yer almaktadır.

VRM.1.U3 Yangın güvenliği yönetmeliklerine uyulması

Bakanlar Kurulu tarafından kararlaştırılan, Resmi Gazete'de yayımlanan, bina yangın korunma yönetmeliği gereksinimlerine uyulmalı, mevcut yangın koruma standartları (örn.

TSE 11925, ISO 11925, DIN 4102 standartları) ve bina denetim şartları mutlaka dikkate alınmalıdır.

Yerel itfaiyenin, yangın güvenliği planlamasına dahil edilmesi önerilmektedir. Bina içerisinde kritik BT bileşenlerini barındıran veri merkezi ile ilgili detaylı bir yangın koruma yaklaşımı oluşturulmalı ve uygulanmalıdır. Yangın ve duman koruma özelliklerine sahip kapıların kurulması, duvarların yükseltilmesi gibi özel tedbirlerle bu odalar üzerinde yangının etkisini en aza indirgemek hedeflenmelidir. Bu amaçla BS EN 1047-2 gibi standartlardan yararlanılabilir.

Kurum bünyesinde yangın güvenliği yönetmeliklerine uyulmasından sorumlu bir kişi belirlenmesi gereklidir. Bu kişi yangın güvenliği konusunda eğitimli bir personel ya da bir yangın güvenliği görevlisi olabilir.

Bina içerisinde yer alan kaçış yollarının iyi bir biçimde tanımlanması özellikle önemlidir. Bu amaçla kaçış yollarını tarif eden işaretler kullanılmalı, kaçış yolları her zaman açık tutulmalı, engellenmemelidir (örneğin koridorlarda gereksiz envanterin tutulmasına izin verilmemelidir).

Yangın ve dumandan koruma kapıları sadece kapalı haldeyken koruma sağlar. Bu nedenle bu kapıların asla açık kalmaması sağlanmalıdır. Sebep her ne olursa olsun bu kapılar kalıcı olarak açık tutulmamalı, istisnalara izin verilmemelidir.

Yangın durumunda hızlı bir şekilde yangın söndürme işlemine başlanması gerekir. Bu yüzden yangın alarm panelinin ve söndürme suyu giriş noktalarının, itfaiye ve ilgili ekipler tarafından hızlı bir şekilde bulunmasını sağlamak için işaretler ile gerekli yönlendirmeler yapılmalıdır.

Etkin yangın korumasına ulaşmak için ilgili tüm tarafların işbirliği gereklidir.

Binada bulunan, yangına sebep olacak veya yangının büyümesine katkıda bulunacak tüm unsurlar bir yangın yükü (tehdidi) yaratır. Mobilyalar, zemin kaplamaları ve perdeler; BT bileşenleri ve kabloları kadar yangın tehlikesi oluşturmaktadır. Malzemelerin alev alması veya yanmazlığı hakkında daha fazla bilgiye TSE 11925, ISO 11925, DIN 4102 standartlarından ulaşılabilir.

BT bileşenlerinin kurulumu öncesinde, aynı odada ve bitişik odalarda mevcut yangın yüklerine önceden dikkat edilmelidir. Örneğin önemli verilerin yer aldığı disk arşivinin, kağıt yığınlarının depolandığı odaların içerisinde veya yakınında bulunması tercih edilmemelidir.

Bina ve odalarda gereksiz yangın yüklerinden kaçınılmaya özen gösterilmelidir. Atıkların, özellikle atık kağıtların ve ambalaj atıklarının, düzenli olarak elden çıkarılması aktif yangın koruması olarak görülmektedir. Ofislerden gerekli görülmeyen dosyalar kaldırılmalı ve özel

olarak belirlenmiş arşivlerde saklanmalıdır. BT bileşenlerinin yer aldığı odalarda gereksiz yangın yüklerinin en yaygın örnekleri, karton veya polistiren gibi ambalaj malzemeleridir. BT odalarından ambalaj malzemeleri çıkartılmalı ve ileride ihtiyaç duyulacağı düşünülüyorsa belirlenmiş depo odalarına taşınmalıdır.

Binaların planlama aşamasından itibaren gereksiz yangın yüklerinin azaltılmasına dikkat edilmeli, mümkün oldukça yanıcı olmayan malzemeler kullanılması sağlanmalıdır (yapı malzemesi sınıf A). Planlama aşaması sonrasında da, yangın koruması açısından güvenli çalışma ortamı sağlamak ve eşik değerleri aşmamak için bina ve odalarında yer alan yangın yüklerinin kontrol altında tutulması gerekir.

VRM.1.U4 Binalarda yangın algılama [Planlama Sorumlusu]

Binalarda yangın algılama ve yangın durumunda zamanında uyarı yapılmasına yönelik önlemler, binada yaşayan herkesin sağlığını ve yaşamını korumak için alınması gereken temel tedbirlerin başında gelir.

Yangın koruma önlemleri konusunda ilgili yangın güvenliği yönetmelikleri gereksinimlerine uyulması veya ulusal bina yönetmeliklerinin, standartların dikkate alınması yanı sıra, bina büyüklüğüne ve kullanımına uygun bir yangın koruma prosedürü oluşturulması önerilmektedir.

Binaların kullanım türüne ve yapısına bağlı olarak, farklı nedenlerle yangınlar meydana gelebilir. Çalışanları korumak ve zamanında yangın oluşumunu önlemek için, yangının mümkün olduğunca hızlı bir biçimde tespit edilmesi, alarmlar üretilerek ilgili ekiplere haber verilmesi ve kısa sürede söndürülmesi gereklidir. Bu amaçla binada uygun yerlere duman detektörlerinin monte edilmesi gerekmektedir.

Dedektörler bir yangın alarm paneli vasıtasıyla kontrol edilebilir ve değerlendirilebilir. Her türlü dedektör, bir yangın alarm paneli ile birlikte yangın alarm sistemini oluşturur. Binada bulunan tüm koridorların ve odaların tavanlarına duman detektörleri yerleştirilir. Özellikle BT bileşenlerinin ve altyapı ekipmanlarının bulunduğu odalarda, odanın hangi bölgesinde yangın oluştuğunu tespit edebilecek, sadece o bölgede yer alan yangının söndürülmesini sağlayabilecek şekilde bölgesel yangın algılama yaklaşımının uygulanması daha doğru olacaktır.

Bina içerisinde bir iklimlendirme sisteminin mevcut olması durumunda, iklimlendirme sistemi tarafından kullanılan havalandırma kanalları da izlenmelidir. Yangın durumunda oluşan dumanın, havalandırma kanalları aracılığıyla yayılmasını önlemek için, gerekli durumlarda iklimlendirme sisteminin, yangın alarm sistemi tarafından merkezi olarak kapatılabilmesi önerilmektedir.

Üreticinin teknik özelliklerine göre duman detektörlerinin doğru şekilde monte edilmesini sağlamak önemlidir. Bina içerisinde ihtiyaçlara uygun bir yangın alarm sisteminin planlanması, kurulması ve işletilmesi için TS 54, EN 54, DIN 14675 standartlarından yararlanılabilir.

Yangın alarm sistemi içerisinde bir kontrol panel bulunması önerilir. Bu sayede, arıza mesajları da dahil olmak üzere, yangın alarm sistemi tarafından üretilen tüm mesajlar merkezi bir yerden takip edilebilir (örn. güvenlik odasından).

Tüm duman dedektörlerinin ve yangın alarm sistemini oluşturan diğer cihazların işlevselliği düzenli olarak kontrol edilmelidir. Belirli aralıklarla, rastgele seçilen dedektör hatlarının bir kısmı, işlevselliği için manuel olarak test edilmelidir.

Duman algılanması durumunda, bina içerisinde herkesin duyabileceği yüksek sesli bir yangın alarmı tetiklenmelidir. Gürültülü ortamlar için sesli yangın alarmının görsel bir alarm ile desteklenmesi de önerilmektedir.

Acil durumlarda, binanın güvenli bir şekilde tahliye edilmesini sağlamak için kullanılacak olan kaçış yollarının kullanılabilir ve engelsiz olması her zaman temin etmelidir. Kaçış yollarının, mobilyalarla, hatta önemli bir yangın yükü oluşturabilecek fotokopi makineleri veya yazıcılar gibi elektrik kullanan ekipmanlarla daraltılmaması sağlanmalıdır. Kaçış yollarının kullanılabilir ve engelsiz olduğu düzenli olarak kontrol edilmelidir.

VRM.1.U5 Taşınabilir yangın söndürücüler

Çoğu büyük yangın, ilk başta kolayca kontrol edilebilecek küçük yangınların genişlemesiyle oluşur. Özellikle ofis ortamlarında yangın, hızlı yayılabileceği yangın yükleri bulur. Bu nedenle yangınların olabildiğince erken kontrolü son derece önemlidir.

Bina içerisinde yangının hızlı bir şekilde söndürülebilmesi için, taşınabilir yangın söndürücülerin (TS 862-3, DIN EN 3-3 standartlarına uygun) yeterli sayıda ve büyüklükte bulunması gereklidir. Kullanılabilecek taşınabilir yangın söndürücülerin büyüklükleri, sınıfları konusunda yerel itfaiyeden görüş alınması önerilir.

Taşınabilir yangın söndürücülerin, yangın durumunda kolayca ulaşılabilecek bir yerde bulundurulması gerekir. Çalışanlar kendilerine en yakın taşınabilir yangın söndürücünün bulunduğu yeri bilmeli veya uygun işaretler yardımıyla söndürücülere hızlıca erişebilmelidir.

Taşınabilir yangın söndürücülerinin ağırlıklarının 20 kg üzerinde olmasına genellikle izin verilmez. Genellikle bina içerisinde bulunan 6 ve 12 kg'lık söndürücülerin doğru şekilde kullanılması ile öngörülenden daha büyük yangınları söndürmek mümkündür. Ancak bilinçsiz kullanımlarda, taşınabilir yangın söndürücü içerisinde bulunan söndürücü madde,

sadece birkaç saniyede tamamen boşalabilir. Bu nedenle, çalışanlara yangın güvenliği eğitimleri verilmeli, eğitimler sırasında taşınabilir yangın söndürücülerin kullanımı ve çalışma mantığı da öğretilmelidir.

BT bileşenleri ve altyapı ekipmanlarına ciddi oranda hasar verebileceği için yangın sınıfları A (katı maddeler), B (yanıcı sıvılar) ve C (gazlar) olan, yangın söndürme maddesi olarak toz kullanan yangın söndürücülerin, özellikle veri merkezleri ve altyapı ekipmanlarını barındıran alanlarda kullanılmaması önerilir. Bu tip alanlarda sadece insan sağlığını tehdit etmeyecek, yangın söndürme maddesi olarak gaz içeren yangın söndürücülerin kullanılması sağlanmalıdır.

Taşınabilir yangın söndürücülerin düzenli kontrol ve bakımı TS 11748 standardına göre yapılabilir. Yangın söndürme cihazlarının doldurulmasını ve bakımını yapan üretici veya servis firmaları Sanayi ve Ticaret Bakanlığı tarafından dolum ve servis yeterlilik belgesine sahip olmalıdır. Yangın söndürücü üzerinde yer alan bir etikette, yangın söndürücü cinsi, gaz tipi, ağırlığı, doldurulduğu tarih, bulunacağı yer, sorumlu kişi, aylık kontrol tarihi ve imza gibi bilgiler yer almalıdır. Yangın söndürücülerin aylık rutin genel durum kontrolleri yanı sıra, altı ayda bir gaz ağırlık ölçümleri, yılda bir söndürücü madde nitelik kontrolleri, beşer yılda bir tüp niteliği kontrolleri düzenlenmesi önerilir. Ayrıca, bu tür düzenli denetimler sırasında özel erişim kısıtlamaları bulunan alanlardaki yangın söndürücülerin unutulmaması da önemlidir.

VRM.1.U6 Kapalı pencereler ve kapılar [Personel]

Bina içerisinde yer alan odaların dışa bakan pencereleri ve dışa açılan kapıları (balkonlar, teraslar), odalar kullanılmadığı zamanlarda kapalı tutulmalıdır. Dış kapılar kilitlenmelidir. Binanın zemin katı ve cephe tasarımına bağlı olarak, üst katlarda bulunan açık pencereler ve kapılar, bir kurumun çalışma saatleri içerisinde dahi hırsızlar için ideal giriş noktaları olarak kullanılabilir.

Bina içerisinde çalışan kişiler, mesaileri sona erdiğinde, açık pencerelerin ve kapıların kapatılması gerektiğini bilmelidirler. Mesai saatleri içerisinde, odanın çalışanlar tarafından uzun süreli kullanılmaması durumunda da açık pencerelerin ve kapıların kapalı tutulması ve kilitlenmesi önerilmektedir.

Özellikle bina içerisinde yer alan yangın ve duman koruma kapıları için hiç bir istisna uygulanmamalıdır. Bu tür kapılar, sadece kapalı haldeyken koruma sağlar ve bu nedenle asla açık kalmamalı veya her hangi bir çalışma/uygulama için açık tutulmamalıdır. (bkz. "VRM.1.U3 Yangın güvenliği yönetmeliklerine uyulması").

Odayı terk eden son kişi (veya varsa bina içerisinde bulunan güvenlik görevlileri), pencerelerin ve kapıların kapalı olup olmadığını kontrol etmelidir. Ayrıca kritik odaların (örneğin veri merkezi, altyapı ekipmanlarının barındırıldığı odalar, vb.) pencereleri ve kapıları belirli aralıklar ile kontrol edilmelidir.

VRM.1.U7 Güvenlik ve Erişim Kontrolü [Organizasyon Yöneticisi]

Bina içerisinde koruma gerektiren alanlara ve odalara erişim düzenlenmeli ve kontrol altında tutulmalıdır. Bu amaçla eski tip anahtarlardan, bireysel kimlik kartları kullanmaya kadar bir çok farklı uygulamadan yararlanılabilir.

Erişim kontrolü için:

- Kontrol edilecek alan açıkça belirlenmeli,
- Erişim hakkına sahip kişilerin sayısı asgari düzeye indirilmeli; bu kişilerin (yetkisiz kişileri belirlenebilmesi için) birbirlerinin yetkilerini bilmesi sağlanmalı,
- Diğer kişilerin (ziyaretçilerin) alan içerisine kabulü ancak gerekliliğin önceden incelenmesinden sonra gerçekleşmeli,
- Erişim izni kayıt altına alınmalıdır.

Tüm kritik alanlara erişim hakkına sahip kişi sayısının asgari düzeyde tutulması, sadece görev tanımları gereği kişilerin ilgili alanlara erişimlerinin sağlanması önerilir. Ayrıca verilen yetkilerin uygunluğu da (örneğin kişilere aşırı yetki verilip verilmediği) kontrol edilmelidir. Erişim kontrol sisteminin tasarımında, basit ve uygulanabilir çözümler çoğunlukla pahalı teknoloji kadar etkili olabilmektedir. Bu düşünceyle aşağıda yer alan temel faaliyetlerin gerçekleştirilmesi tavsiye edilmektedir:

- Erişim izni verilen kişilerin bilgilendirilmesi,
- Erişim kontrolü konusunda kurum içi farkındalığın artırılması,
- İzin değişikliklerinin duyurulması,
- Çalışan ve ziyaretçi kimlik kartları kullanılması,
- Ziyaretçilere refakat edilmesi,
- Yetkilendirme ihlalinin tespit edilmesi durumunda yapılacakların belirlenmesi,
- Yetkisiz kişiler için erişimin kısıtlanması.

Erişim kontrolü, çeşitli mimari, organizasyonel ve personel ile ilgili önlemlerin alınmasını gerektirebilir. Bu farklı konularda alınması gereken önlemlerin birbirleriyle etkileşimleri; çevre, bina ve ekipman koruması için genel talimatları tanımlayan bir erişim kontrol prosedürü hazırlanması önerilmektedir. Erişim kontrol prosedürü içerisinde:

- Korunacak bölgeler tanımlanmalı (yerleşke, bina, sistem odası, BT bileşenleri, altyapı ekipmanları, arşiv odası, iletişim ekipmanlarının bulunduğu odalar, vb.),

farklı güvenlik gereksinimlerine sahip bölgeler için güvenlik bölgeleri oluşturulmalı (bkz. "VRM.1.U22 Güvenlik bölgelerinin oluşturulması"),

- Erişim yetkileri atanmalı,
- Erişim kontrolünden sorumlu bir kişi belirlenmeli; bu kişinin, kurum bilgi güvenliği politikasında tanımlanan ilkelere göre çalışanlara erişim haklarını tayin etmesi sağlanmalı,
- Zaman bağımlılıkları tanımlanmalı; erişim haklarıyla ilgili zaman kısıtlamaları gerekip gerekmediği açıklığa kavuşturulmalı (örneğin yalnızca çalışma saatleri içinde erişim, günde bir kez erişme veya belirli bir tarihe kadar geçici erişim gibi),
- Korunan bölgeye girerken ve çıkarken hangi verilerin kaydedileceği belirlenmeli; kurum güvenlik hedefleri ile kişisel verinin korunumu arasında bir denge oluşturulmalı,
- İstisnai durumlarda bile, yetkisiz kişilerin bina veya odalara girememesi sağlanmalıdır.

Bunlara ek olarak, bina içerisinde farklı kilitlerin ve kart okuyucularının kurulumu yararlı olabilir. Kilitler ve anahtarlar ile ilgili ayrıntılı bilgi " VRM.1.U11 Anahtar/kilit yönetimi" içerisinde bulunmaktadır.

Bina ve içerisinde yer alan güvenlikli bölgelere erişimi tam anlamıyla kontrol altına alabilmek için BT tabanlı bir yetkilendirme yönetim sistemi kurulabilir. Bu sistem aracılığı ile daha kapsamlı bir model oluşturularak, kullanımda esneklik, doğrulanabilirlik ve şeffaflık sağlanabilir.

Erişim kontrolü için kullanılan terminallerin her türlü kötü niyetli kullanıma karşı (manipülasyon, zorlama, vb.) korunması sağlanmalıdır. Kişiye ait kimlik bilgilerinin (kullanıcı adı, parola, PIN, vb.) girişi yapılırken, gizlilik garanti edilmeli, veri girişinin güvenli bir şekilde gerçekleştirilmesi sağlanmalıdır (örneğin PIN girişi için erişim kontrol terminali üzerinde bir tuş takımının bulunması beklenir).

Kimlik bilgileri, erişim kontrol terminaline bağlı olmayan bir cihaz aracılığı ile sağlanıyorsa, veri girişi yapılan cihaz ile erişim kontrol terminali arasındaki veri iletiminin şifreli olarak gerçekleşmesi sağlanmalıdır (örneğin temassız kart kullanılan durumlarda, kart okuyucu ve erişim kontrol terminali arasındaki veri iletimi şifreli bir biçimde gerçekleşmelidir).

Belirli aralıklar ile erişim kontrolünün kullanımına ilişkin düzenlemelere uyulup uyulmadığı, uygulanan tüm teknik ve organizasyonel erişim kontrolü önlemlerinin etkinliği kontrol edilmelidir. Özellikle sorunlu olabilecek bölgelerde, erişim kontrolünün kesintiye uğrayıp uğramadığının düzenli olarak izlenmesi tavsiye edilir (örneğin malzeme teslim alanları, sigara içilen alanlar, vb.).

2.2 2. SEVİYE UYGULAMALAR

1.seviye uygulamalar sonrasında, binaların durumlarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar, aşağıdaki uygulama maddelerini dikkate alarak, iyileştirme/geliştirme faaliyetlerini planlayabilirler.

VRM.1.U8 Binanın fiziksel güvenlik çerçevesi [Bina Hizmetleri Yöneticisi, Planlama Sorumlusu, Bilgi Güvenliği Sorumlusu]

Etkili bir bina kullanımı güvenlik konsepti oluşturmak için öncelikle, bir bina içinde gerçekleştirilen iş süreçlerine ilişkin koruma gereksinimlerinin belirlenmesi ve işletme faaliyetinden kaynaklanan temel koruma hedeflerinin tanımlanması gerekir. Sonrasında geliştirilecek güvenlik konsepti (modeli) içerisinde genel koruma hedefleri, kurum için değerli varlıkların, kritik odaların ve alanların, personelin korunmasına yönelik önlemler ile birlikte erişim kontrolü, yangın koruma, altyapı güvenliğini sağlama gibi unsurlar yer almalıdır.

Korunması gereken bölgelere yetkisiz kişilerin girememesi için tüm erişimlerin kontrol ve güvence altına alınması sağlanmalıdır. Yetkisiz girişlerin kontrolü ilave tedbirlerle desteklenebilir ("VRM.1.U26 Hırsızlığa Karşı Koruma" ya bakınız).

Bina kamuya açık veya yarı kamusal alanlara sahipse ya da dışarıya bakan pencereler aracılığıyla bina içi görülebiliyorsa, " VRM.1.U15 Korunma gerektiren bina bölümlerine ilişkin konum/tabela bilgilendirilmelerinden kaçınma " uygulamasından yararlanılmalıdır.

Binanın korunması gereken bölgelerinde su sızıntılarına karşı önlemlerin alınması da düşünmelidir. Bu konuyla ilgili bilgi " VRM.1.U23 Otomatik drenaj" uygulama maddesinden edinilebilir.

Binaya ve bina içerisinde yer alan alanlara yönelik tehlikelerin belirlenmesi, bu tehlikelere yönelik gerekli önlemlerin alınması, kurulacak bir alarm sistemi ile sistematik bir şekilde izlemenin gerçekleştirilmesi ve sonrasında belirlenen ihlalleri giderici ve önleyici faaliyetlerin uygulanması bina kullanımı güvenlik konseptini tamamlayıcı hususlar olarak düşünülmelidir.

Bina kullanımı güvenlik konsepti, kurumun genel güvenlik konseptine uygun olmalıdır. Özellikle binanın kullanımında değişiklikler olması durumunda bina kullanımı güvenlik konseptinin de güncellenmesi sağlanmalıdır.

VRM.1.U9 Uygulanabilir standartlara ve düzenlemelere uyum [Yüklenici, Bina Hizmetleri Yöneticisi]

Teknolojinin hemen hemen tüm alanlarına yönelik kurallar, standartlar ve düzenlemeler bulunmaktadır. ISO, DIN, TSE bu tür standartlar üreten kurumlara örnek olarak verilebilir. Bu tür kurumlar tarafından hazırlanmış standartlar dışında ilgili kamu kurumlarınca yayınlanmış ve yürürlüğe konulmuş yönetmelikler veya düzenlemeler de bulunmaktadır. Bu kurallar, kurumların veri merkezlerinin, BT bileşenlerinin, etkin, verimli ve güvenli bir biçimde kurulabilmesi ve işletilebilmesi için yardımcı olur.

Fakat günümüzde kurumların sadece standarda uymuş olmak, ilgili belgeyi (sertifikayı) alabilmek için, madde madde standartlara uyum sağlamaya çalıştıkları, kendilerini standarda uyuyormuş gibi gösterdikleri gözlenmektedir. Bu tür bir yaklaşımın her zaman etkin, verimli ve güvenli bir çalışmayı garanti altına alamayacağı bilinmelidir. Bununla birlikte, standartlar içerisinde yer alan maddelerin kurum içerisinde uygulanması son derece sağlam bir temel oluşturabilmektedir. Binaların planlanması, inşa edilmesi, işletilmesi ve yenilenmesi sırasında; bina içerisinde yer alacak BT bileşenlerinin ve altyapı ekipmanlarının kurulumu, inşa edilmesi, işletilmesi ve yenilenmesi sırasında ilgili tüm standartların ve düzenlemelerin dikkate alınması önerilir.

VRM.1.U10 Kapıların kilitlenmesi [Personel]

Çalışma saatleri dışında, boşaltılan odaların kapıları kilitlenmeli, yetkisiz kişilerin oda içerisinde yer alan belgelere ve BT bileşenlerine erişimi önlenmelidir. Özellikle kamu erişimine açık alanlarda bulunan veya erişim kontrolü sağlama olanağı bulunmayan, bireysel olarak kullanılan ofislerin kilitlenmesi önemlidir.

Oda kapıları dışarıdan sadece uygun anahtar ile açılabiliyor ise kapının ayrıca kilitlenmesi gerekli değildir. Bu durumda yetkili çalışanların anahtarlarını daima yanında taşımaları sağlanmalıdır.

Oda veya çalışma alanlarında da kaçış kapıları bulunabilir. Kaçış kapılarının, içeride çalışanlar olduğu sürece içeride bulunan herkes tarafından açılması mümkün olmalıdır. Oda ile dış ortam arasında direk bağlantı kuran bu tür kapıların, dışarıdan içeriye yetkisiz erişimleri önleyecek şekilde korunmaları gerekir.

Açık ofis gibi bazı alanlarda ofislerin kilitlenmesi çok mümkün değildir. Bu durumda, her çalışanın kendine ait belgeleri ("Temiz masa" politikası ile ortada hiç bir kritik belge bırakmamak, belgeleri kilitli bir dolapta tutmak) kendi kullanmakta olduğu BT bileşenlerini (“Temiz ekran” politikası ile bilgisayarın kullanılmadığı zamanlarda kilitli olmasını sağlamak) ve diğer ekipmanları (masa, telefon, vb.) güvence altına alması gerekmektedir.

Toplantı, etkinlik ve eğitim salonlarında yer alan belgeleri, BT bileşenlerini, altyapı ekipmanlarını vb. korumak daha zordur. Bu nedenle en azından toplantılar ve etkinlikler sonrasında söz konusu alanların kontrol edilmesi sağlanmalıdır.

İçerisinde korunma ihtiyacı olan varlıkların yer almadığı odaların kilitli tutulması gerekmemektedir. Benzer şekilde içerisinde ancak bir kimlik doğrulama sonrasında kullanılabilecek bilgisayarların bulunduğu odaların da sürekli kilitli tutulması gerekli değildir.

Bina içerisinde çalışanlar, çalışma saatleri dışında ofis kapılarını kapatmaları ve masalarındaki belgeleri güvenli olarak saklamaları hususunda bilgilendirilmelidirler. Çalışanların bu uygulamaya uyumlulukları belirli aralıklarla kontrol edilmelidir. Ayrıca bina güvenlik görevlileri veya bu konuda yetkilendirilmiş çalışanlar tarafından, çalışma saatleri dışında odaların kilitli olduğuna, önemli belgelerin güvenli bir şekilde saklandığına (bilgisayarlarda kullanıcı oturumlarının sonlandırıldığına veya bilgisayarın kapatıldığına) ilişkin kontroller gerçekleştirilmelidir.

VRM.1.U11 Anahtar/kilit yönetimi

Binanın tüm anahtarları (katlar, koridorlar ve odalar) için bir kilitleme planı oluşturulmalıdır. Anahtarların üretimi, saklanması, yönetimi ve yetkili kişilere verilmesi merkezi olarak düzenlenmelidir. Yedek anahtarlar güvenli bir şekilde saklanmalıdır. Benzer yaklaşım, manyetik kartlar veya akıllı kartlar gibi tüm kimlik araçları için de uygulanmalıdır. Aşağıdaki hususlara dikkat edilmesi önerilir:

- Özel koruma gerektiren yüksek güvenlikli alanlara giriş için, farklı anahtarların birlikte kullanılmasıyla kilidin açılabileceği bir sistem kurulmalı, kilidi açacak her anahtar yetkilendirilmiş farklı kişilere verilmelidir. Bu tür yüksek güvenlikli alanların ancak anahtara sahip yetkili kişilerin bir araya gelmesi ile açılabilmesi sağlanmalıdır.
- Çalışanlara tahsis edilmeyen ve yedek tutulan anahtarlar yetkisiz erişime karşı korunmalıdır.
- Kilitli alanlara giriş için gerekli olan anahtarlar, sadece görevi gereği alana giriş yetkisi olan kişilere verilmeli ve kayıt altına alınmalıdır.
- Anahtarın kaybedilmesi durumunda (kaybın bildirimi, anahtarın değişimi, masrafların karşılanması, kilidin değiştirilmesi, kilitleme gruplarının değiştirilmesi, vb. gibi) gerekli düzenlemeler gerçekleştirilmelidir.
- Çalışan rolünün veya sorumluluğunun değişmesi durumunda, giriş yetkileri kontrol edilmeli ve kişiye gerekli olmayan anahtarlar geri alınmalıdır.

- Çalışanın kurumdaki (veya binadaki) görevinden ayrılması durumunda, kendisinde bulunan tüm anahtarlar geri alınmalıdır (görevden ayrılmadan önce tamamlanması gereken mevzuat içerisinde erişim haklarının iptaline de yer verilmelidir).
- Özel koruma gerektiren alanlarda, yetkisiz erişimden şüphelenilmesi durumunda, bu alanlarda yer alan kilitlerin ve alanlara giriş için kullanılan anahtarların değiştirilmesi sağlanmalıdır.

VRM.1.U12 Dağıtım panolarına erişimle ilgili düzenlemeler

Bina içerisinde yer alan dağıtım panolarının (elektrik panosu, ağ ve telefon panoları, vb.) altyapı ekipmanlarının yer aldığı odalarda barındırılması önerilir. Özellikle kamuya açık alanlarda dağıtım panoların bulundurulmaması gerekir.

Bir binadaki tüm iletim hatlarının ilgili dağıtım panolarına (elektrik, su, gaz, telefon, alarm sistemi vb.) erişimi düzenlenmelidir. Ayrıca:

- Panolar boya veya duvar kâğıtlarıyla görünmez kılınmamalı,
- Panoların önünde mobilya, ekipman, palet vb. ile engeller oluşturulmamalı,
- Anahtarlı panoların anahtarları yetkili kişilerce ulaşılabilir tutulmalı ve kilitlerinin çalışır olup olmadığı düzenli aralıklarla kontrol edilmelidir.

Dağıtım panolarını açabilecek kişiler ilgili hizmetten sorumlu kişiler arasından belirlenmeli ve tanımlanmış olmalıdır. Panolar kilitli tutulmalı ve yalnızca ilgili hizmetten sorumlu belirlenmiş kişiler tarafından açılmalıdır.

Elektrik panoları içerisinde bulunan sigortalar güç kaynağı şebekesinin dağıtıcılarına monte edilmişse, uygun yedek sigortalar bulunmalıdır. Elektrik panolarının kullanımına ilişkin ayrıntılı bilgi, Elektrik Kablolama rehberi içerisinde bulunmaktadır.

Tüm dağıtım panoları içerisinde etiketler kullanılmalı, pano içi düzenlemelerin yetkili kişiler tarafından anlaşılır olması sağlanmalıdır.

VRM.1.U13 Yıldırımdan korunma cihazları

Olası bir yıldırımın binaya doğrudan verebileceği hasarlar (bina yapısına zarar, yangın çıkması, vb.), uygun bir yıldırımdan korunma sistemi ile mümkün olduğunca önlenebilir. Bununla birlikte, binadaki mevcut elektrik tesisatının ve ekipmanlarının yıldırım ve diğer etkilerden daha iyi korunabilmesi için aşırı voltaj koruması da gereklidir (bkz. "Elektrik kabloları rehberi").

Bu tür cihazlar ile ilgili çeşitli standartlar bulunmaktadır. ISO 62305, IEC 61643-11, IEC 60634, UL 1449 bunlardan bir kısmıdır. Türkiye'de TS EN 62305-1/2/3/4 standardı yıldırıma karşı korunmanın sağlanması için genel kuralları açıklar.

Standardın ikinci bölümü olan “Risk Yönetimi” yıldırım ve yıldırım sonucunda oluşabilecek elektriksel dalgalanmaların önlenmesinde risk odaklı bir yaklaşım sunmaktadır. Üçüncü bölüm, yapıların ve kişilerin korunması yani harici yıldırımdan korunma ile ilgilidir. Harici yıldırımdan korunma, yıldırım iletkeni, özellikleri bakımından dört koruma sınıfına (kısaca Yıldırımdan Koruma Seviyesi) ayrılmıştır. Koruma sınıfı-1 en iyi koruma sağlarken, Koruma sınıfı-4 en düşük koruma değerine sahiptir. Söz konusu dört koruma sınıfı arasındaki kolayca ayırt edilebilen fark, yıldırım yakalama genişlik mesafeleridir. Kapsamlı bilişim donanımına sahip binalar için yıldırım koruma cihazlarının, en azından TS EN 62305 standardı Koruma sınıfı-2'ye uyacak şekilde yapılandırılması önerilmektedir.

Alıcı cihazdan geçen yıldırım akımı, en üst şimşek noktasından en alt topraklama noktası boyunca düşen gerilim ile devam eder. Yakalama cihazının en üst noktasında gerilim birkaç yüz bin volta kadar çıkabilir. Bu nedenle, özellikle bir binanın üst katlarında bulunan tesisatların (veri kablolama, elektrik kablolama, su boruları, vb.), yakalama cihazlarından yeterli uzaklığa sahip olması gerektiğine dikkat edilmelidir. Ayrıca bu özellik standartlarda “ayırma mesafesi” olarak kabul edilmektedir.

Yıldırımdan korunma sistemi düzenli olarak kontrol edilmelidir. Yıldırım koruma cihazları yılda bir kez görsel olarak incelenmeli ve her iki yılda bir işlevsellikleri tam olarak test edilmelidir. Güvenlik ve kullanılabilirlik seviyeleri yüksek tesisler için kapsamlı bir denetimin her yıl gerçekleştirilmesi önerilmektedir. Denetimler sırasında tespit edilen eksiklikler, kusurlar giderilmeli, tüm denetim faaliyetleri, elde edilen bulgular, gerçekleştirilen düzeltme faaliyetleri kayıt altına alınmalıdır.

VRM.1.U14 Altyapı tesisat hatlarının yerleşim planları

Bina içerisinde (ve çevresinde) yer alan tesisat hatlarına ilişkin detaylı bilgileri içeren yerleşim planları hazırlanmalıdır. Yerleşim planları aracılığı ile tesisat hatları (elektrik, su, gaz, telefon, iklimlendirme, vb.) görsel bir biçimde, açıklayıcı olarak tanımlanmaktadır. Tesisat hatlarına ilişkin doğru ve güncel yerleşim planları sayesinde, gerçekleştirilecek çalışmalar öncesinde yapılabilecek bir takım hazırlıklar ile hatların zarar görmeleri engellenebilir, hasar durumunda nasıl/nereye müdahale edilebileceği hızlı ve kolay şekilde belirlenebilir. Bu nedenle, tüm tesisat hatlarının doğru ve güncel haritaları binada ve ilgili yerleşkede tutulmalıdır. Yerleşim planları içerisinde:

- Hat yolları ve yönlendirmeleri (kat ve yer planlarında işaretleme),
- Detaylı teknik veriler (tip ve ölçümler),
- Hat kullanımları, bağlı olan ağların adlandırılması,
- Tehlikeli olabilecek noktalar,

- Mevcut güvenlik önlemleri, değerlendirilmesi gereken koruma önlemleri bulunması önerilir.

Tesisat planlarını güncelleyecek kişiler/ekipler önceden belirlenmeli ve tesisat planlarının herhangi bir değişiklik/yenilik sonrası güncellenmesi sağlanmalıdır. Planlar, yalnızca yetkili kişilerin erişebileceği şekilde muhafaza edilmeli ve ihtiyaç duyulduğunda hızlı bir şekilde kullanılabilir halde tutulmalıdır.

VRM.1.U15 Korunma gerektiren bina bölümlerine ilişkin konum/tabela bilgilendirilmelerinden kaçınma

Her binada farklı amaçlar için kullanılan ve farklı koruma ihtiyaçlarına sahip alanlar bulunmaktadır. Korumaya değer bina bölümleri arasında veri merkezi, veri disk arşivi, iklimlendirme kontrol merkezi, elektrik panoları, yedek parça depoları, vb. gösterilebilir.

Bu gibi alanların kullanımlarına dair bilgilendirme veya yönlendirme tabelaları (örneğin VERİ MERKEZİ veya ARŞİV gibi kapı tabelaları) binaya erişen kötü niyetli kişilere değerli varlıklarının nerede olduğuna dair ipuçları vermektedir. Bu yüzden binanın özel koruma gerektiren bölümlerinde (veri merkezi, sunucu odası, vb.), bu bölümleri açığa çıkaracak bir biçimde gösterge/tabela kullanılmasından kaçınılmalıdır. Ayrıca bu bölümlerin gerek içeriden gerekse dışarıdan kolay bir biçimde görülmesi engellenmelidir.

VRM.1.U16 Dumandan koruma [Planlama Sorumlusu]

Yangında meydana gelen can ve mal kayıplarının önemli sebeplerinden biri de dumandır. Ölümlerin %90'dan fazlasının duman sebebiyle (zehirlenme) gerçekleştiği gözlenmektedir. Duman içeriğindeki zehirli maddeler ve gazlar doğrudan hayatı tehdit etmekte, bünyesindeki diğer katı ve sıvı tanecikler de BT bileşenleri üzerinde çeşitli hasarlara yol açmaktadır. Bu nedenle, bina içerisinde kapsamlı duman korumasına önem verilmelidir.

Dumandan koruma için aşağıdaki maddelerin dikkate alınması tavsiye edilmektedir:

- Yangın kapıları dumana karşı dayanıklı olmalıdır.
- Koridorlarda bulunan duman kapılarının duman detektörleri ile kontrol edilmesi sağlanmalıdır. Böylelikle her zaman açık olabilen bu tür kapıların, duman tespit edildiğinde otomatik olarak kapatılması mümkün olacaktır.
- BT bileşenlerinin barındırıldığı odalarda, hızlı duman tahliyesi için duman tahliye sistemleri kurulmalıdır.
- İklimlendirme sistemi tarafından kullanılan havalandırma kanallarına (hava koridorları) kanal dedektörleri takılmalıdır. Bu dedektörler sayesinde, temiz hava girişinde herhangi bir sorun (duman) tespit edildiğinde otomatik olarak iklimlendirme sisteminin kilitlenmesi sağlanmalıdır.

Yapısal duman koruması, her türlü kurulum ve dönüştürme çalışması sonrası gözden geçirilmelidir.

Çalışanlar duman koruma sistemleri tarafından üretilen uyarı mesajları (örneğin hangi mesajın ne anlama geldiği bilinmeli) hakkında ve uyarı mesajı sonrası nasıl hareket edilmesi gerektiği ile ilgili önceden bilgilendirilmelidir.

Belirli aralıklar ile düzenlenen testler/tatbikatlar aracılığıyla duman koruma bileşenlerinin işlevleri kontrol edilmelidir.

VRM.1.U17 Yangın güvenlik kontrolleri

Bina bünyesinde alınmış yangın önlemlerinin kontrolünü sağlamak amacıyla, düzenli aralıklarla (yılda en az bir veya iki kez olmak üzere) yangın önleme denetimlerinin gerçekleştirilmesi önerilir. Yangın önleme denetimleri ile önleyici yangın korumasında zayıf noktaların ortaya çıkarılması ve önleyici tedbirlerin nasıl uygulanabileceği konusunda farkındalık oluşturulması hedeflenir.

Kamu kurumlarına ait bir çok binada, belirlenmiş depoların ve alanların dışında yanıcı veya patlayıcı maddelerin toplanmakta olduğu, teknik/sistem odaları içinde kağıt malzemelerin veya mobilyaların tutulduğu gözlenmektedir. Yangın önleme denetimlerinde bu gibi konulara odaklanılması önerilmektedir. Duman dedektörlerinin çalışıp çalışmadığı; yangın bölmesi veya duman kontrol kapılarının açık tutulup tutulmadığı; yangın bariyerlerinin çalışma sonrası açık tutulup tutulmadığı ve çalışma sırasında hasar görüp görmedikleri, hasar sonrası düzgün bir şekilde eski haline getirilip getirilmedikleri yangın önleme denetimlerinde kontrol edilmelidir.

Denetimler sırasında ortaya çıkan bulgular kayıt altına alınmalı ve eksikliklerin, kusurların hızlı bir biçimde düzeltilmesi sağlanmalıdır. Ortaya çıkan bulgular sonrasında acil durum sorumlusu koordinasyonunda, yangın önleme tedbirlerinin alınması, düzgün bir biçimde işletilmesi, gerektiğinde güncellenmesi ve kontrol edilmesi sağlanmalıdır.

VRM.1.U18 Acil durum sorumlusunun zamanında bilgilendirilmesi

Kurum içerisinde yangın önlemleri ile ilgili en yetkili kişi olan acil durum sorumlusu, tesisat hattı güzergâhları, koridorlar, kaçış ve kurtarma güzergâhları üzerinde gerçekleştirilecek çalışmalara ilişkin detaylı bilginin çalışma öncesinde aktarılması gereklidir. Acil durum sorumlusuna zamanında bilgi verilmesi ile bu kişinin yangından korunma önlemlerinin düzgün yürütülüp yürütülmediğini kontrol edebilmesi veya devam eden işler sırasında bile inşaat ilerlemeden gerekli kontrollerin yapılmasını sağlaması mümkün olabilecektir.

Gerekli tesisat güzergahlarının, koridorların, kaçış ve kurtarma yollarının yanı sıra, duvarların içinde yer alan boru ve kablo kanallarında gerçekleştirilecek tüm çalışmalar ile

ilgili de yangın koruma görevlisinin bilgilendirilmesi önerilir. Çalışma öncesi yapılacak bu tür bir bilgilendirme ile acil durum sorumlusu, önleyici yangın korumasının işin uygulamasına dahil edilebilmesini sağlayabilecektir.

Acil durum sorumlusunun bu tür çalışmalara katılımı, çalışmalar öncesinde hazırlanan inşaat projesinin planlama ve kabul belgelerinin acil durum sorumlusu tarafından (yangın önlemleri açısından) değerlendirilmesi önerilmektedir. Çalışma kapsamında, acil durum sorumlusu koordinasyonunda, yangın önleme tedbirlerinin alınması, düzgün bir biçimde işletilmesi, gerektiğinde güncellenmesi ve kontrol edilmesi sağlanmalıdır.

VRM.1.U19 Acil durum planı ve yangın tatbikatları

Yangın durumunda alınması gereken önlemler, bir alarm planı içerisinde yazılı hale getirilmelidir. Böyle bir plan içerisinde:

- Hangi olaylar karşısında ne tip önlemlerin alınacağı,
- Bina tahliyesinin gerekip gerekmediği, gerekiyorsa tahliyenin nasıl gerçekleştirileceği,
- Böyle bir durumda kimlerin bilgilendirileceği,
- Hangi destek personeline ve acil servise (itfaiye, hastane, polis, vb.) bilgi verileceği,
- Yangın durumunda çalışanlardan beklenen davranış biçimleri gibi bilgilerin yer alması önerilmektedir.

Hazırlanan alarm planının yayınlanması, tüm çalışanlara duyurulması sağlanmalıdır.

Bununla birlikte, en iyi alarm planı bile içerisinde yer alan önlemler doğru ve uygulanabilir değilse çok faydalı olmayacaktır. Bu nedenle, alarm planının uygulanabilirliğinin düzenli olarak kontrol edilmesi ve gerekli durumlarda alarm planının güncellenmesi gereklidir.

Alarm planının kontrolü sırasında, yararlanılan yöntemlerden biri de yangın tatbikatlarıdır. Birçok kurumda düzenli yangın tatbikatlarının gerçekleştirilmediği, yangın tatbikatlarının gerçekleştirildiği kurumlarda ise örneğin çalışanların yangın söndürücünün nerede olduğu, nasıl kullanılacağı konusunda bilgi sahibi olmadıkları; kaçış yolunun neresi olduğunu, en yakın merdiveni, çıkış kapılarının yerlerini bilmedikleri gözlenmektedir. Hatta kimi çalışanların, tatbikat sırasında normal çalışmalarına devam ettikleri, tatbikatı göz ardı ettikleri de bilinmektedir. Acil durumlarda bu tip bilgi yetersizliği felaket ile sonuçlanabilir.

Özellikle yangın güvenliği tatbikatlarında insan hayatının ve BT bileşenlerinin korunması için doğru davranış eğitimlerinin verilmesi sağlanmalıdır. Bu tür tatbikatların uygulanması için öncelikle yetkili makamlar veya şirket üst yönetimi ile anlaşmaya varılmalı, tatbikat sonuçları üst yönetime raporlanmalıdır.

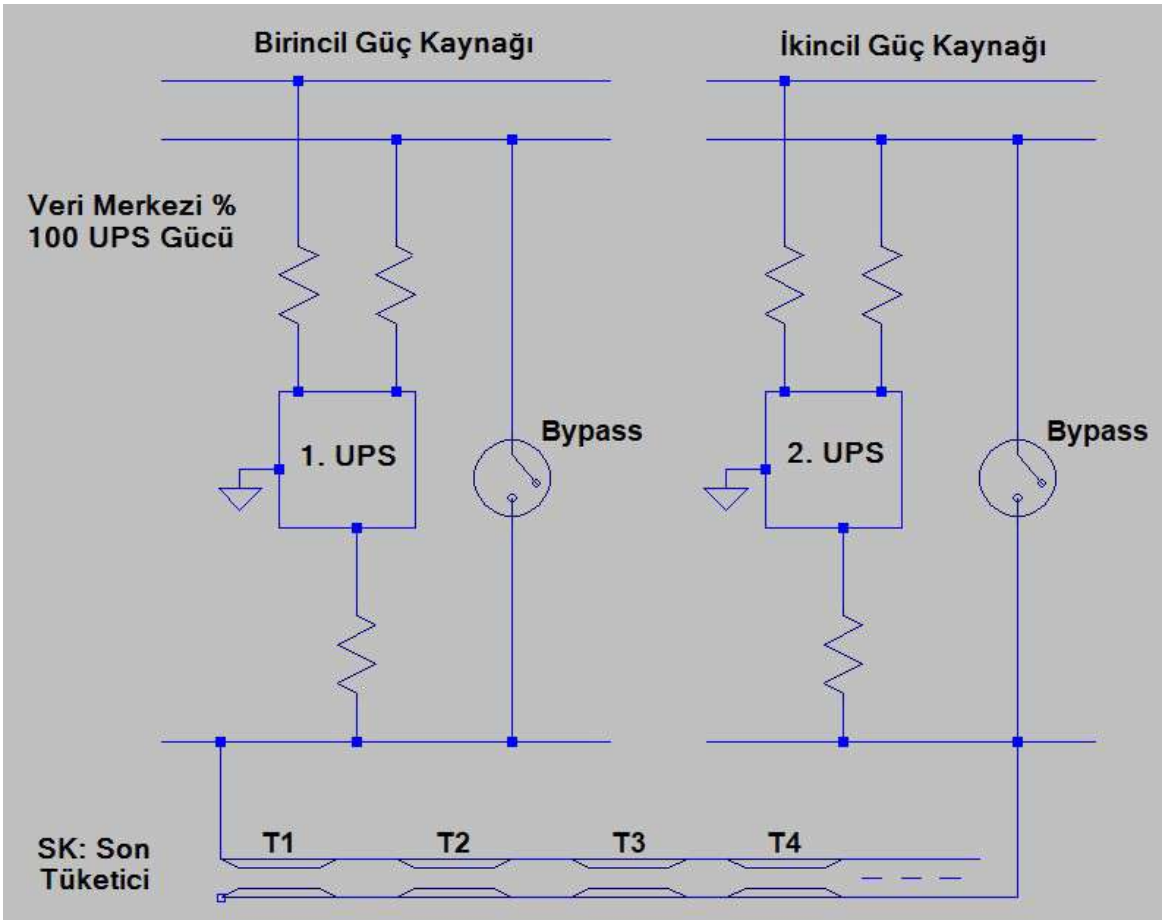
2.3 3. SEVİYE UYGULAMALAR

1. ve 2. seviye uygulamalar sonrasında, binalar için artan koruma koşullarında dikkate alınması gereken uygulamalar aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda, risk analizi çerçevesinde uygun uygulamalardan faydalanmaları önerilir. Uygulama kapsamında öncelikli koruma sağlanan prensip parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.1.U20 Bağımsız elektrik hatları üzerinden beslenme (E)

Kurumun yüksek erişilebilirlik gereksinimleri doğrultusunda, bina içerisinde bulunan (genellikle veri merkezi içerisinde barındırılan) kritik BT bileşenlerinin iki bağımsız elektrik hattı üzerinden beslenmesi sağlanmalıdır.

İmkânların uygun olması durumunda, kurum için kritik BT bileşenlerinin (merkezi depolama bileşenleri, merkezi ağ cihazları veya kritik sunucular) aşağıda yer alan çizimde gösterildiği şekilde iki farklı elektrik hattı üzerinden, birbirinden bağımsız iki farkı güç kaynağından beslenmesi önerilir. Bu sayede herhangi bir güç kaynağında sıkıntı yaşanması durumunda, diğer güç kaynağı kritik BT bileşenlerine enerji sağlamaya devam edebilecektir. Kritik olmayan BT bileşenleri tek güç kaynağından beslenebilir.



Şekil 9. Bağımsız elektrik hatları

Ayrıca düzenli olarak, kritik BT bileşenlerinin güç kaynağı besleme bağlantılarının doğru olup olmadıklarının, bir elektrik hattında sorun yaşanması durumunda diğer hat üzerinden elektrik iletiminin devam edip etmeyeceğinin kontrol edilmesi önerilmektedir.

VRM.1.U21 Güvenli Kapılar ve Pencereler (GBE)

Farklı güvenlik gereksinimine sahip bölgeler arasında geçiş sağlayan kapılar ve pencereler yeterli korumayı sağlayacak şekilde seçilmelidir. Örneğin; harici kapılarda hırsızlıklara karşı korunma önlemleri alınmalı ve dışarıdan erişilebilir durumda olan pencereler sağlamlaştırılmalıdır. Bina içinde yer alan, yangın bölmesi sınırını oluşturan kapıların ateşe dayanıklı olması, güvenli olması gereken iç bölge için ikinci bir hırsızlık koruması hattı oluşturması önerilmektedir.

Güvenli kapılar ve pencereler için birçok farklı standart bulunmaktadır. Bina içerisinde korunacak alanın koruma hedeflerine ve kurumun koruma ihtiyaçlarına göre uygun standardın belirlenmesi ve belirlenen standarda uygun kapı ve pencere seçilmesi gerekmektedir.

TS EN 1627 standardı kapılar, pencereler, giydirme cepheler, korkuluklar ve panjurların hırsızlığa karşı direnç özelliklerine dair kuralları ve sınıflandırmayı kapsamaktadır. Kapılar hırsızlığa karşı gösterecekleri direnç ve dayanıklılığa göre altı sınıfta (güvenlik sınıfı 1 en düşük güvenlik seviyesi, güvenlik sınıfı 6 en yüksek güvenlik seviyesi olacak şekilde) derecelendirilirler. Güvenlik sınıfı 3 ve üzeri kapılar sağlamlıklarından dolayı hırsızlığa karşı daha yüksek koruma sağlarlar.

Kendiliğinden kapanan yangın geciktirici ve duman geçirmez kapılar, yangının ve dumanın yayılmasını önler. Duman, içerisinde yer alan ince taneler nedeniyle özellikle verilerin saklandığı sabit diskler üzerinde çok büyük hasarlara neden olabilmektedir.

Farklı koruyucu özelliklerin bir arada bulunduğu kapıların (örneğin hırsızlığa karşı koruma sağlayan, duman geçirmez yangın kapıları) kullanılması tercih edilmelidir.

Korunması gereken güvenli odanın, kapıları ve pencereleri ile birlikte odayı çevreleyen diğer unsurlar için de güvenlik önlemleri düşünülmelidir. Örneğin en yüksek güvenlik sınıfı, hırsızlığa karşı yüksek koruma sağlayan bir kapıyı, kolaylıkla kırılabilecek alçıpan bir duvara monte etmek doğru olmayacaktır. TS EN 1627 standardı bu konuda da yararlanılabilecek bir kaynak olarak kullanılabilir.

Yangın geciktirici veya duman geçirmez bir kapı monte edilirken, kapıyı çevreleyen duvarın eşit derecede yangın geciktirici ve duman geçirmez olduğundan; ayrıca çatı pencereleri, kablo yolları, vb. bileşenlerin yangın ve duman için bir atlama yolu (bypass) oluşturmadığından emin olunması gerekmektedir.

Güvenli kapıların oluşturulmasına ilişkin gereksinimler, Veri merkezi ve sistem odası rehberi içerisinde; uygulamaya ilişkin bilgeler ise VRM.1.U26 Hırsızlığa Karşı Koruma uygulama maddesi içerisinde bulunabilir.

Özellikle veri merkezi, belge veya veri disk arşivi gibi alanlarda, yapı denetimi ve itfaiye tarafından belirtilen özelliklerde yangın koruma güvenlik kapılarının kullanılması (bkz. VRM.1.U3 Yangın güvenliği yönetmeliklerine uyulması) uygun olacaktır. Yüksek seviyede koruma gerektiren odalar için güvenlik kapılarının kurulumu, ikaz ve alarm sistemi aracılığı ile tehlike bildirimi, kontrol ve müdahale için uyarıları içeren bir koruma yaklaşımı oluşturulmalıdır. Hırsızlığa karşı koruma sağlayan dayanıklı kapılar, tek başına potansiyel bir saldırganı caydıramaz.

Veri merkezi için TS EN 1627 standardına göre güvenlik sınıfı 3 ve üzeri kapılar kullanılmalıdır. Ancak, odanın bina güvenlik görevlileri tarafından hızlı müdahale etmeye yakın olması (en fazla 2 dakika), güvenlik açısından elverişli bir durum olması (örneğin kapının yakınında 7/24 çalışan bir ekibin bulunması) gibi istisnai durumlarda güvenlik sınıfı 2 olan bir kapı da yeterli olabilir. Öte yandan, odanın güvenliği yüksek olmadığı bir bölgede bulunması, bina güvenlik görevlilerinin müdahale süresinin uzun olması gibi durumlarda, güvenlik sınıfı 3 yerine (daha güvenli) güvenlik sınıfı 4 kapıların kurulması düşünülebilir.

Veri merkezine girmek isteyen kötü niyetli kişilerin niyeti oda içerisinde yer alan BT bileşenlerini, veriyi kendi ihtiyaçları doğrultusunda değiştirmek; BT bileşenlerine, veriye zarar vermek de olabilir. Bu nedenle, her türlü izinsiz müdahale sonrasında BT bileşenlerinin bütünlükleri kontrol edilmelidir.

Güvenliği sağlamak için kullanılan tüm kapıların (özellikle yangın ve dumandan koruma kapılarının) kapalı olduğundan emin olunmalıdır. Bu kapıların zaman zaman çalışanlar tarafından bilinçli bir şekilde açık bırakıldığı gözlenmektedir, bu tür bir davranış biçimi engellenmelidir. Bu duruma çözüm olarak, ikaz ve alarm sistemleri aracılığı ile izlenebilen, otomatik kilitleme/kapatma mekanizmasına sahip kapılar kullanılmalıdır.

Buna ek olarak, güvenli kapıların ve pencerelerin uygun şekilde çalışıp çalışmadıklarının düzenli olarak kontrol edilmesi gerekmektedir. Kapıların ve pencerelerin önerilen özelliklere uygun, düzgün bir mekanik yapıda olup olmadıkları, güvenli bir biçimde kapanıp kapanmadıkları gibi özelliklerin test edilmesi sağlanmalıdır.

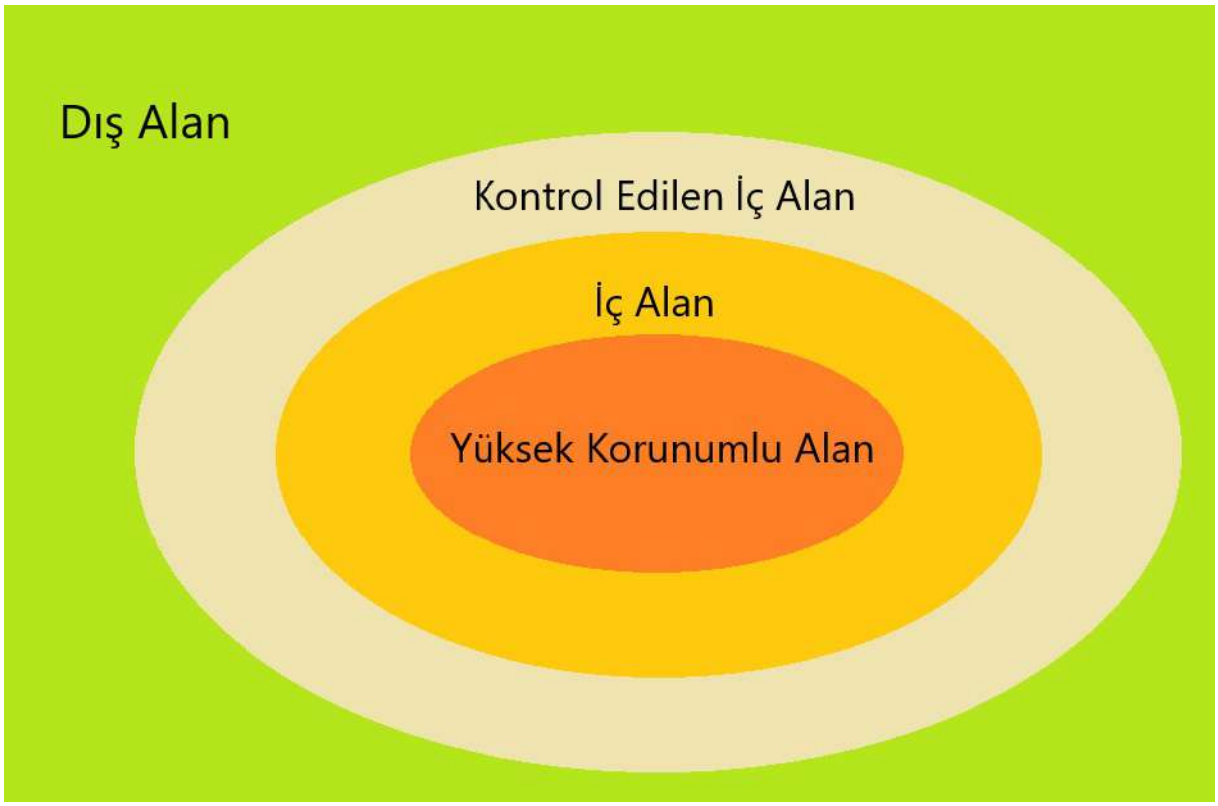
VRM.1.U22 Güvenlik bölgelerinin oluşturulması [Planlama Sorumlusu] (B)

Bina odalarının ve bölümlerinin korunma ihtiyacı, kullanımlarına bağlı olarak değişmektedir. Bu ihtiyaçlar doğrultusunda gerekli güvenlik önlemleri alınmalıdır. Buna göre duvarların, pencerelerin ve kapıların yapısal tasarımları, güvenlik ve gözetim için

kullanılacak sistemler ile tamamlanmalıdır. Yeni bir bina planlarken veya mevcut bir binayı yenilerken, benzer koruma ihtiyaçlarına sahip bölgelerin birlikte (birbirine yakın) inşa edilmesi önerilir. Bu sayede ortak riskler birlikte ele alınabilir ve güvenlik önlemlerinin toplam maliyeti düşürülebilir.

Binadaki her bir odayı, odada çalışan kimse kalmadığında kilitlemek veya devamlı gözlemlemekten kaçınmak için ziyaretçi trafiği olan bölgeler koruma gerektiren bölgelerden ayrılmalıdır. Kantin gibi ziyaretçilerin de yararlandığı alanlar ya da toplantı, eğitim veya etkinlik odaları gibi kamuya açık alanlar, bina girişinin yakınında bulunmalıdır. Ofisler gibi iç alanlar güvenlik görevlileri tarafından kolayca izlenebilir olmalıdır. Özellikle araştırma geliştirme birimlerinin kullandığı, BT bileşenlerinin ve altyapı ekipmanlarının barındırıldığı, hassas ve kritik odalar ilave bir erişim kontrolü ile korunmalıdır.

Bina ve yerleşkenin fiziksel güvenliğini sağlamak için kademeli bir derinlik anlayışı ile güvenlik önlemlerinin (soğan kabuğu ilkesi) planlanması ve uygulanması düşünülmelidir. Aşağıda dört güvenlik bölgesine (açık alan, kontrollü iç alan, iç alan ve yüksek güvenlik alanı) ayrılmış örnek bir model tanıtılmaktadır.



Şekil 10. Güvenlik bölgelerinin oluşturulması

Güvenlik bölgesi 0, yani açık alan, yerleşke sınırlarını kapsar. İlk erişim kontrolü burada yapılabilir.

Güvenlik bölgesi 1, kontrollü iç alandır. Güvenlik görevlileri veya erişim kontrol sistemi aracılığı ile gerçekleştirilecek uygun erişim kontrolü, bölgeye yalnızca yetkili kişilerin (çalışanlar, davet edilen ziyaretçiler) erişmesine izin verecektir. Yüksek bir koruma ihtiyacı olması durumunda, bölgede bulunan kişilerin kimlik kartlarını (veya ziyaretçi kartlarını) görünür bir şekilde taşımaları zorunlu tutulmalıdır. Bu bölgenin dış cephe ve alanları (genellikle binanın dış cepheleri olarak da düşünülebilir) yapısal ve teknik önlemler alınarak sabotaj ve hırsızlığa karşı korunmalıdır.

Güvenlik bölgesi 2, yalnızca yetkili kişiler tarafından erişilebilir bir iç alandır. Burada tanımlanmış erişim yetkileri geçerlidir. Bu bölgede yer alan odaların ve bölümlerin tek bir girişi bulunmalıdır. Diğer kapılar sadece kaçış ve kurtarma güzergahları olarak kullanılmalı ve günlük çalışma sırasında daima kapalı tutulmalıdır. Bu kapılar güvenlik cihazları tarafından izlenmeli ve yanlış kullanıma karşı gerekli önlemlerin alınması sağlanmalıdır.

Güvenlik bölgesi 3, yüksek güvenlik alanını oluşturur (örneğin yöneticilerin odaları, kritik BT bileşenlerinin ve altyapı ekipmanlarının barındırıldıkları odalar, vb.). Bu alana erişebilecek yetkili kişi sayısı son derece sınırlı, alanı korumak için alınan güvenlik önlemleri ise katı olmalıdır. Örneğin bu alana erişim ancak bir güvenlik kapısı vasıtasıyla, iki faktörlü kimlik doğrulama ile bu alandan çıkış ise tek faktörlü kimlik doğrulama ile mümkün olmalıdır. Odaların kullanılmadığı ve kimsenin olmadığı zamanlarda, hırsız alarm sisteminin otomatik olarak devreye girmesi sağlanmalıdır.

Postalar ve kargolar için teslimat ve yükleme alanları güvenlik bölgesi 1'de bulunmalıdır. Teslimatların, ilgili tedarikçilerin binanın daha kritik alanlarına girmek zorunda kalmadan teslim edilebilmesini sağlayacak bir yapılanma oluşturulmalıdır. Bu alanlarda bulunan kapılar uzun süre açık bırakılmamalıdır. Yüksek koruma için sadece dışarıya açılan kapı veya iç bölgelere bağlantı kuran kapılar açılabilir olmalıdır. Gelen teslimatların risk içerip içermedikleri teslimat bölgesinde gerçekleştirilecek kontroller ile belirlenmelidir. İncelemelerin türü ve derinliği ilgili tehlikenin potansiyeline (örneğin mektup bombaları) bağlı olarak değişebilmelidir. Gelen ve giden teslimatların mümkün olduğunca ayrı tutulmaları önerilmektedir.

VRM.1.U23 Otomatik drenaj (A)

Binalarda suyun toplanabileceği ve birikebileceği veya hasar meydana getirebilecek akan ve durgun haldeki su barındırabilecek alanlar, binaya zarar verebilecek suyun tahliye edilebilmesi için otomatik drenaj ve su dedektörleri ile donatılmalıdır. Otomatik drenaj düşünülebilecek alanlar arasında;

- Bodrumlar,
- Yükseltilmiş zeminler altındaki hava boşlukları,

- Kuyular,
- Kalorifer sistemlerinin bulunduğu odalar yer alabilir.

Drenaj pasif olarak gerçekleştiriliyor ise, yani binanın kanalizasyon sistemine doğrudan drenaj yapılıyorsa, tahliye edilen suyun geri gelmesini engellemek için geri akış önleyiciler (yer süzgeçleri) kullanılması gereklidir. Bu önleyicilerin kullanılmaması durumunda, kanalizasyon kapasitesi dolduğunda, bina içerisine suyun girmesi söz konusu olabilir. Aşırı yağışların ardından, bu yoldan su bodrum kattan içeriye girebilir. Geri akış önleyicilerin doğru çalışıp çalışmadıklarının düzenli olarak kontrol edilmesi sağlanmalıdır.

Kanalizasyon sistemi seviyesi çok yüksek ise pasif drenaj mümkün olmayabilir. Bu durumda, şamandıralı şalterler veya su dedektörleri vasıtasıyla otomatik olarak devreye giren pompalar kullanılabilir. Bu tekniği kullanırken, özellikle aşağıdakilere dikkat edilmelidir:

- Pompalama kapasitesi yeterli olmalıdır.
- Pompanın tahliye hattı, geri akış vanası ile donatılmalıdır.
- Pompanın, suda yüzen nesneler tarafından engellenememesi için önlemler alınmalıdır (emme filtresi, vb.).
- Pompanın çalıştırıldığı bilgisi ilgili kişilere (örneğin bina teknisyenlerine) otomatik olarak bildirilmelidir.
- Pompanın ve şalterin işlevselliği düzenli olarak test edilmelidir.
- Pompanın tahliye hattı, kanalizasyon sisteminin borusu yakınlarına bağlanmamalıdır.

Özellikle şiddetli yağışlar sırasında, dışarıdan suyun binaya girmesini önlemek için, drenaj sisteminin durumu kontrol edilmeli ve gerekirse onarılmalıdır. Bina yerleşkesinin konumu nedeniyle, su taşkın riskleri söz konusu ise özel su koruma kapılarının kurulması düşünülmelidir.

VRM.1.U24 Uygun yer seçimi [Kurum Yöneticisi] (E)

Binanın inşa edileceği yerin seçimi ve planlanmasında, alan gereksinimleri ve maliyet gibi konuların yanında bilgi güvenliğini etkileyebilecek çevresel koşullar da dikkate alınmalıdır:

- Bina yapısındaki zayıflıklar nedeniyle, yakın trafik güzergahlarının (otoyol, demiryolu, metro, vb.) sarsıntı ve darbeleri BT bileşenlerinde hasarlara neden olabilir.
- Ana yol üzerinde bulunan binalar (demiryolu, otoyol, ana yol, havaalanı, vb.) trafik kazalarından etkilenebilir, hasar görebilir.

- Yakınlarda (sinyal) yayın ekipmanının bulunması BT bileşenleri için kesintiler oluşturabilir.
- Binaların, havayolu yakınında, uçakların iniş-kalkış güzergahlarında bulunması BT bileşenlerini olumsuz bir biçimde etkileyebilir.
- Dere yatakları ve alçak bölgelerde bulunan binalar su baskınlarından etkilenebilir.
- Enerji santralleri ya da fabrikalar çevresinde oluşabilecek kaza ve büyük arızalar (patlama, zararlı maddelerin boşaltılması) çevreye ulaşımın engellenmesi durumunda binaya erişimi etkileyebilir.

Korunmaya değer bina kısımlarının uygun şekilde düzenlenmesiyle olası tehditlere yönelik önlemler alınabilir. Bu durum planlama ve uygulama sırasında dikkate alınmalıdır.

Yerleşke ve konuma ilişkin riskler ve bu riskleri kontrol altına almak için gerekli (azaltıcı veya önleyici) önlemler bina kullanımı güvenlik konsepti içerisinde kayıt altına alınmalıdır. Buna ek olarak, söz konusu risklerin ve önlemlerin acil durum / felaket kurtarma çalışmaları sırasında da kullanılması sağlanmalıdır.

VRM.1.U25 Güvenlik görevlileri ve bina güvenlik hizmetleri (GBE)

Binaya ve yerleşkeye erişimin kontrol altına alınması, binanın ve yerleşkenin izlenmesi ve genel güvenliğin sağlanması amacı ile güvenlik görevlilerinden yararlanılması, bir bina güvenlik hizmeti kurulması önerilmektedir. Bununla birlikte bu hizmetler yerine getirilirken bazı temel ilkelere uyulmalıdır.

- Güvenlik görevlileri, kapıdaki ve diğer tüm girişlerdeki hareketleri gözlemlemeli ve kontrol etmelidir.
- Giriş noktalarına uzak olan tüm kapıların ve pencerelerin kamera gözetimi ile güvenlik görevlileri tarafından izlenmesi ve kontrol edilmesi sağlanmalıdır.
- Güvenlik görevlileri binada görev yapan çalışanları tanımalıdır. Bununla birlikte bilinen çalışanların kimlikleri ile kendilerini tanıtarak, kapılardan geçmeleri sağlanmalıdır. Çalışanın kurumdan ayrılması veya kurum içindeki konumunun değişmesi gibi durumlarda, çalışanın yeni erişim izinleri (özellikle bina giriş/çıkışları ve bina içerisindeki güvenlikli alanlara erişim) hususunda güvenlik görevlilerine bilgi verilmelidir.
- Bilinmeyen kişilerin kendilerini güvenlikte tanıtmaları sağlanmalıdır.
- Ziyaretçilerin bina içerisine giriş nedeni/ihtiyacı sorgulanmalı, gerekli onay alınması durumunda giriş izni verilmelidir. Sadece geçerli nedeni olan ziyaretçiler binaya giriş yapmasına izin verilmeli, ziyaretçilerin binaya girişi kayıt altına alınmalıdır. Ziyaretçi kimlik kartları aracılığı ile ziyaretçilerin bina içerisinde tanınması ve çalışanlardan ayırt edilebilmesi sağlanmalıdır.

- Çalışanlar veya güvenlik görevlileri ziyaretçilere refakat etmelidir. Herhangi bir refakatçi olmaksızın binaya veya yerleşkeye giriş yapabilecek ziyaretçilerin bir listesi bulunmalıdır.
- Bina içerisinde yaşanan güvenlik olayları ve ihlalleri, kullanılan ikaz ve alarm sistemi aracılığı ile yetkili güvenlik görevlilerine hızlıca iletilebilmeli, güvenlik görevlisinin zamanında müdahale etmesi sağlanmalıdır.

Güvenlik görevlerinin sorumlulukları, açık ve net bir şekilde tanımlanmalı ve yazılı hale getirilmelidir. Görev tanımı içerisinde güvenlik görevlilerinin diğer koruyucu tedbirler ile ilişkili faaliyetleri (örneğin, iş veya mesai saatlerinden sonra güvenlik kontrolleri, alarm sisteminin devreye alınması, dış kapıların ve pencerelerin kontrol edilmesi gibi) yer almalıdır.

Görevler tanımlanırken, atanan görevlerin herhangi bir güvenlik boşluğu oluşturmaması, birbiriyle çelişmemesi sağlanmalıdır. Örneğin bir kapıda sadece bir görevli bulunuyorsa ve kapının geçici olarak kapatılması mümkün değilse, görevlinin ziyaretçilere eşlik etmemesi (bunun yerine ilgili çalışanın ziyaretçiye eşlik etmesi) doğru olacaktır.

VRM.1.U26 Hırsızlığa Karşı Koruma (GBE)

Bina içerisinde hırsızlığa ve saldırıya karşı gerekli önlemlerin uygulanması gereklidir. Uygulanabilecek önlemler arasında:

- Bina içerisinde bulunan odanın/alanın korunma gereksinimine göre “VRM.1.U21 Güvenli Kapı ve Pencereler” uygulama maddesinde bahsedilen hırsızlığa dayanıklı kapı ve pencerelerin kullanılması (veri merkezi ve sistem odaları için güvenlik sınıfı 3 veya üzeri tercih edilmelidir),
- Özellikle giriş katında bulunan kapılar veya pencereler için kilitlenebilir kepenkler kullanılması,
- Özel kilitlerden ve sürgülerden yararlanılması,
- Kullanılmayan tüm girişlerin kapatılması ve kilitlenmesi,
- Acil çıkış kapılarının dışarıdan zorla açılmaya karşı dayanıklı olması,
- Yolcu ve yük asansörlerinin çalışma saatleri dışında kapatılması düşünülebilir.

Bunlar ile birlikte kurumun bulunduğu bölgede yer alan emniyet müdürlüğü ile görüşülmesi, emniyet müdürlüğü tarafından önerilen önlemlerin de uygulanması tavsiye edilir.

Hırsızlığa karşı korumaya yönelik tüm önlemler, yetkisiz erişime karşı korunması gereken alanın/odanın etrafında uçtan uca bir koruma oluşturacak şekilde uygulanmalıdır. Örneğin kapılar yeterince sağlam duvarlara monte edilmelidir. Havalandırma açıklıkları, insan girişine izin vermeyecek şekilde tasarlanmalıdır (azami genişlik 10x20 cm). Yükseltilmiş

zemin ve asma tavanda erişim koruma önlemleri uygulanmalıdır. Alınan tüm önlemler önce planlama ve uygulama, daha sonra işletim aşamalarında yetkili bir kişi tarafından düzenli olarak kontrol edilmelidir.

Hırsızlığa karşı koruma için gerekli fiziksel güvenlik önlemleri planlanırken, yangın ve kişisel koruma için kullanılan uygulamaların ve hükümlerin ihlal edilmemesine özen gösterilmelidir. Örneğin alınacak bir fiziksel güvenlik önlemi ile yangından kaçış yolları bloke edilmiyor olmalıdır.

Çalışanların hırsızlığa karşı koruma için hangi düzenlemelere ve önlemlere uymaları gerektiğine ilişkin (örneğin kapı, pencere veya kepenklerin çalışma alanından ayrılan son çalışan tarafından kilitlenmesi gerektiği gibi) bilgilendirilmelerin yapılması önerilir. Özellikle yönetim odaları, veri merkezi ve veri arşivi gibi kritik alanlarda hırsızlığa karşı koruma önlemlerinin alınmalıdır.

VRM.1.U27 İklimlendirme (Klima) Sistemleri (BE)

Binalarda havalandırma, çalışanların uygun ortamlarda çalışabilmesini sağlayacak biçimde, havalandırma/iklimlendirme sistemleri ile sağlanır. İklimlendirme sistemleri havanın taşınmasını (havalandırma), kapalı ortamda insan sağlığına uygun olarak kaliteli havanın dolaşmasını ve odada uygun iklim koşullarının oluşturulmasını sağlayarak, çalışanlar için rahat bir çalışma ortamının oluşturulmasına yardımcı olur. İklimlendirme sistemi aracılığı ile odaya verilen hava, çalışanların sağlığına zarar vermemeli, herhangi bir koku sıkıntısı oluşturmamalı ve ısı açısından konforlu bir ortam sağlanmasını mümkün kılmalıdır.

Tüm bunlarla birlikte iklimlendirme sistemi tek başına bina içerisinde kaliteli hava oluşması için yeterli değildir. Bina yapımında kullanılan inşaat malzemeleri, zemin kaplamaları ve mobilyaları da kaliteli hava için önemlidir. Bu unsurların seçiminde, oda havasını etkilemeyecek ve gereksiz yük yaratmayacak zararsız malzemelerin kullanımına dikkat edilmelidir.

Konut dışı binalar için iklimlendirme sistemlerinin planlanması DIN EN 13779 "Konut dışı havalandırma - Havalandırma ve klima sistemleri ile oda soğutma sistemleri için genel ilkeler ve gereksinimler" standardı içerisinde detaylı bir biçimde anlatılmaktadır. DIN EN 13779 içerisinde aşağıdaki tanımlar yer alır:

- Bina çalışma sıcaklıkları,
- Odanın bağıl nemi,
- Ses basınç seviyeleri
- Çalışanlar ile ilgili diğer faktörler

Hava kalitesinin, sürekli kullanılan ofislerde ve odalarda, her zaman kullanılmayan odalara oranla daha yüksek olması gerekir. İklimlendirme sistemlerinin planlanması sırasında bu durumun göz önünde bulundurulması oldukça önemlidir.

Konforlu oda ikliminin oluşturulmasında yaz sıcağı, soğuk havaya kıyasla daha büyük problem teşkil eder. Sağlıklı bir işyeri ortamının oluşturulması için uygun oda sıcaklığı kadar ve güneş ışınlarından korunma da göz önünde bulundurulmalıdır. Sıcak yaz günlerinde rahat bir ortam sıcaklığı oluşturabilmek için iklimlendirme sistemi etkin pencere gölgelendirmesi (perde ve panjur sistemleri) ile desteklenmelidir.

İklimlendirme sistemlerinin bakımları düzenli olarak gerçekleştirilmelidir. Tüm bina içerisinde gerçekleşen hava dolaşımı düşünüldüğünde, iklimlendirme sistemlerinin bakımı uygun çalışma ortamının oluşturulmasının yanı sıra bina içerisinde yer alan tüm çalışanların sağlığını garanti altına almaya da yardımcı olur. Kullanılan iklimlendirme sistemleri belirli aralıklar ile kontrol edilmeli, bakımı ve temizliği yapılmalı özellikle de hava filtrelerinin belirli aralıklar ile değişimleri sağlanmalı ve kayıt altına alınmalıdır.

İklimlendirme sistemleri herkesin erişimine açık olmamalıdır. Bu sistemleri kötü niyetli kullanımlara ve sabotaja karşı korumak gereklidir. Ayrıca iklimlendirme sistemlerinin, acil durum planlamasında dikkate alınması önerilmektedir.

VRM.1.U28 Bina temizliği için prosedürler (GBE)

Binanın ve içerisinde yer alan odaların temizliği için görev yapan temizlik personeli, yalnızca belirli çalışan gruplarının erişimi olan teknik odalar, kritik belgelerin saklandığı arşiv odaları veya üst düzey yöneticilerin odaları gibi yerler dahil olmak üzere binanın tüm odalarına ve alanlarına girebilmektedir. Genellikle çalışma saatleri dışında gerçekleşen temizlik faaliyeti sırasında görevlilerin bilinçli veya bilinçsiz hareketleri nedeniyle BT bileşenleri ve altyapı ekipmanları zarar görebilir, kurum için hassas bilgiler açığa çıkabilir, kullanılamaz hale gelebilir.

Bina içi temizliğin sağlanmasından sorumlu temizlik görevlilerinin veya bina temizliği için görevlendirilen temizlik şirketi çalışanlarının, temizlik süresince görevleri dışında başka bir faaliyet gerçekleştirip gerçekleştirmedikleri; bina içi erişim için kendilerine verilen anahtarları veya kimlikleri uygun bir biçimde kullanıp kullanmadıkları kontrol edilmelidir.

Temizlik görevlilerinin temizleme faaliyetlerini gerçekleştirmek için kullanacakları zaman çizelgesi ile birlikte özellikle temizlik görevlileri tarafından erişilmemesi gereken alanlar belirtilmelidir.

Temizlik görevlileri, çalışmalarına başlamadan önce görevleri hakkında bilgilendirilmelidir. Kurumların bu konuda çeşitli yönergeler ile temizlik görevlileri için gerçekleştirilecek

faaliyetleri tanımlamaları ve sınırları net bir şekilde çizmeleri önerilir. Bu yönergeler içerisinde temizlik görevlilerinin hangi şartlar altında nasıl davranacakları, hangi alanlara erişilebilecekleri, BT bileşenlerini nasıl temizleyecekleri ve BT bileşenlerinin yer aldığı alanlarda nelere dikkat etmeleri gerektiği gibi unsurlar yer almalıdır. Temizlik görevlilerinin özellikle çalışmaları sırasında öğrendikleri bilgiler (masalarda bulunan dokümanlar, kulak misafiri olunan konuşmalar, vb.) ile ilgili nasıl davranmaları gerektiği konusunda da bilgi sahibi olmalarını sağlamak gereklidir.

Veri merkezleri, altyapı ekipmanlarının barındırıldığı teknik odalar veya iletişim merkezleri gibi daha yüksek güvenlik gereksinimi olan alanlar için ek güvenlik tedbirleri gereklidir. Bu gibi alanlarda görev yapacak temizlik görevlilerinin gözlemler yolu ile güvenilirliklerine dikkat edilmesi önerilir.

Temizlik görevlileri genellikle BT bileşenleri konusunda çok bilgi sahibi değildirler. Bu nedenle temizlik görevlilerinin, BT bileşenleri ve kurum içi bilgi yönetimi hakkında, özellikle BT bileşenlerinin bulunduğu alanların temizlenmesi sırasında nelere dikkat edilmesi gerektiği konusunda bilgilendirilmeleri önerilir. Temizlik görevlilerinin örneğin:

- Klavyeyi temizlerken, sunuculara veya diğer önemli bileşenlere kasıtsız işlem komutları vermeleri,
- BT bileşenlerini, kritik sunucu veya ağ cihazlarını yanlışlıkla kapatmaları,
- Güç veya iletişim kablolarının hasar görmesine veya yırtılmasına neden olmaları,
- Kullandıkları su veya temizleme sıvısı nedeniyle BT bileşenleri veya altyapı ekipmanları üzerinde kısa devrelere neden olmaları oldukça sık rastlanılan olaylardır.

Temizlik görevlilerini bu olası olaylar hakkında bilgilendirmek ve yapılması gereken faaliyetler hakkında eğitmek gereklidir.

Veri merkezi, alt yapı ekipmanlarının bulundurulduklari odalar veya veri disk arşivi gibi kritik alanların yetkili bir çalışan eşliğinde ve gözetiminde temizlenmesi önerilmektedir.

VRM.1.U29 Uygun bina seçimi (GBE)

Binanın içerisinde bulunacağı yerleşkenin özelliklerine (bkz. VRM.1.U24 Uygun yer seçimi) ek olarak, bir binanın iç uygunluğu açısından değerlendirilmesi gerekmektedir. Prensip olarak, bina seçimi sırasında binanın kullanım gereksinimlerine uygunluğunu, alınması düşünülen tüm önlemlerin uygulanıp uygulanamayacağını kontrol etmek gereklidir.

Bununla birlikte binayı, üzerinde gerçekleştirilecek bir takım çalışmalar ile istenilen kullanıma uygun hale getirmek son derece zor ve maliyetli olabilir. Bir binanın seçiminde

aşağıda yer alan unsurlar, mümkün olduğunca sonradan oluşabilecek problemleri fark etmek, mümkünse bunların oluşmalarını önlemek için kullanılabilir. Bu unsurlar yeni bir bina planlaması sırasında da kurumlara yardımcı olacaktır.

Bilgi güvenliği açısından, bina yapısının durumu ile ilgili olarak aşağıdakiler de dikkate alınmalıdır:

- Yapının yük taşıma gücü (maksimum zemin taşıma yükü, taşıyıcı duvarlar), içerisinde ağır ekipmanlar barındırabilen odaların (veri merkezi, sistem odası, altyapı ekipmanlarının yer aldığı odalar, vb.) kurulumu/yenilenmesi çalışmaları için yeterli midir?
- Mevcut erişim güzergâhları (koridorlar, merdivenler, asansörler) yeterli midir? Veya gerekli görülürse ilave erişim güzergahları kurulabilir mi? VRM.1.U7 Güvenlik ve Erişim Kontrolü maddesi bu güzergahlar üzerinde uygulanabilir mi?
- Yüksek güvenlik gereksinimlerine sahip alanları, düşük güvenlik gereksinimlerine sahip alanlardan ayırmak mümkün müdür? Bina içerisinde güvenlik bölgeleri oluşturulabilir mi?
- Geniş ve ağır BT bileşenlerini ve altyapı ekipmanlarını taşımak için mevcut erişim güzergâhları (koridorlar, merdivenler, asansörler) kullanılabilir mi? Veya gerekli görülürse ilave erişim güzergahları kurulabilir mi? Bu durumun güvence altına alınmaması, olası bir donanım hasarına ve gecikmelere neden olabilir.
- "VRM.1.U3 Yangın güvenliği yönetmeliklerine uyulması" maddesinin uygulanabilmesi için oda dağılımı/düzeni mümkün müdür?
- Elektrik tesisatı, "VRM.1.U2 Elektrik yük dağılımının ayarlanması/yapılandırılması " maddesine uygun bir biçimde yapılandırılabilir mi?
- Bina içerisinde harici yıldırım koruması bulunmakta mıdır? Yakınlarda yaşanacak bir yıldırımın bina içerisinde bulunan elektrik tesisatına ve ağ yapılanmasına olası etkilerini en aza indirgemek için gerekli önlemler alınmış mıdır?

Kurum tarafından kullanılacak binanın kiralanması düşünülüyor ise:

- Kiracı olarak bina üzerinde gerekli tadilatların yapılması için gerekli izinler bulunuyor mu?
- Sözleşme süresinin sonunda yapılan tüm tadilatların geri alınması gerekiyor mu?
- Bina aynı anda farklı kurumlar tarafından kullanılacak mı?

gibi soruların göz önünde bulundurulması yerinde olacaktır.

Bina seçiminde göz önünde bulundurulan güvenlik gereksinimleri kayıt altına alınmalı, özellikle saptanan güvenlik riskleri ve bunların önlenmesi veya azaltılması için alınan tedbirler detaylı bir biçimde belirtilmelidir.

VRM.1.U30 Bina tahliyesi [Teknisyen] (B)

Binanın belirli bir bölümünün veya tamamının taşınması gerekiyorsa,

- Taşınma öncesinde BT bileşenlerini ve kurum için kritik bilgi varlıklarını (donanım, yazılım, medya, klasörler, belgeler vb.) içeren bir envanter hazırlanmalıdır.
- Tüm çalışanların taşınma sırasında rolleri ve sorumlulukları tanımlanmalı, çalışanlara bu roller ve sorumluluklar bildirilmelidir.
- Taşınma sırasında kullanılmayacak olan eski cihazlar, kurum yönetmelikleri ve bilgi güvenliği politikalarına uygun bir biçimde elden çıkarılmalı veya imha edilmelidir.
- Tahliye sonrası, daha önce hazırlanan envanter kullanılarak, BT bileşenlerinin ve kritik bilgi varlıklarının düzgün bir biçimde taşınıp taşınmadığı kontrol edilmelidir.

Taşınma bir proje ekibi tarafından koordine edilmeli, taşınacak tüm BT bileşenleri, altyapı ekipmanları ve diğer varlıklar sistematik bir şekilde toplanmalı, taşınmalı (gerekiyorsa elden çıkarılmalı veya ihmal edilmeli) ve yeni bina kullanıma hazır hale getirilmelidir.

VRM.1.U31 Korunması gereken alanların düzenlenmesi (GBE)

Bina içerisinde korunması gereken odalar ve bölümler, dışarıdan görülebilen, dış tehditlere açık ve tehlikeli olabilecek alanlarda konumlandırılmamalıdır:

- Bodrum katta bulunan odalar su baskını ile karşı karşıya kalabilir.
- Zemin katta yer alan odalar saldırılara, trafik kazalarına maruz kalabilir.
- Zemin katta bulunan odalar (özellikle görünmeyen odalar) için soygun ve sabotaj tehditleri bulunur.
- Zemin katta bulunan kolay ulaşılabilir odalarda ya da halka açık alanlarda, hırsızlık ya da gizli bilginin açığa çıkması gibi olaylar yaşanabilir.
- Çatıların altında bulunan odalar, yağmur suyu sızıntısından etkilenebilir.
- Yeraltı otoparkları birçok riski de beraberinde getirir; görünmeyen arka kapılar, herkes tarafından kolayca ulaşılabilen BT kabloları, vb. gibi. hatta kötü niyetli kişilerin otoparklara park ettikleri araçları içerisinden, yeterince korunmamış kablosuz ağ hattı üzerinden kurum bilgilerine ulaşabilmeleri mümkün olabilir. Yangın koruması açısından, yeraltı garajlarında bulunan, depolama alanı olarak kullanılan alanlar da sorunlu olabilir.

Genel bir kural olarak, koruma gerektiren odaların veya alanların binanın merkezinde konumlandırılmaları önerilir.

En uygun olan, tüm bu unsurların yeni bir binanın planlaması sırasında veya mevcut bir binaya taşınma öncesinde göz önünde bulundurulması, gerekli önlemlerin alınması için yapılacak çalışmaların projeye dahil edilmesidir.

Korunması gereken odalarda ve alanlarda söz konusu riskler kontrol altına alınamıyorsa, bu durum bina kullanımı güvenlik konseptinde açıkça belirtilmelidir. Buna ek olarak, riskleri azaltmak veya ortadan kaldırmak için ilave önlemlerin alınması düşünülmelidir. Örneğin, elektrik odalarında veya zemin katta yer alan veri merkezi ve sistem odalarında, su sızıntısını tespit edecek dedektörlerin kullanılması ve otomatik drenaj önlemlerinin hazırlanması ile su sızıntısı riski kontrol edilebilir.

VRM.1.U32 İkaz ve Alarm Sistemi (E)

Alarm sistemi, bir kontrol merkezi ile iletişim halinde bulunan, gerektiğinde alarmı tetikleyen çok sayıda yerel dedektörden oluşur. Bir alarm sistemi aracılığı ile bilişim teknolojisinin temel alanları (sistem odaları, veri disk arşivleri, teknik altyapı odası) izlenebilir; hırsızlık, yangın, su sızıntısı, vb. durumlar erken tespit edilip gerekli önlemler alınabilir.

Sistemin etkin ve verimli çalışabilmesi için alarm sistemi tarafından üretilen mesajların, güvenlik odaları gibi sürekli bir personelin bulunduğu merkezlere iletilmesi gerekmektedir. Ayrıca bu merkezde bulunan, alarmları karşılayacak personelin, gelen alarmlara tepki verebilecek kabiliyette olması sağlanmalıdır. Bu konularda kurumların özellikle "TS EN 50518 Görüntüleme ve alarm izleme merkezi" gereksinimlerine uymaları tavsiye edilmektedir.

Binanın farklı alanlarının, farklı kullanım biçimleri göz önünde bulundurularak, ihtiyaçlara uygun tehlike algılama ve yönlendirme, alarm üretme yaklaşımları oluşturmaları gerekmektedir. Bu yaklaşım, alan kullanımlarındaki değişikliklere göre uyarlanabilir olmalıdır. Alarm sistemi, bina tipine ve risklere göre planlanması ve kurulması gereken karmaşık bir genel sistemdir. Bu yüzden alarm sisteminin planlanması, kurulumu ve işletimi yetkin ve deneyimli uzmanlar tarafından gerçekleştirilmelidir. Bu yetkinlik şirket içinde mevcut değilse dış destek kullanılması düşünülmelidir. Örneğin, güvenlik gereksinimlerine ve binanın çevresel koşullarına göre seçilebilecek birçok farklı alarm sistemleri bulunur. Hırsızlık tespiti için örneğin, hareket algılayıcılar, cam kırılma dedektörleri, video kameralar, vb. kullanılabilir. Fakat yangın için ihtiyaç duyulan detektörler daha farklı olacaktır.

Dedektörler ve algılayıcılar farklı şekillerde birbirlerine bağlanabilir. Korunacak alanların türüne ve boyutuna ve geçerli politikalara bağlı olarak, uygun sistemler seçilmeli ve kurulmalıdır. Bir alarm sistemi planlanırken veya genişletilirken, kablo kanal altyapısının

(taşıma sistemlerinin) yeterli olmasına ve mümkün olduğunca kablolar ve kablo yollarında az değişiklik yapılmasına dikkat edilmelidir.

Alarm sisteminin çalışırlığının güvence altına alınması için, düzenli bakımlar ve fonksiyon testleri yapılmalıdır.

Binada herhangi bir alarm sistemi mevcut değilse veya mevcut bir sistem aktif olarak kullanılamıyor ise başlangıçta sadece önemli alanlarda alarm dedektörlerinin yerel olarak kullanılması düşünülebilir. Yerel olarak çalışan alarm dedektörleri merkezi bir servise bağlanmadan tamamen bağımsız çalışırlar. Dedektör tarafından olağan dışı bir durum tespit edildiğinde, alarm sesli olarak, tehlike tespit edilen bölgede üretilir veya basit bir kablo (çoğu zaman telefon hattı) vasıtasıyla başka bir bölgeye iletilir.

Veri merkezi, veri disk arşivi gibi yüksek koruma gerektiren odalarda alarm sistemi bulunması gereklidir. Merkezi alarm sisteminin bulunmadığı binalarda, bu tür kritik odalarda en azından yerel çalışan alarm dedektörleri kurulmalıdır. Kurulan yerel alarm dedektörlerinin, etkilenen alanların dışından da algılanacak biçimde sesli (ve mümkünse görsel) mesajlar üretmesi sağlanmalıdır. Üretilen mesajlar çeşitli kanallar aracılığıyla, günün 24 saati hizmet veren bir merkeze iletilmelidir. (Örneğin çalışanların cep telefonlarına haftanın 7 günü, günün 24 saati alarm mesajlarını SMS olarak iletebilecek çözümler bulunmaktadır.)

Bir alarm sistemini planlamadan önce, üzerinde çalışılan bina için bir bina kullanım güvenlik konsepti geliştirilmelidir. Kurulacak alarm sistemi, bu konsept ile tutarlı olmalıdır. Özel ya da ticari mülklerin alarm sistemleri planlanırken, özellikle hırsızlığa karşı sigortanın olup olmadığı öğrenilmeli, sigorta koşulları kurumun birlikte çalıştığı sigorta firması ile açıklığa kavuşturulmalıdır.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

- ISO/IEC 27001:2013 - Annex A.11 Physical and enviornmental security
  ISO, Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.11 Physical and environmental security, 2013
  https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
- NIST Special Publication 800-53 Revision 4 - APPENDIX PAGE F-213
  Assesing Security and Privacy Controls for Federal Information Systems and Organizations, insbesondere APPENDIX F-PS PAGE F-213, FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION, NIST, 2013
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- TSE 11925, ISO 11925, DIN 4102

- DIN V ENV 0185, 0298, 0833, 1143, 12056
- BSI-Bundesamt für Sicherheit in der Informationstechnik, Umsetzungshinweise zum Baustein INF.1 Allgemeines Gebäude https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html

VRM.2.U: VERİ MERKEZİ VE/VEYA SİSTEM ODASI

1 AÇIKLAMA

1.1 TANIM

Günümüzde hemen hemen tüm stratejik ve operasyonel görevler, bilgi teknolojisi (BT) tarafından önemli ölçüde desteklenmekte, BT olmadan yürütülememektedir. Bu yüzden, BT sistemlerinin performans, erişilebilirlik ve ağ bağlantı gereksinimleri giderek artmaktadır. Bu gereksinimleri karşılamak, kaynakları korumak ve BT'yi ekonomik bir şekilde işletebilmek için kurumlar ve şirketler BT birimlerine yoğunlaşmaktadır.

Veri merkezleri; sunucular, depolama, ağ (network) ve haberleşme cihazları ile benzeri BT donanımlarının güvenli bir şekilde çalışmalarının sağlandığı, verilerin saklandığı, korunduğu, bununla birlikte kullanıcıların kesintisiz ve hızlı bir şekilde verilere ulaşması için gerekli tüm teknik altyapının yer aldığı odalardır. Bu odalar fazla miktarda bileşen içerdiğinden olası hasarlar ciddi sonuçlar doğurabilmektedir. Veri merkezleri, ait oldukları kurumların işletme büyüklüğü, kritiklik seviyesi ve kapasitesi gibi unsurlara göre tasarlanmaktadır. Kapasite belirlenirken personelin çalışma şekli (vardiyalı olarak çalışma, çağrı üzerine hizmet sunma, vb.) dikkate alınmalıdır.

Bu rehber öncelikle orta ölçekli veri merkezleri için tasarlanmıştır. . Sektörde pratikte çok kullanılan, işe yaradığı gözlenmiş, kendini ispatlamış uygulama maddelerinin, küçük ölçekli sunucu odaları ile (banka ve telekomünikasyon sektöründe kullanılan) büyük ölçekli veri merkezleri arasında kalan kritik alanlar için kullanılması tavsiye edilmektedir. Detaylı ve sadece belirli kullanımlara özgü uygulama maddeleri bu anlamda kapsama dahil edilmemiştir (örneğin, terörizm ve 4.seviye gereksinimler sınırlı şekilde açıklanmıştır).

Veri merkezi içerisinde, BT bileşenleri ile destek altyapısını oluşturan ekipmanlar (elektrik güç kaynağı, klima teknolojisi vb.) genellikle farklı odalarda bulunurlar. Fakat birçok kurum, içinde bulundukları koşullar nedeniyle tüm gerekli ekipmanları tek bir oda içerisinde barındırmayı tercih etmektedir. Elinizdeki rehber içerisinde bu tip odalar, sistem odası olarak adlandırılmaktadır.

Veri merkezi işleten veya veri merkezi hizmetinden yararlanan kurumların bu rehber içerisinde yer alan gereksinim maddelerini incelemeleri, öncelikle temel maddelerden başlayarak ihtiyaçları doğrultusunda diğer maddeleri uygulamaları önerilmektedir.

Diğer yandan sistem odasına sahip kurumların, sahip oldukları imkanlar doğrultusunda, bu rehberde yer alan gereksinim maddelerini dikkate almaları ve en azından **temel gereksinimleri** yerine getirmeleri beklenmektedir

1.2 YAŞAM DÖNGÜSÜ

Veri merkezi tasarlanırken veya kurulurken bir takım çalışmaların yapılması gerekmektedir. Duruma bağlı olarak (yeni binada kurulum, mevcut binada yenileme) bazı maddeler veya uygulamalar farklılık gösterebilir. Mevcut veri merkezindeki genişlemelerde uygulanacak maddeler, yeni kurulumlara göre daha sınırlıdır. Veri merkezi ve/veya sistem odalarında uygulanması gereken maddeler seviyelendirilmiş bir şekilde bu **Rehberin** uygulama başlığı altında yer almaktadır.

Planlama ve Konsept

Veri merkezinin planlama aşamasında uygulanması gereken temel prensip, altyapı ve BT sistemlerinin birbirinden ayrı tutulmasıdır. BT sistemleri ve destek bileşenleri (güç kaynakları, UPS'ler, klima sistemleri, vb.) farklı odalarda konumlandırılmalıdır. Ek olarak yangın ve duman tehditlerinden kaçınmak, güç kaynakları ve klima sistemlerinin güvenliğini sağlamak için bir dizi fiziksel koruma önlemi uygulanmalıdır. Su sızıntıları büyük miktarda hasara ve hatta tüm BT sistemlerinin kullanılmaz hale gelmesine neden olabileceğinden, bu alanlarda su borularından kaçınılmalıdır. Fiziksel koruma ayrıca, veri merkezinin ayrı bir yangın koruma bölgesinde olmasını da kapsar. Bu tür kritik alanlar dışarıdan görünür olmamalıdır.

Genel olarak teknik altyapının yedekliliğine özen gösterilmeli, şebekeyi destekleyecek bir ikincil enerji sağlayıcının (örneğin jeneratör) kullanılması planlanmalıdır. Oluşan hasarların olabildiğince çabuk algılanabilmesi ve ilgili ekiplere aktarılabilmesi için ikaz ve alarm sistemleri ile gerekli unsurlar (yangın, yetkisiz erişim, vb.) izlenmelidir.

Devreye Alma/Yerine Getirme

Veri merkezi ve/veya sistem odalarına sadece görev tanımları gereği o alanda çalışan yetkili kişilerin erişimi sağlanmalıdır. Kritik alanların bakımı veya temizliği için verilen erişim yetkisi asgari düzeyde tutulacak şekilde düzenlenmeli ve mümkünse gözetim halinde takip edilmelidir. Bu alanlarda yangın yüklerinden kaçınılmalıdır.

Operasyon

Veri merkezi kullanılmadığı zamanlarda kilitli tutulmalıdır. Bakım çalışmaları için erişime ihtiyaç duyan firma veya ziyaretçilere, çalışmaları süresince eşlik edilmelidir. İzleme ve alarm sistemlerinden gelen uyarılara hızlı tepki verecek şekilde sorumluluklar belirlenmeli ve işleyiş düzenli olarak kontrol edilmelidir.

Acil durum hazırlık

Düzenli olarak tatbik edilmeyen güvenlik önlemleri, acil durumlarda normal şekilde uygulanamayabilir. Bundan dolayı düzenli tatbikatların yapılması gereklidir. Tatbikatlar, uyarı planlarının güncelliğini korumaya da yardımcı olurlar. Hasar sonrası, hayati önem taşıyan verilere hızlı bir şekilde erişmek için, kritik veriler düzenli olarak yedeklenmelidir.

2 UYGULAMALAR

Aşağıda yer alan maddeler, veri merkezi ve sistem odası bölümüne özel uygulama maddeleridir.

2.1 1.SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

VRM.2.U1 İhtiyaçların Tanımlanması

Veri merkezi tamamen kapalı bir güvenlik bölgesi olarak tasarlanmalıdır. Bir veri merkezi planlanırken veya uygun bina seçiminde, çevresel etkilerden kaynaklanabilecek olası tehlikeler mümkün olduğunca en aza indirilmelidir. Bu nedenle yetkisiz kişilerin erişimi, çatı veya bodrum katlardan olası su sızıntıları, elektro manyetik alan oluşturabilecek baz istasyonları veya jeneratör gibi etkenler dikkate alınmalıdır.

Veri merkezinde BT bileşenleri (sunucu, ağ bileşenleri ve depolama cihazları, vb.), altyapı ekipmanlarından (jeneratör, UPS, iklimlendirme sistemleri, vb.) farklı odalarda bulundurulmalıdır. Veri merkezinin teknik altyapısı da aynı şekilde ayrı odalarda kurulmalıdır.

Dış dünyayla iletişimde yer alan aktif ağ bileşenlerine (routers, switches, vb.) ilişkin güvenlik gereksinimlerinin, veri merkezinin en kritik alanına ilişkin güvenlik gereksinimleriyle aynı olduğu düşünülerek planlama yapılmalıdır. Bu yüzden telekomünikasyon ve iletişim bileşenleri için kullanılacak güvenlik önlemlerinin iç bileşenler ile aynı seviyede olması sağlanmalıdır. Fiziksel güvenliğin yanı sıra, bu bileşenlerin barındırıldıkları alanların alarm sistemleri ile güvenli hale getirilmesi de düşünülmelidir.

Bu sebeple,

- İletişim teknolojisi bileşenleri,
- İklimlendirme ve havalandırma,
- Güç kaynakları,
- Depo, vb.

için ayrı odalar oluşturulması (isteğe bağlı olarak ayrı yangın bölümünde) tavsiye edilmektedir.

Planlama sırasında, bina içerisinde yer alan boru hatlarının (örneğin su ve gaz boruları - bkz. VRM.2.U18 Su sızıntısına karşı koruma) veri merkezinin yakın çevresinde bulunmaması ya da hassas alanlarından geçmemesi sağlanmalıdır. Benzer şekilde örneğin veri merkezinin hemen üstünde, mutfak, tuvalet, vb. alanlardan kaçınılmalıdır.

Veri merkezi için yapısal değişiklikler veya yeni kurulumlar planlanırken, aşağıda açıklanan parametreler hesaba katılmalıdır.

Pratikte, sistem odaları için 1:1 ile 2:3 aralığında değişen uzunluk/genişlik oranları uygun görülmektedir. Bu oranlarda oluşturulacak bir sistem odası, BT bileşenlerinin yerleşim düzeni ve kablolama açısından kolaylık sağlayacaktır.

Binanın fiziksel koşulları izin veriyorsa, kritik alanlarda “yükseltilmiş zemin” kullanılması önerilir. Yükseltilmiş zemin yüksekliği, veri merkezinin kullanım amacına ve barındırılacak BT bileşenleri ile altyapı ekipmanlarına bağlı olarak değişebilir. Yükseltilmiş zemin, iklimlendirme için kullanılacaksa en az 50 cm’lik net yüksekliğe sahip olması gerekir. Metrekare başına 1000 Watt üzeri ısı yükü olan veri merkezlerinde, 90-100 cm'lik net yükseklik önerilmektedir.

Veri merkezi boyutları belirlenirken, aşağıdaki önerilen ölçülerden faydalanılması önerilir:

Tablo 6. Örnek Veri Merkezi Boyutları

Nesne	Yükseklik (metre)
Yükseltilmiş zemin ile tavan yüksekliği	3.00
Kapı genişliği	1.10
Kapı yüksekliği	2.10

Yükseltilmiş zemin, en az 10 kN / m2'lik bir yük taşıyacak şekilde tasarlanmalıdır.

Yükseltilmiş zemin düzgün bir şekilde döşenmeli, zemini tamamen kaplamalı, en az 20 cm'lik bir yükseklikte ve F30 yangın direnci sınıfında olmalıdır. Genel olarak konu ile ilgili güvenlik politikalarına uyulmalıdır (örneğin TS EN 12825 "Yükseltilmiş döşeme sistemleri" standardı).

Not: Yükseltilmiş zemin ve asma tavan, veri merkezindeki zemini veya tavanı tamamen kaplamalı, herhangi bir açıklık (güvenli olmayan giriş noktası) oluşturmamalıdır.

Koridorlar en az 1,80 metre genişliğinde olmalı ve yüksek yüklere dayanabilen, kaymayan, yumuşak zemin kaplamaları ile tasarlanmalıdır.

Veri merkezinde dikey taşıma güzergahları olarak kullanılan asansörler, en az 1500 kg'lık bir yük taşıma kapasitesine sahip olmalıdır. Asansör kabininin net derinliği, genişliği ve yüksekliği sırasıyla 2.80 m, 1.50 m ve 2.20 m olmalıdır.

Tüm veri merkezi güvenlik alanının yalnızca bir veya iki giriş kapısı olmalı, olası tüm giriş noktaları izlenmelidir (ayrıca bkz. VRM.1.U22 Güvenli Kapı ve Pencereler). Erişim, yüksek kaliteli erişim kontrol sistemleri ile kontrol edilmelidir (ayrıca bkz. VRM.2.U6 Erişim kontrolleri). Veri merkezinde mümkünse pencere bulunmaması sağlanmalıdır.

Bir veri merkezi için izinsiz girişlere yönelik, uygun yapısal ve teknik önlemler son derece önemlidir. Bu konuda ek tavsiyeler “VRM.1.U27 Hırsızlığa Karşı Koruma” maddesinde yer almaktadır.

Veri merkezleri yüksek korunma gerektiren alanlar olduğu için, yalnızca ilgili yetkililerin (örneğin BT bileşenlerini yöneten sistem yöneticileri) veri merkezine erişmesine izin verilmelidir. Kullanılacak erişim kontrolleri ile gerek kurum çalışanlarının, gerekse geçici görevlilerin (örn. veri merkezi bakımını gerçekleştirmek için görevli bir firma çalışanı), kendi faaliyet alanı dışındaki sistemlere erişememeleri sağlanmalıdır.

Veri merkezi içerisine, kurumun kontrolünde olmayan mobil BT bileşenleri, taşınabilir bellekler, kişisel cep telefonları veya kameralar gibi cihazların veri merkezine sokulmasına izin verilmemesi önerilmektedir.

Çoğu durumda, veri merkezlerinde bulunan BT bileşenleri için yüksek seviyede erişilebilirlik gerekmektedir. Bu gereksinimlerin karşılanabilmesi için altyapı ve teknik tesislerin yedekli tasarımı düşünülmelidir (bkz. VRM.2.U29 Teknik altyapıda yedeklilik, modülerlik ve ölçeklenebilirlik).

VRM.2.U2 Yangın bölgelerinin oluşturulması [Planlama sorumlusu]

Yangın bölgelerinin oluşturulması, bir veri merkezinin yangından korunması için son derece önemlidir. Yangın ve dumana dayanımlı bölgelerinin önemi, birçok büyük yangında ortaya çıkmıştır.

Veri merkezlerindeki yangın bölgelerinin gereksinimleri, bazı yönetmelikler ve standartlarda açıklanmaktadır. Yangın bölgelerinin oluşturulması sırasında Bakanlar Kurulu tarafından kararlaştırılan ve Resmi Gazete’de yayımlanan bina yangın korunma yönetmeliği gereksinimlerine uyulmalı, mevcut yangın koruma standartları (örn. TSE 11925, ISO 11925, DIN 4102 standartları) ve bina denetim şartları mutlaka dikkate alınmalıdır.

Yangın bölgesinin amacı sadece binayı ve içindeki kişileri korumak değil aynı zamanda içerisinde yer alan BT bileşenlerini ve bu bileşenlere erişilebilirliği de sağlamaktır. Bu

bölgeler, yangın alevleri ve sıcak dumanın genişlemesini önleyeceği gibi ısı ve soğuk dumanın da yayılmasını önlemektedir.

DIN 4102 standardına göre izin verilen termal radyasyon seviyesi bile, özellikle ısıya duyarlı BT bileşenleri ve altyapı ekipmanları üzerinde olumsuz etkilere neden olabilir. Bu sebepten dolayı, binalarda (ihtiyaca göre büyük veya küçük) birden fazla yangın ve duman bölgesi oluşturulması önerilmektedir.

Veri merkezi içerisinde ek yangın bölgelerinin gerekliliği ayrıca incelenmelidir. Kritik bileşenlerin bulunduğu bölgeler (BT odaları, veri arşivleri) için ayrı bir yangın bölümü oluşturulması gerekiyorsa; duvarlar, kapılar, gerekli zemin ve tavan açıklıkları F90 yangın dayanıklılık sınıfı şartlarına uygun hale getirilmelidir.

DIN 4102'nin dikkate alınması gereken özelliklerine ek olarak; veri merkezlerinde, sistem odalarında ve veri arşivlerinde bulunan nem, BS EN 1047-2 standardı, bölüm 4.1'de belirtilen maksimum bağıl nem sınırlarının altında tutulmalıdır.

Veri merkezi yangın bölgesi içerisinde ofis birimleri yer alıyorsa, bu ofisler ile veri merkezi arasındaki F30 duvarları ve T30 kapıları kullanılması yeterli olacaktır. Bu durumda bulunan ofisler yangın alarm sistemine dahil edilmelidir. Veri merkezi ile operasyonel olarak ilişkisi bulunulmayan ofis birimleri için farklı yangın bölgeleri düzenlenmelidir.

Binada bulunan, yangına sebep olacak veya yangının büyümesine katkıda bulunacak tüm unsurlar bir yangın yükü (tehdidi) yaratır. Mobilyalar, zemin kaplamaları ve perdeler; BT bileşenleri ve kabloları kadar yangın tehlikesi oluşturmaktadır. Malzemelerin alev alması veya yanmazlığı hakkında daha fazla bilgiye TSE 11925, ISO 11925, DIN 4102 standartlarından ulaşılabilir.

Veri merkezinde ve bitişik odalarda mevcut yangın yüklerine önceden dikkat edilmelidir. Örneğin önemli verilerin yer aldığı disk arşivinin, kâğıt yığınlarının depolandığı odaların içerisinde veya yakınında bulunması tercih edilmemelidir.

VRM.2.U3 Kesintisiz güç kaynağı (UPS) kullanımı [Bina hizmetleri]

Veri merkezinde yer alan kritik BT bileşenlerinin, elektrik kesintilerinden en az biçimde etkilenmesi için kesintisiz güç kaynağı (UPS) kurulmalıdır. UPS kullanımı ile:

- Ani enerji kesintilerinde sistemlerde oluşabilecek donanımsal arızaların, veri bozulmalarının ve veri kayıplarının engellenmesi,
- Enerji kaynağı üzerinde meydana gelebilecek gerilim dalgalanmaları, harmonikler, gürültü vb. anormalliklerin sistemlere zarar vermesinin önlenmesi,
- Jeneratörler devreye girene kadar geçen sürede sistemlerin çalışabilmesi için gerekli enerjinin sağlanması

amaçlanır.

UPS'ler, IEC 62040-3 standardı içerisinde üç farklı sınıfa ayrılmıştır. Bunlar:

• Gerilim ve frekans bağımlı UPS (VFD-UPS: Voltage and Frequency Dependent UPS)

Off-line UPS olarak da bilinir. Bu çalışma modunda, şebeke BT bileşenlerini direkt olarak beslemektedir. Ancak elektrik kesintisi olduğunda gerekli enerji UPS akülerinden sağlanır, dolayısıyla UPS'e bağlı BT bileşenleri elektrik kesintisini hissetmez. UPS akülerinden beslemenin başlaması için 10 ms kadar bir süre gerekebilir. Bu süre bazı BT bileşenleri için uzun sayılabilir. Ayrıca şebekenin BT bileşenlerini direkt beslediği durumda, herhangi enerji herhangi bir düzeltme işlemine tabi tutulmadan direkt olarak aktarıldığı için, şebekeden kaynaklı bütün olumsuz durumlardan BT bileşenleri de etkilenecektir.

• Gerilim bağımsız UPS (VI-UPS: Voltage Independent UPS),

Line Interaktif UPS olarak da bilinir. Bu çalışma şeklinde de BT bileşenleri şebekeden direkt olarak beslenir. Fakat şebeke gerilimi, belli bir oranda regüle edilerek (düzenlenerek) BT bileşenlerine aktarılır. Şebeke gerilimi belirli limit değerlerinin dışına çıktığı ya da tamamen kesinti yaşandığı durumlarda, aküler üzerinden besleme devam edecektir.

• Gerilim ve frekans bağımsız UPS (VFI-UPS: Voltage and Frequency Independent UPS)

Çift çevrim (on-line) UPS olarak da bilinir. On-Line UPS'lerde giriş şebekesinden doğrultulan enerji ara devreye aktarılır (birinci çevrim AC->DC). Ara devre bir taraftan UPS akülerini şarj ederken diğer taraftan eviriciye gerekli gücü sağlar. Hem ara devre, hem de aküler tarafından beslenen evirici, BT bileşenlerine gerekli gücü sağlar (ikinci çevrim DC->AC). Şebekedeki gerilim veya frekans değişimleri, çıkış tarafında BT bileşenlerine sağlanan enerjiyi hiçbir zaman etkilemez. Evirici aküler tarafından da beslendiği için şebekede kesinti yaşanması durumunda bile BT bileşenlerine gerekli enerji sağlanır. On-Line UPS'lerin, arıza yaptığında veya aşırı yüklendiğinde kendini koruyabilmesi için Static By-Pass üniteleri vardır.

UPS türleri kıyaslandığında, VFI UPS'nin en iyi performansa sahiptir ve hassas BT sistemleri için tercih edilmelidir. Ek özellikler göz önünde bulundurulduğunda, DIN IEC 62040-3 standardı içerisinde tanımlanan VFI-SS-111 sınıfı UPS, BT bileşenleri için en iyi tercih olarak öne çıkmaktadır.

Bilinenin aksine, UPS'ler tam anlamıyla aşırı gerilim koruması sağlamaz. UPS'ler normal işlevi bağlamında, kendisine bağlı olan cihazları yüksek gerilimlerden uzak tutabilir fakat aşırı gerilim korum cihazı olarak tasarlanmamışlardır. Hatta UPS'leri aşırı gerilime karşı korumak gerekir.

Bir UPS'i boyutlandırırken iki unsur önemlidir, besleme (destekleme) süresi ve güç faktörü (çıkış gücü değeri).

Besleme süresi, elektrik kesintilerinde yüklerin, UPS tarafından kullanılan akülerde depo edilen enerji ile ne kadar süre ile besleneceğini belirtir bir büyüklüktür. UPS'nin besleme süresinin belirlenmesinde, UPS amacı, beslenecek BT bileşenlerinin sayısı ve niteliği, kurum tarafından kullanılan diğer yedek güç önlemlerinin varlığı dikkate alınmalıdır.

Eğer şebekede yaşanan dalgalanmalarda, kısa süreli elektrik kesintilerinde UPS tarafından sağlanan enerji, BT bileşenlerinin işlemlerine sorunsuz devam etmesi için yeterli oluyorsa, UPS tasarımının bu durum göz önünde bulundurularak gerçekleştirilmesi önerilmektedir. Elektrik kesintilerinin çoğunluğu birkaç dakika sürdüğünden, 10 ila 15 dakika arasında bir besleme süresi yeterli görülebilir.

Diğer taraftan, kısa süreli kesintilerden dahi BT bileşeninin işleme devam edebilmesi için düzgün biçimde kapatılması gerekiyorsa, kısa besleme süresi yeterli olmayacaktır. Bu durumda, elektrik kesintisi oluştuktan sonra bir süre beklemek ve sistemleri hemen kapatmamak en iyisidir. Kapatma öncesi yaklaşık 10 dakika bekleme süresi uygundur. BT bileşenlerinin kapanma süreleri, bileşenler arasında büyük farklılık gösterir, UPS'e bağlı olan her BT bileşeni için ayrı olarak belirlenmelidir. Bu tür durumlarda besleme süresini hesaplarken, aşağıdaki temel kuraldan yararlanılır:

Besleme süresi = bekleme süresi + kapanma süresinin iki katı.

Besleme süresi değerleri genellikle 30 ila 60 dakika arasında değişir. Kapatma süresinin iki katına çıkarılması ek bir koruma tamponu oluşturur.

Özel durumlarda (örn. telekomünikasyon sistemleri), gerekli besleme süresi birkaç saat olabilir. UPS tarafından beslenen bileşenler değiştirildiğinde veya UPS'e yeni bir bileşen eklendiğinde, mevcut besleme süresinin yeterli olup olmadığı tekrar kontrol edilmelidir.

Besleme süresi, akü sayısı ve kapasitesi (Ah) ile orantılıdır ve ilave aküler ile güç kaynağı kapasitesi artırılabilir. Güç faktörü (çıkış güç değeri) için ise aynısını söylemek mümkün değildir. Bu değer UPS'te yer alan düzeltici (rectifier) ve evirici (inverter) içindeki elektronik parçalara bağlıdır. Güç faktörü UPS tarafından sağlanabilen asgari besleme kapasitesini belirler. Örneğin 100 kVA'lık bir UPS, 0.8 oranında bir güç faktörüne sahip ise, (100*0,8=80) 80 kW'lık bir çıkış gücü sağlayabilir. Ekstra ekipman ekleyerek güç faktörünü artırmak genellikle imkânsızdır, güç faktörünün artırılabilmesi ancak kapsamlı değişikliklerle mümkündür. UPS'in istenilen kapasitede çıkış gücü sağlayabilmesi için, (genellikle aküler tarafından sağlanacak olan) yeterli bir güç rezervinin planlanması gerekir.

Bir UPS'nin en hassas kısmı akülerdir. Aküler, sadece imalatçı tarafından belirlenen uygun sıcaklık değerlerine sahip (genellikle 20-25 ° C civarına) alanlarda, maksimum performans ve hizmet ömrüne ulaşabilirler. Ortam sıcaklığının belli bir oranda artması, akü performans ve ömrünün belirli bir oranda azalmasına neden olur (8,3 ° C'lik sıcaklık artışı, akü ömrünü %50 oranında azaltmaktadır). Dolayısıyla büyük veri merkezi ve sistem odalarında, akülerin farklı odalarda tutulması önerilmektedir. Özellikle büyük UPS tasarımlarında, aküler ve yüksek ısı üreten güç devreleri hiçbir şekilde ortak bir odada bulundurulmaması gerekmektedir.

Diğer tüm elektrikli cihazlarda olduğu gibi, UPS'lerin yer aldığı odalar içerisinde üretici tarafından belirtilen iklim koşullarının sağlanması gerekir. Gerek UPS, gerekse akülerin bulunduğu odalar doğru biçimde iklimlendirilmelidir. Odalar için gerekli soğutma kapasitesi belirlenirken, üreticinin önerdiği sıcaklık aralıkları dikkate alınmalıdır.

UPS'nin gerekli besleme süresini karşıladığını güvence altına almak için, gerçek besleme süresi yılda bir kez test edilmelidir. Bu amaçla bazı UPS sistemleri içerisinde yerleşik test mekanizmaları bulunur. Yerleşik test mekanizmaları içermeyen UPS sistemlerinin besleme süreleri bir yük testi ile belirlenebilir.

UPS, BT bileşenlerinin erişilebilirliği açısından son derece önemli bir altyapı ekipmanıdır. Bu nedenle beslediği BT bileşenleri kadar korunması ve ihtiyaca göre yedeklenmesi gerekir. Buna ek olarak, UPS'nin yetkisiz erişime, yangına ve suya karşı korunması hususunda özel dikkat gösterilmelidir. Yangına karşı ciddi bir koruma sağlamak için yedekli UPS ünitelerinin ayrı yangın bölgelerinde muhafaza edilmesi önerilir. Bu sayede bir UPS ünitesi yangından etkilense de, yedek UPS ünitesi çalışmaya devam edebilecektir.

Bir UPS'nin koruyucu etkisini sürdürebilmesi için, bakımları düzenli olarak yapılmalıdır. Bu sebeple üretici tarafından belirtilen bakım çizelgesi izlenmelidir.

VRM.2.U4 Acil durumlarda elektrik iletiminin kapatılması [bina hizmetleri]

Elektrikli cihazlar çalışırken ortama ısı yayarlar. Cihaz yoğunluğunun fazla olduğu odalarda, ısı artışı daha hızlı meydana geldiği için yangın riski önemli ölçüde artar. Yangın riskinin fazla olduğu bölümlerde ve acil bir durumda, veri merkezinin elektrik bağlantısını hızlı bir biçimde kesebilmek için, acil durum devre kesicilerin kurulması planlanmalıdır. Örneğin bir acil durdurma (emergency power off – EPO) anahtarı kurulması düşünülebilir.

Genellikle önceden belirlenmiş bir kişi tarafından çalıştırılması gerekecek olan acil durdurma anahtarının, ulaşılabilir fakat korunan (kaza veya yanlışlık ile kullanılmayacak) alanlarda bulunması önerilir. Özellikle çalışanların bulunmadığı (veya ender bulundukları) alanlarda, yangın algılama sistemlerine entegre acil kapatma sistemleri daha etkilidir.

Elektrik iletiminin acil durumlarda kapatılması ile önemli bir yangın kaynağı riski bertaraf edilebilir ve ufak yangınların büyümesi engellenebilir. Ayrıca yangın ile uğraşılırken elektrik çarpması gibi durumların önüne geçilmiş olur.

Kesintisiz güç kaynaklarının (UPS'ler) harici güç kaynağı kapatıldıktan sonra otomatik olarak devreye girip enerji sağlamaya başlayacakları ve buna bağlı BT bileşenlerinin işlemlerini sürdürecekleri dikkate alınmalıdır. Bu tarz bir mekanizma yardımı ile gerekli bir durumda harici elektrik kaynağının bağlantısı yanı sıra tüm UPS sisteminin kapatılması sağlanmalıdır. Bu nedenle acil durdurma anahtarının, acil durumlarda tüm güç kaynaklarını kapattığına emin olunmalıdır.

Acil durdurma anahtarının, veri merkezi giriş kapısına veya yakınlarına monte edilmesi önerilmektedir (kapı dışındaki bir konum göstergesi ile). Bununla birlikte, acil durdurma anahtarı kazara veya kasıtlı olarak çalıştırılabilir. Acil durdurma anahtarı kazara veya yetkisiz kullanılmaya karşı fiziksel olarak korunmalı, yanlışlıkla çalıştırılmaması için kilitli tutulmalıdır.

Olumsuz Örnek:

Orta ölçekli bir sistem odası yaklaşık 10 sunucu, 5 yazıcı ve diğer BT bileşenleri ile donatılmıştır. Odada duvarlar, pencereler ve kapılar hırsızlığa karşı koruma özelliklerine göre tasarlanmış fakat acil durdurma anahtarı düşünülmemiştir. Odanın iki şekilde elektriği kesilebiliyordu: bodrumdaki ana bina panosu veya oda içerisindeki giriş kapısının karşı duvarına yerleştirilen dağıtım panosu. Oda içerisindeki bir yangında, oda dağıtım panosuna ulaşılamaz konumda bulunmaktaydı. Bodrumdaki ana bina panosuna ulaşmak ise zaman alacaktı.

VRM.2.U5 Hava sıcaklığı ve nemi ile uyumluluk [Bina hizmetleri]

İklimlendirme sistemleri veri merkezinde sıcaklık ve nemi kontrol etmek için kullanılırlar. Bu konuda başvurulan kaynaklardan biri olan ASHRAE standardı, veri işleme ortamlarında 16-27 ° C arası bir sıcaklık ve çiğ noktası 15 ° C derece olan %40-55 arası nem oranını tavsiye etmektedir.

Veri merkezlerinde, BT bileşenlerinin çalışması sırasında ısınan havadan dolayı sıcaklık yükselir, bu yüksek sıcaklık elektronik cihazlarda ve BT bileşenlerinde işlevsel bozukluklara sebebiyet verebilir. Ortam sıcaklığı kontrol edilerek, BT bileşenleri içerisinde yer alan elektronik parçalar üretici tarafından belirlenen sıcaklık değerlerinde tutulmalıdır. İklimlendirme sistemleri ayrıca, çiğ noktasının altında soğutarak nemi kontrol ederler.

Bir veri merkezinde bağıl nem ile ilgili olarak iki olası tehlike bulunur:

- Elektrostatik deşarj: Nem çok düşük olduğunda gerçekleşir. Ayrıca, elektrostatik deşarj olasılığı sıcaklık düşük olduğunda artar. İnsanlar tarafından oldukça zor fark edilebilir ve genelde yaralanmalara yol açmaz. Ancak 10 Volt değerindeki bir deşarj donanıma zarar verebilir.
- Korozyon: Bu durum metalik bir donanım, donanım ıslandığında veya yüksek nemden dolayı havadaki su yoğunlaşması sonucu donanım küçük damlalara maruz kaldığında oluşur. BT bileşenlerinin içerisindeki elektronik parçalar hasar görebilir ve veri kaybı yaşanabilir.

Bu amaçla, veri merkezi içerisinde iklimlendirme sistemleri kullanılarak uygun iklim koşulları oluşturulmalıdır. Veri merkezi içerisinde soğutulan alanlardaki gerçek ısı yükü, düzenli aralıklarla (veya veri merkezi içerisinde kapsamlı ve büyük değişiklikler yapıldıktan sonra) kontrol edilmelidir.

Ayrıca kullanılan iklimlendirme sisteminin bakımları düzenli olarak yapılmalı, ortam sıcaklığı ve nem sürekli izlenerek kayıt altına alınmalıdır. Takibi yapılan sıcaklık ve nem değerlerinde anormal sapmalar olması durumunda, gerekli düzeltici faaliyetler uygulanacak şekilde planlamalar yapılmalıdır.

VRM.2.U6 Erişim kontrolleri [Bina hizmetleri, BT operasyon uzmanı, Bilgi güvenliği sorumlusu]

Veri merkezi ve/veya sistem odaları, içerisinde yer alan tüm BT bileşenleri ile kritik alan olarak kabul edilmeli ve yetkisiz erişime karşı korunmalıdır. Bir erişim yönetmeliği/prosedürü/politikası yardımı ile veri merkezine, sadece görev tanımları gereği o alanda çalışmakla yetkilendirilmiş kişilerin erişebilmeleri sağlanmalıdır. Yetkili kişilerin (kurum içerisinden veya dışarısından), ne kadar bir süre boyunca, veri merkezi içerisinde yer alan hangi alanlara erişmeleri gerektiği belirlenmeli, kişilere gereksiz veya çok geniş erişim haklarının verilmesi engellenmelidir.

Düşük koruma gereksinimlerine sahip sistem odalarına erişim, genellikle kullanıcının sahip olduğu bir nesne (örneğin giriş kartı) veya kullanıcının bildiği bir bilgi (örneğin kullanıcı adı, PIN/parola, vb.) ile sağlanabilir. Kullanıcılar, kendilerine verilen giriş kartını kapıya yerleştirilen kart okuyucuya gösterir. Kart okuyucu, karttan edindiği kimlik bilgilerini, üzerinde yer alan (veya merkezi bir sunucuda bulunan) erişim listesi ile karşılaştırır, kullanıcının sistem odasına erişimini kabul ya da ret edileceği belirlenir. Okuyucudan geçen kart ile erişim listesindeki kod eşleşiyor ise erişim paneline entegre röle aracılığı ile manyetik kapı kilidi açılır. Gerçekleştirilen kart okuma işlemi ve sonucu (sistem odasına erişim kabulü veya reddi) kayıt altına alınır. Bu temel tanımlamalar dışında erişim paneline çeşitli özellikler eklemek mümkündür.

Yüksek koruma gerektiren veri merkezi ve/veya sistem odaları için daha kapsamlı erişim kontrol mekanizmaları gerekebilir. Örneğin yukarıda belirtilen kontrollerin her ikisi birden (kullanıcı giriş kartı ve PIN) kullanılarak çok faktörlü kimlik doğrulama gerçekleştirilebilir. Veya kullanıcının sahip olduğu bir nesne ve bildiği bir bilgiye ek olarak kullanıcıya ait biyometrik unsurlar (parmak izi, retina, vb.) kullanılabilir.

Veri merkezinde çalışma yapması gereken ziyaretçilerin veya harici personelin, bir yetkili kurum çalışanı nezaretinde (gerçekten ihtiyaç duyulması halinde) veri merkezine giriş yapması ve çalışmalarını icra etmesi; tüm girişlerin ve çıkışların kayıt altına alınması ve denetlenmesi sağlanmalıdır. Ziyaretçilere ziyaretleri boyunca eşlik edilmelidir. Ziyaretçilerin bina içerisinde veya çevresinde, belirli bölgelerde yalnız başlarına bulunmasına izin verilebiliyor olsa da veri merkezinde yalnız kalmalarına kesinlikle izin verilmemelidir. Veri merkezi personeli veya ilgili çalışanlar, bagaj/çanta açma, anahtar kartları paylaşma, yabancılar ile tesis içine girme riskleri konusunda eğitim almaları önerilmektedir.

Yetkili kişilerin kontrol edilen alana başka kişileri getirmesini önlemek için, aynı anda sadece ve sadece tek bir kişinin giriş yapmasına imkan sağlayacak bir erişim kontrol kabin (camlı turnike vs.) sistemi kurgulanabilir. Bu mümkün değilse, erişim kontrolüne yardımcı olmak için ilgili organizasyonel ve teknik yönetmelikler uygulanmalıdır. Teknik destek anti-pass back fonksiyonuyla (kişinin giriş yapmadan çıkış yapamaması/çıkış yapmadan giriş yapamaması kontrolü) sağlanabilir. Böylelikle aynı kartla binaya birden fazla kişinin veri merkezinin içerisine girmesi ve sistemin By-Pass edilmesi engellenir. Mükerrer giriş ve çıkışlara izin verilmemelidir.

Ayrıca veri merkezine tüm girişler ve çıkışlar, veri merkezi içerisinde gerçekleştirilen tüm faaliyetler izlenmelidir. Küçük ölçekli sistem odaları için daha basit (sadece giriş/çıkış) bir izleme gerçekleştirilebilir.

Düzenli aralıklar ile veri merkezi için tanımlanmış olan erişim kontrol mekanizmalarının kullanımına ilişkin düzenlemelere uyulup uyulmadığı kontrol edilmelidir.

VRM.2.U7 Kilitleme ve koruma [Çalışanlar, bina hizmetleri]

Veri merkezinde bulunan tüm kapılar daima kilitli tutulmalı ve hiçbir istisna uygulanmamalıdır. Kapıların gerekli korumayı sağlaması için, her hangi bir çalışma/uygulama sırasında dahi açık tutulmaması sağlanmalıdır. Hırsızlık ve kötü niyetli kişilerin BT bileşen ayarlarını veya veriyi değiştirmeleri gibi tehlikelerin yanında, açık kapı veya pencere aracılığıyla odanın içerisine girebilecek duman tehlikesi de unutulmamalıdır.

Veri merkezi ve altyapı ekipmanlarının barındırıldığı alanlardaki pencereler ve kapılar belirli aralıklar ile kontrol edilmelidir.

Eğer veri merkezi ve/veya sistem odalarında havalandırma pencereleri çok büyükse, bir saldırganın havalandırma kanalları boyunca ilerleyerek sistem odasına ulaşması ve kapağı açarak içeri girmesi mümkün olabilir. Havalandırma kapaklarından gelebilecek saldırılara karşı alınabilecek önlemler aşağıdaki gibidir:

- Sistem odasında havalandırma ihtiyacı yüksekse, bunu gidermek üzere tek bir büyük havalandırma penceresi yerine küçük ancak fazla sayıda havalandırma penceresi kullanılmalıdır. Küçük havalandırma pencerelerinin her biri, bir insanın sürünerek geçemeyeceği kadar küçük olmalıdır.
- Yukarıda önerilen çözüme alternatif ya da ek olarak, havalandırma pencerelerinin önündeki kapaklar tel ızgaralar ile kapatılabilir, daha sonra tel ızgaralar duvara (kaynaklanarak) sabitlenebilir.

Büyük pencereler ve cam duvarlar, dekoratif olarak çarpıcı olsalar da, kolayca kırılabilir olmaları nedeniyle farklı biçimlerde gerçekleştirilebilecek saldırılara neden olabilirler. Kırılan camdan içeri fırlatılabilecek bir yanıcı madde, yangın oluşumuna sebebiyet verebilir ya da sert bir cisimle camı kırarak içeri girebilecek bir saldırgan bilgisayar sistemlerini sonsuza dek çalışmaz hale getirebilir. Pencere ve cam duvar kaynaklı tehlikeleri azaltmak üzere, mümkün olduğunca sistem odasını çevreleyen duvarlar üzerinde cam kullanımından kaçınılmalıdır.

Bu unsurlara özellikle planlama aşamasından itibaren dikkat edilmelidir.

VMR.2.U8 Yangın alarm sisteminin kullanımı [Planlama sorumlusu]

Bir veri merkezinde, BT alanına özel uyarlanmış alarm, acil durum planları ve yangın koruma yönetmeliklerinin oluşturulmasına ek olarak, yangın alarm sisteminin kurulması son derece önemlidir.

Veri merkezlerinde oluşan tüm yangın hasarlarının % 90'ından fazlasını çevre yangınlardan kaynaklandığı tahmin edilmektedir. Bu sebeple sadece veri merkezi içerisinin değil, çevre alanların da yangın alarm sistemi tarafından izlenmesi önerilmektedir.

Özellikle yüksek koruma gereksinimleri bulunan BT alanlarının izlenmesi sırasında, tavanda bulunan dedektörlerin yanı sıra, yükseltilmiş zemine yangın algılama sistemleri kurulabilir.

Bir yangın durumunda hangi dedektörün tetiklendiği saptanabilmelidir. Yangın kaynağını ortaya çıkarmak ve yangının ne kadar yayılabileceğini belirleyebilmek hayati değer taşır.

Kurulum için önerilen yangın alarm sistemi asgari olarak aşağıdaki özellikleri içermelidir:

- (BT bileşenlerinin ve altyapı ekipmanlarının bulunduğu tüm odalarda) Yükseltilmiş zemin ve tavana monte edilen duman dedektörleri,
- Acil durum güç sisteminin yer aldığı odalarda maksimum sıcaklık veya sıcaklık farkı dedektörleri,
- Klima sistemini içeren tüm odaların yükseltilmiş zemin ve tavan duman detektörleri,
- Klima sisteminin giriş ve çıkış (supply and exhaust) kanallarındaki kanal dedektörleri,
- Dışarıdan alınan temiz hava kanalına yerleştirilecek, duman ve hava kirliliği dedektörleri.

Yangın alarm sistemi tarafından üretilen tüm mesajların, sürekli personel barındırılan merkezi bir yerden takip edilmesi önerilmektedir (örn. güvenlik odasından). Ayrıca gerekli durumlarda kısa süre içerisinde gerekli bildirimlerin yapılabilmesi için yerel itfaiye ile de direk bağlantı oluşturulmalıdır.

Örnek:

Bir toplantı esnasında, katılımcılardan biri yakınlardaki bir kimyasal tesiste büyük bir yangının ortaya çıktığını fark eder. Yangın dumanının veri merkezine ulaşmasından önce, yetkili kişi klima temiz hava vanasını kapatır. Bu önlem alınmasaydı, birkaç dakika sonra yangın dumanları, veri merkezine ulaşmış ve kritik cihazlara zarar vermiş olacaktı. Temiz hava kanalına yerleştirilebilecek dedektörler aracılığı ile bu tür bir tehlike durumunda, temiz hava vanasının otomatik olarak kapatılması sağlanabilir.

Tüm duman dedektörlerin ve yangın alarm sistemini oluşturan diğer cihazların işlevsellikleri düzenli olarak kontrol edilmelidir. Belirli aralıklarla ve örnekleme yöntemiyle görsel olarak seçilen dedektörlerin işlevselliği test edilmelidir. Yangın alarm sisteminin farklı bir dış firma/kurum tarafından işletilmesi durumunda dahi, kurum bünyesinde yangın alarm sisteminden sorumlu, mümkünse en az iki kişi belirlenmelidir. Bu kişilerin yangın alarm sisteminin temel fonksiyonları ve yönetimi konusunda yeterli bilgi ve birikime sahip olmaları sağlanmalıdır.

VRM.2.U9 Yangın önleme veya yangın söndürme sistemi kullanımı [Planlama sorumlusu]

Veri merkezinde, güncel yöntemler ve teknoloji kullanılarak bir yangın önleme ve söndürme sistemi kurulması gerekir. Sınırlı sayıda BT bileşenin bulunduğu sistem odalarında yeterli sayıda ve boyutta taşınabilir yangın söndürücülerin kullanılması yeterli

olabilir. Daha büyük veri merkezlerinde, erken algılama sistemi ile entegre çalışan bir otomatik yangın söndürme sistemi düşünülmelidir.

Veri merkezi/sistem odası gibi kritik alanlar için yangın algılama ve yangın durumunda zamanında uyarı yapılmasına yönelik önlemler, herkesin sağlığını ve yaşamını korumak için alınması gereken temel tedbirlerin başında gelir.

Yangın koruma önlemleri konusunda ilgili yangın güvenliği yönetmeliklerine ve gereksinimlerine uyulması; ulusal bina yönetmeliklerinin ve standartlarının dikkate alınması ve bina büyüklüğüne ve kullanımına uygun bir yangın koruma yaklaşımı oluşturulması önerilmektedir.

Çoğu büyük yangın, ilk başta kolayca kontrol edilebilecek küçük yangınların genişlemesiyle oluşur. Özellikle ofis ortamlarında yangın, hızlı yayılabileceği yangın yükleri bulur. Bu nedenle yangınların olabildiğince erken kontrolü son derece önemlidir.

Veri merkezi ve/veya sistem odalarında yangının hızlı bir şekilde söndürülebilmesi için, taşınabilir yangın söndürücülerin (TS 862-3, DIN EN 3-3 standartlarına uygun) yeterli sayıda ve büyüklükte bulunması gereklidir. Taşınabilir yangın söndürücülerin büyüklükleri ve sınıfları konusunda yerel itfaiyeden görüş alınması önerilir.

Taşınabilir yangın söndürücülerin, yangın durumunda kolayca ulaşılabilecek bir yerde bulundurulması gerekir. Çalışanlar kendilerine en yakın taşınabilir yangın söndürücünün bulunduğu yeri bilmeli veya uygun işaretler yardımıyla söndürücülere hızlıca erişebilmelidir.

Taşınabilir yangın söndürücülerinin ağırlıklarının 20 kg üzerinde olmasına genellikle izin verilmez. Genellikle bina içerisinde bulunan 6 ve 12 kg'lık söndürücülerin doğru şekilde kullanılması ile öngörülenden daha büyük yangınları söndürmek mümkündür. Ancak bilinçsiz kullanımlarda, taşınabilir yangın söndürücü içerisinde bulunan söndürücü madde, sadece birkaç saniyede tamamen boşalabilir. Bu nedenle, çalışanlara yangın güvenliği eğitimleri verilmeli, eğitimler sırasında taşınabilir yangın söndürücülerin kullanımı ve çalışma mantığı da öğretilmelidir.

BT bileşenleri ve altyapı ekipmanlarına ciddi oranda hasar verebileceği için yangın sınıfları:

- A sınıfı: Kâğıt, ahşap, kumaş, kâğıt gibi katı madde yangınları,
- B sınıfı: Akaryakıt, solvent, tiner gibi yanıcı ve parlayıcı sıvı yangınları,
- C sınıfı: Metan propan, LPG gibi yanıcı ve parlayıcı gaz yangınları

olan ve yangın söndürme maddesi olarak toz kullanan yangın söndürücülerin, özellikle veri merkezleri ve altyapı ekipmanlarını barındıran alanlarda kullanılmaması önerilir. Bu tip

alanlarda sadece insan sağlığını tehdit etmeyecek, yangın söndürme maddesi olarak gaz içeren yangın söndürücülerin kullanılması sağlanmalıdır.

Taşınabilir yangın söndürücülerin düzenli kontrolü ve bakımı TS 11748 standardına göre yapılabilir. Yangın söndürme cihazlarının doldurulmasını ve bakımını yapan üretici veya servis firmaları Sanayi ve Ticaret Bakanlığı tarafından dolum ve servis yeterlilik belgesine sahip olmalıdır. Yangın söndürücü üzerinde yer alan bir etikette, yangın söndürücü cinsi, gaz tipi, ağırlığı, doldurulduğu tarih, bulunacağı yer, sorumlu kişi, aylık kontrol tarihi ve imza gibi bilgiler yer almalıdır. Yangın söndürücülerin aylık rutin genel durum kontrollerinin yanı sıra, altı ayda bir gaz ağırlık ölçümleri, yılda bir söndürücü madde nitelik kontrolleri, beşer yılda bir tüp niteliği kontrolleri düzenlenmesi önerilir. Ayrıca, bu tür düzenli denetimler sırasında özel erişim kısıtlamaları bulunan alanlardaki yangın söndürücülerin unutulmaması da önemlidir.

VMR.2.U10 Altyapı kontrol ve bakım çalışmaları [Bina hizmetleri, BT operasyon uzmanı, bakım personeli]

Üretici firma tarafından belirtilen tavsiyelere veya kullanılmakta olan bileşenlere ilişkin standartlara uygun olarak, düzenli aralıklar ile veri merkezi altyapı ekipmanları kontrol edilmeli ve bakım faaliyetleri gerçekleştirilmelidir. Kontroller, ekipmanın güncel durumu hakkında doğru bilginin edinilmesine yardımcı olurken, bakım çalışmaları ekipmanların sorunsuz bir biçimde çalışabilmelerini sağlamak için önleyici önlemler alınmasını sağlar. Örneğin, parçaların aşınmadan değiştirilmesi ile ekipmanın herhangi bir kesinti yaşamadan çalışmaya devam etmesi sağlanabilir.

Kontrol ve bakım çalışmaları, yoğun olmayan saatlerde yapılmalıdır. Bu iş düzenli ve bilinçli şekilde yapılırsa, bileşen arızası nedeniyle kesinti yaşama ihtimali azalacaktır. Aksi takdirde, bir bileşen arızası daha kapsamlı tamir çalışması gerektirebilecek ve sonuç olarak belki de bu durum, operasyonun daha uzun süre aksamasına neden olabilecektir.

Bakım çalışmaları ile sistemlerin erişilebilirliği ve ekonomik bir biçimde işletilmesi güvence altına alınır. Örneğin, bir iklimlendirme sistemine ait filtrelerin düzenli olarak temizlenmesi veya değiştirilmesi, iklimlendirme performansı, verimliliği ve işletme maliyetlerinin azaltılması açısından oldukça önemlidir.

Üretici tarafından belirtilen kontrol ve bakım aralıkları, gerçek koşulları yansıtacak şekilde uyarlanmalıdır. Örneğin belirli parçaların, üreticinin belirttiğinden çok daha erken aşındıkları tespit edilirse, önerilen bakım aralıkları kısaltılmalıdır. Aynı zamanda bu gibi bir durumda, mümkünse, parça ömrünün beklenenden kısa sürmesinin nedenleri belirlenmeli ve ortadan kaldırılmalıdır.

Gerçekleştirilen çalışmalar, çalışmanın zamanı, çalışmayı gerçekleştiren kişi(ler), gerçekleştirilen faaliyet detayları vb. bilgiler ile birlikte kontrol ve bakım günlükleri içerisinde kayıt altına alınmalıdır.

VMR.2.U11 Altyapı ortam izleme [Bina hizmetleri, BT operasyon uzmanı]

Altyapı ekipmanları (ve bu ekipmanları yönetmek için kullanılan sistemler) tarafından üretilen tüm arıza mesajları kayıt altına alınarak ilgili kişilere iletilmelidir. Özellikle iklimlendirme, elektrik ve UPS sistemleri (bir izleme sistemi vasıtasıyla) otomatik olarak izlenmeli ve gerekli durumlarda ilgili ekiplerin mümkün olduğunca hızlı faaliyete geçmesi sağlanmalıdır.

Bir veri merkezinde aşağıdaki sistemler izlenebilir:

BT'yi destekleyen sistemler:

- Bina ve erişim denetimi ve güvenliği,
- Sistem odası iklimlendirme ekipmanları,
- Elektrik sağlama ve dağıtımı,
- Soğutma sistemlerinin verimliliği ve devamlılığı.

BT Sistemleri (BT ile doğrudan ilgili olan sistemlerdir):

- Dış bağlantılar,
- Ağ cihazları,
- Sunucu sistemleri,
- Depolama sistemleri.

Veri merkezinin kritik ortam parametreleri, sıcaklık, nem, su kaçağı veya baskını, duman, hava akışı, hareket, sarsıntı, kapı erişimi ve ışık şiddeti seviyesi vb. izlenmesi, kullanılacak farklı dedektörler sayesinde sağlanabilir.

Veri merkezi altyapısının izleme adımları aşağıdaki şekilde listelenmektedir:

1.ADIM – İZLEME

Ana üniteler ve dedektörler ile donanımsal izleme:

- Sıcaklık
- Nem
- Su kaçağı veya baskını (Su Algılama kablosu üzerinden)
- Hava Akışı
- Enerji analizi (3 faz üzerinden gerilim, akım, frekans, reaktif güç, kapasitif güç, güç faktörü vb.)
- Duman

- Kapı durumu, açık / kapalı
- Hareket dedektörü
- Proximity Geçiş Entegrasyonu
- IP kamera
- Tüm kuru kontak & dijital giriş unsurları
- Tüm analog girişler
- UPS, Jeneratör, Hassas Klima, Doğrultucu, Enerji Analizörleri, Telekom Ekipmanı vb.

2.ADIM – ALARM BİLDİRİMİ

- SMS
- E-mail
- Sesli Arama
- Sinyal Kulesi ve Sesli İkaz
- LCD modülü üzerinden
- SNMP trap mesajları ile network üzerinden vb.

3.ADIM – YÖNETİM

Donanım bazlı yönetim:

- İklimlendirme sistemleri, aydınlatma armatörleri, elektronik cihazların elektik altyapısı üzerinde herhangi bir harici cihaz, kurulacak bir röle çıkışı üzerinden elektriksel olarak açılıp kapatılabilir veya aynı şekilde yazılımlar üzerinden güç dağıtım birimi PDU üzerinden yönetilebilir.

Yazılım bazlı yönetim:

- Herhangi bir harici cihaz eğer desteği varsa RS-232, RS-485, Modbus, SNMP, vb. bağlantılar ve protokoller üzerinden yönetilebilir.

4.ADIM – RAPORLAMA & ANALİZ

- Dönemsel analiz raporlarının oluşturulması,
- Risk Yönetimi
- Altyapı maliyetlerinin kontrolü
- Operasyon maliyetlerinin düşürülmesi
- Hizmet kalitesinin artırılması

Merkezi izleme yazılımı yedekli biçimde kurulmalı; gerekli tüm kayıtları üretebilen, kaynaklardan kayıtları alıp bunları sayısal veri olarak saklayabilen, rapor ve alarm üretebilen, geçmişe dönük verilere ulaşabilen bir yapıda olmalıdır.

İzlenecek unsurlara ilişkin, en uygun çalışma koşullarını yansıtacak, normal ve eşik değerleri belirlenmeli, belirlenen eşik değerlerin aşılması durumunda ilgili personele uyarı mesajlarının gönderileceği bir alarm mekanizması kurgulanmalıdır.

Daha ufak çaplı kurumlarda, sistem odası içerisinde yer alan ve genellikle az sayıda kişi tarafından işletilen BT ve destek ekipmanları da uzaktan izlenmeli ve gerekli durumlarda sorumlu çalışanlar tarafından vakitli olarak uyarılmalıdır.

2.2 2.SEVİYE UYGULAMALAR

1.seviye uygulamalar sonrasında, veri merkezi ve/veya sistem odalarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar, aşağıdaki uygulama maddelerini dikkate alarak, iyileştirme/geliştirme faaliyetlerini planlayabilirler.

VRM.2.U12 Veri merkezi için çevre koruma tasarımı ve uygulanması [Planlama sorumlusu, bina hizmetleri]

Veri merkezinin içerisinde bulunduğu binanın güvenliği ile birlikte, çevrenin korunması için de gerekli önlemler alınmalıdır. Özellikle veri merkezine giriş yapacak kişiler ve onları taşıyan araçlar için erişim kontrolünün ilk aşaması çevre koruması ile başlatılabilir.

Veri merkezinin yer aldığı bölge, koruma gereksinimleri ve çevresel etmenler (veri merkezinin şehir merkezine, karakola, hastaneye, vb. yakınlığı gibi) göz önünde bulundurularak, çevre koruma önlemleri oluşturulmalıdır. Çevre koruma önlemleri arasında:

- Bina/kampüs dış muhafazası,
- Bina/kampüs sınırının kasıtsız olarak geçilmesine karşı ihtiyati tedbirler,
- Bina/kampüs sınırının kasıtlı, şiddet içermeyen aşılmasına karşı alınacak önlemler,
- Bina/kampüs sınırının kasıtlı olarak, şiddet yoluyla aşılmasına karşı alınacak tedbirler,
- Açık hava güvenliği (dış güvenlik) önlemleri,
- Bina/kampüs giriş/çıkış kontrolü,
- Harici yolcu ve araç tanımlaması (görsel ve/veya sensor sistemleri ile erişim kontrolünün ilk adımı olarak görülebilir ve yetkisiz erişime karşı koruma sağlar. Güvenlik görevlilerine bu sorumluluk verilebilir.)

Çevre koruma önlemlerinin uygulanmasından önce, bina ve çevre için yukarıda belirtilen hususları ve binanın korunmasını kapsayan, tutarlı bir güvenlik konsepti hazırlanmalıdır (bkz. VRM.1.U23 Güvenlik bölgelerinin oluşturulması). Doğru ihtiyaç analizi ve planlama yapılmaması, gereksiz (ve çoğu zaman maliyetli) güvenlik önlemlerinin uygulanmasına neden olabilir.

Güvenlik konseptinin amacı, mevcut kaynakları kullanarak mümkün olan en etkin önlemleri uygulamak olmalıdır. Bu, özellikle çevre koruması için geçerlidir. Bu alanda uygulanan güvenlik önlemleri genel güvenlik düzeyini artırmalı ve sadece "yüksek güvenlikli bir alan" imajı vermemelidir (örneğin, profesyonel bir hırsızı yüksek çitler ve video gözetim kameraları caydıramayacaktır).

VRM.2.U13 Alarm sistemlerinin planlanması ve kurulumu

Bina/kampüs ve veri merkezi için birbiriyle uyumlu, tutarlı ve birlikte çalışabilecek alarm sistemlerinin kullanılması gerekir. Bu amaçla; kullanılacak alarm sisteminin türü öncelikle belirlenmeli, alarm sisteminin kullanılacağı alanlar planlanmalı, alarm sistemleri kurulmalı ve oluşan alarm mesajlarının ne şekilde yönetileceği kurgulanmalıdır.

Sistemin etkin ve verimli çalışabilmesi için alarm sistemi tarafından üretilen mesajlar, güvenlik odaları gibi sürekli bir personelin bulunduğu merkezlere iletilmelidir. Ayrıca bu merkezde bulunan ve alarmları karşılayacak personelin, gelen alarmlara tepki verebilecek kabiliyette olması sağlanmalıdır. Bu konularda kurumların özellikle "TS EN 50518 Görüntüleme ve alarm izleme merkezi" gereksinimlerine uymaları tavsiye edilmektedir.

Binanın farklı alanlarının, farklı kullanım biçimleri göz önünde bulundurularak, ihtiyaçlara uygun tehlike algılama, yönlendirme ve alarm üretme yaklaşımları gerekmektedir. Bu yaklaşım, alan kullanımlarındaki değişikliklere göre uyarlanabilir olmalıdır. Alarm sistemi, veri merkezi ve/veya sistem odasının risklerine göre planlanması ve kurulması gereken karmaşık bir genel sistemdir. Bu yüzden alarm sisteminin planlanması, kurulumu ve işletimi yetkin ve deneyimli uzmanlar tarafından gerçekleştirilmelidir. Bu yetkinlik şirket içinde mevcut değilse dış destek kullanılması düşünülmelidir. Örneğin, güvenlik gereksinimlerine ve binanın çevresel koşullarına göre seçilebilecek birçok farklı alarm sistemleri bulunur. Hırsızlık tespiti için hareket algılayıcılar, cam kırılma dedektörleri, video kameralar, vb. kullanılabilir. Fakat yangın için ihtiyaç duyulan dedektörler daha farklı olacaktır.

Dedektörler ve algılayıcılar farklı şekillerde birbirlerine bağlanabilir. Korunacak alanların türüne, boyutuna ve geçerli politikalara bağlı olarak, uygun sistemler seçilmeli ve kurulmalıdır. Bir alarm sistemi planlanırken veya genişletilirken, kablo kanal altyapısının (taşıma sistemlerinin) yeterli olmasına ve mümkün olduğunca kablolarda ve kablo yollarında az değişiklik yapılmasına dikkat edilmelidir.

Alarm sisteminin çalışırlığının güvence altına alınması için, düzenli bakımlar ve fonksiyon testleri gereklidir.

Veri merkezinde herhangi bir alarm sistemi mevcut değilse veya mevcut bir sistem aktif olarak kullanılamıyor ise başlangıçta sadece önemli alanlarda alarm dedektörlerinin yerel olarak kullanılması düşünülebilir. Yerel olarak çalışan alarm dedektörleri merkezi bir servise bağlanmadan tamamen bağımsız çalışırlar. Dedektör tarafından olağan dışı bir durum tespit edildiğinde, alarm sesli olarak, tehlikenin tespit edildiği bölgede üretilmeli veya basit bir kablo (çoğu zaman telefon kablosu) vasıtasıyla başka bir bölgeye iletilmelidir.

Bina/kampüs alanı ve/veya veri merkezi üzerinde gerçekleştirilen değişiklikler sonrası, alarm sistemi üzerinde gerekli uyarlamalar gerçekleştirilir.

VRM.2.U14 Jeneratör kullanımı

Elektrik dağıtım şirketleri, veri merkezine, her zaman, her koşulda kesintisiz enerji sağlamayı garanti edemezler. Elektrik şebekesinde yaşanan kesintilerin veri merkezini etkilememesini sağlamak için kullanılan UPS'ler ise sahip oldukları akülerden yararlanarak geçici bir süre BT bileşenlerini besleyebilirler. Bu yüzden şebekede yaşanacak olası bir kesinti durumunda veri merkezine enerji sağlayacak yedek sistemler düşünülmelidir. Veri merkezinin bulunduğu bölgede, enerji sağlayabilecek ikinci bir elektrik dağıtım şirketi veya şebeke yoksa ve veri merkezi erişilebilirlik gereksinimleri doğrultusunda yedeklilik gerekiyorsa, ikincil güç kaynağı olarak jeneratör düşünülebilir.

UPS (VRM.2.U3 Kesintisiz güç kaynağı (UPS) kullanımı), şebekedeki dalgalanmalar veya kısa süreli elektrik kesintilerini tolere edebilirken, jeneratör daha uzun süreli elektrik kesintilerinde veri merkezini besler.

Kullanılacak jeneratörü belirlerken kapsamlı bir yük analizi yapılması gereklidir. Veri merkezinde yer alan, jeneratör tarafından enerji yedeklemesi yapılacak tüm bileşenlerin ihtiyaçlarını karşılayacak güç tespitinin yapılması önerilir. Analiz sırasında sadece normal çalışma şartları değil, ilk kalkınma (çalışma) akımlarının da analizleri iyi yapılmalı, bu akımların jeneratör kontrol modülleri tarafından ayarlanabilecek değerleri geçmemesine özen gösterilmelidir. Bu değerlerin aşılması durumunda "yüksek akım arızası" nedeniyle kontrol modülü jeneratörü durduracaktır.

Jeneratörün yakıt seviyesi düzenli olarak kontrol edilmeli ve en az 48 saatlik çalışma için yeterli yakıt bulunması sağlanmalıdır. Erişilebilirlik gereksinimleri yüksek veri merkezleri için alt sınır 120 saate kadar çıkabilir. Yakıt stok miktarı belirlenirken, jeneratörün çalışması esnasında yakıt ikmalinin teknik ve lojistik olarak mümkün olup olmadığı dikkate alınmalıdır. Teknik uygunluk incelenirken, (özellikle dizel yakıt çalışan jeneratörlerde) yakıt ikmali sırasında tankta oluşacak türbülansın arızalara neden olup olmayacağı, dipte bulunan tortuların filtreleri tıkayıp tıkamayacağı incelenmelidir. Lojistik uygunluk

kapsamında, elektrik kesintisinin yakıt ikmalini engelleyip engellemeyeceği dikkate alınmalıdır.

Birincil güç kaynağının uzun süreli arızalanması durumlarında, BT operasyonlarının sürdürülebilmesi için gerekli enerji jeneratör tarafından sağlanır. Bu yüzden jeneratör, BT bileşenlerinin erişilebilirliği açısından son derece önemli bir altyapı ekipmanıdır. Beslediği BT bileşenleri kadar korunması ve özellikle yüksek erişilebilirlik gereksinimleri söz konusu olduğun da, ihtiyaca göre yedeklenmesi gerekir. Buna ek olarak, jeneratörünün yetkisiz erişime, yangına ve suya karşı korunması hususunda özel dikkat gösterilmelidir. Yangına karşı makul bir koruma sağlamak için yedekli jeneratörlerin ayrı yangın bölgelerinde muhafaza edilmesi önerilir. Bu sayede bir jeneratör yangından etkilense de, yedek jeneratör çalışmaya devam edebilecektir.

Acil durum güç kaynağının koruyucu etkisinin güvence altına alınması için iki unsur gereklidir:

- Düzenli bakım,
- Gerçek koşul testleri.

Jeneratörlerin belirli aralıklar ile kontrol edilmesi, bakımı, temizliği, yük ve fonksiyonel testleri yapılmalıdır.

Testlerin gerçek koşullarda yapılması özellikle önemlidir. Bu sayede, acil durumlarda tüm bileşenlerin sorunsuz ve birlikte çalışıp, sistemleri besleyeceği güvence altına alınır. Genellikle testler sırasında, şebeke elektriğinin, jeneratörün başarılı bir şekilde devreye sokulmasından sonra kapatıldığı gözlenmektedir. Bu tür bir uygulama gerçek hayatta ve (şebeke elektriğinin birden kesildiği) acil durumlarda, her şeyin planlandığı biçimde otomatik olarak çalışıp çalışmayacağına dair hiçbir bilgi sağlamaz. Yapılması gereken, aynen gerçek hayatta yaşanabileceği gibi, BT bileşenleri çalışır durumda iken birden şebeke elektriğinin kapatılması ve sonrasında, güç kaynağının otomatik olarak devreye girmesinin test edilmesidir. Ancak bu şekilde acil durumlarda yedekliliğin sağlanıp sağlanmayacağı tespit edilebilir. Aynı şekilde normale geri dönüş yolunun test edilmesi için, jeneratör tarafından BT bileşenlerine enerji sağlanırken, birincil güç kaynağı (şebek elektriği) tekrar açılmalı, sonrasında tüm jeneratör kaynaklarının otomatik olarak bekleme moduna geri dönüp dönmedikleri izlenmelidir. Jeneratör testleri en az iki yılda bir gerçekleştirilmelidir.

VRM.2.U15 Aşırı gerilimden korunma sistemleri

Veri veya elektrik ileten ağlarda (güç veya veri iletimi olup olmadığına bakılmaksızın) her an aşırı gerilim oluşabilir. Çoğunlukla bu tür aşırı gerilimlere, aynı şebeke içerisinde

bulunan diğer tüketiciler neden olur. Diğer taraftan, yıldırım nedeniyle oluşan aşırı gerilim daha az yaşanmakla birlikte, çok daha yüksek hasarlara yol açabilir.

Aşırı gerilimler, kullanılan (veri veya elektrik taşıyan) kabloların yanı sıra telefon hatları, su veya gaz boruları gibi elektriksel iletken hatlar ile de binaya ve BT bileşenlerine ulaşabilir, iç hatlara yansıyabilir.

BT bileşenlerini ve altyapı ekipmanlarını korumak için alınabilecek gerekli tedbirler, aşırı gerilimin oluşma nedenine bakılmaksızın esasen aynıdır. Yıldırım ve aşırı gerilimden korunma ile ilgili çeşitli standartlar bulunmaktadır. ISO 62305, IEC 61643-11, IEC 60634, UL 1449 bunlardan bir kısmıdır. Türkiye'de TS EN 62305-1/2/3/4 standardı yıldırıma ve aşırı gerilime karşı koruma oluşturmanın genel kurallarını açıklar. Standardın ikinci bölümü olan "Risk Yönetimi", yıldırım ve yıldırım sonucunda oluşabilecek aşırı gerilimin önlenmesine risk odaklı bir yaklaşım sunmaktadır. Üçüncü bölüm, yapıların ve kişilerin fiziksel olarak korunmasını, dördüncü bölüm "Yapılarda Elektrik ve Elektronik Sistemler" ise bina içerisinde yer alan elektrik ve elektronik sistemler için uygulanabilecek önlemleri ele almaktadır.

Kurumların aşırı gerilimden korunabilmeleri için, TS EN 62305 standardına uygun bir aşırı gerilim korunma konsepti oluşturulmaları gereklidir.

Aşırı gerilim korunma konsepti içerisinde; elektrik dalgalanmalarından ve aşırı gerilimden korunma cihazları, alternatif güç kaynakları (jeneratör sistemleri) ve kesintisiz güç kaynakları (UPS'ler) dikkate alınmalıdır. UPS'ler, kendisine bağlı ekipmanlara bir miktar koruma sağlamakla birlikte hiçbir şekilde aşırı gerilim koruyucusu olarak kabul edilmemeli, aksine aşırı gerilimden korunması gereken bir elektronik cihaz olarak düşünülmelidir.

Yıldırım akımının binaya nüfuz etme ihtimali, standartlara uygun olarak tasarlanmış dış yıldırımdan korunma sisteminin varlığı ile önemli ölçüde azaltılmaktadır. İç yıldırımdan korunma sistemi ise aşırı gerilim darbe koruyucuları kullanılarak oluşturulur. Aşırı gerilim darbe koruyucuları, yıldırım ve diğer aşırı gerilim kaynaklarının oluşturduğu gerilimleri önlemek için kullanılmaktadır. Cihaz yanmaları, telefon santrallerinin yanması vb. gibi durumlarla karşılaşmamak ve muhtemel bir yangını engellemek için aşırı gerilim darbe koruyucularının kullanılması gerekir.

Dış yıldırımdan korunma sistemlerinde iki temel sistem vardır. Bunlar;

- Pasif yakalama ucu
  a) Franklin Çubuğu
  b) Faraday Kafesi
- Aktif yakalama ucu: Paratoner

Pasif yakalama sistemlerinde, bina bir kafes içerisine alınacak şekilde iletkenlerle donatılır, pasif yakalama uçları ve topraklama sistemleri ile birlikte bina için güvenli bir yıldırımdan korunma yaklaşımı oluşturulur.

İnsanların ve içerisinde veri merkezi ve/veya kritik BT sistemlerini barındıran binaları yıldırımdan koruma yöntemlerinden bir diğeri aktif yakalama sistemlerini oluşturan erken akış uyarım sistemli paratonerlerdir. Aktif paratonerler montajın yapıldığı yerden itibaren belirli bir koruma çapı içerisinde kalan alanı ve yapıları koruyabilmektedir. Aktif paratonerler, radyoaktif kaynak içerikli paratonerlerin alternatifi olabilecek, radyoaktif kaynak içermeyen bir sistem geliştirmek için yapılan çalışmalar neticesinde ortaya çıkmıştır. Radyoaktif paratonerlerin yasaklanmasıyla aktif paratonerlerin dünya çapında kullanılması yaygınlaşmıştır.

Aktif paratonerler; piezoelektrik kristalli ve elektrostatik alan etkili aktif paratonerler olarak ikiye ayrılır. Piezoelektrik kristalli aktif paratonerler, en büyük yıldırım darbelerine bile dayanımı garanti edilmiş, aynı zamanda iyonizasyon hücresi bulunan bir yakalama başlığına sahiptir. Bu başlık, içinde özel bir hücrede, piezoelektrik kristal bulunduran bölümle, sağlam ve dayanıklı, paslanmaz özellikte metal bağlantı ile birleştirilmiştir. Piezoelektrik kristal, başlıktaki türbülansların etkisi ile üzerine uygulanan titreşimler şeklindeki moment sebebi sayesinde iyonizasyonu meydana getirir. Meydana gelen iyonizasyon, hava püskürtme tekniği ile iyonize bir hava akımını yakalama deşarjı şeklinde oluşturur.

Elektrostatik alan etkili aktif paratonerlerin çalışması yıldırım öncesi havada değişen, yoğunlaşan elektromanyetik alanın kullanılmasına dayanmaktadır. Hava ile yeryüzü arasında elektromanyetik alan farkı yükseldiği zaman, içlerindeki mekanizmalar bu farkı kullanarak bir iyonizasyon sistemine geçer. Bir iyon yayılımı başlatılır. Bu iyon yayılımı ile yıldırım kanalı oluşturulup yıldırımı kendi üzerlerinden toprağa aktarırlar.

Paratoner tesisatları temel olarak 3 aşamadan oluşmaktadır.

Tesisatın birinci aşaması olan aktif paratoner başlığı TS 62305 standardına uygun çalışmalıdır. İkinci aşama olan iniş iletkenleri ise mümkün olan en kısa yoldan toprağa iletilmelidir. Son aşama ise yıldırım akımının toprağa temas ettiği noktada iyi bir topraklamanın olmasıdır.

Paratoner tesisatlarında yıldırım sayacı da kullanılmaktadır. Aslında yıldırım sayacı pasif yakalama ucu tesisatlarından biri olan faraday kafesinde de kullanılmaktadır. Yıldırım sayacının kullanılması zorunlu değildir, fakat tavsiye edilmektedir. Yıldırım sayaçları, monte edilmiş yıldırımdan korunma tesisatlarının, yıldırım deşarjına maruz kalıp kalmadığını tespit etmek amacıyla tasarlanmış cihazlardır. Bu cihaz sayesinde aktif

paratonere veya faraday kafesine kaç defa yıldırım düştüğünü tespit edilebilir. Böylelikle yıldırıma maruz kalan aktif paratonerde, yıldırımdan korunma veya topraklama tesisatında oluşması muhtemel hasarları daha çabuk tespit edebilir ve paratoner, kontrollerini daha verimli aralıklarla yapılabilir. Yıldırım sayacı kullanımıyla, yıldırımdan korunma ekipmanlarının koruma sağlayıp sağlamadığı ve güvenliği tespit edilebilir. Bu cihaz test klemensinin üzerine veya toprağın 2 m yukarısına, iniş iletkeni üzerine seri olarak ve daima deşarj akımı yönünde monte edilir. Faraday kafesi uygulamalarında birçok iniş iletkeni mevcut olduğundan, yıldırım sayacı tüm korunma tesisatının en yüksek noktasında iletken üzerine veya yapının orta kısmına monte edilir. Yıldırım sayacı, maksimum 100kA şiddetindeki yıldırım darbelerine kadar olan darbeleri sayar. Çalışması için dâhili ve harici güç kaynağına gereksinimi yoktur.

Aslında yıldırım sayacı gibi kullanılması zorunlu olmayan ve kullanılması tavsiye edilen diğer bir cihaz da aktif paratoner test cihazıdır. Test cihazı can ve mal güvenliğimizi sağlamak amacıyla tesis edilmiş ya da edilecek olan aktif paratonerlerin çalışıp çalışmadığını anında test etmek amacıyla tasarlanmıştır. Aktif paratonerler, test probu sayesinde test cihazıyla her an paratonerlerin çalışması gereken bölümlerini kontrol edebilmektedir.

Paratoner tesisatına yıldırım akımının düşmesi, yıldırım sayacı sayesinde anlaşılabilmekte ve kaç kere düştüğü görülebilmektedir. Yıldırım sayacı ile test cihazı genellikle karıştırılmaktadır. Yıldırım sayacı paratoneri test etmemekte, sadece yıldırım düşüp düşmediğini göstermektedir. Test cihazı ise paratonerlerin çalışıp çalışmadığını gösterebilmektedir.

Yıldırımdan korunma tesisatının bakımı her yıl yapılmalıdır. Topraklama direnci her yıl ölçülmeli ve hedeflenen değerler sağlanmalıdır. Bu bakımlarda aktif paratonerler de test edilmelidir. Yıldırım tesisatında yıldırım düştüğü kabul edildiği takdirde ise tesisat kontrol edilmeli ve bozukluk varsa giderilmelidir.

Piyasada bulunan her marka aktif paratonerin test cihazı farklıdır. Aktif paratoner test cihazlarının girişleri birbirinden farklıdır. Bu nedenle, tesisattaki aktif paratoner hangi marka ise o markaya ait test cihazı ya da aktif paratonere uygun test cihazı olmalıdır.

Aktif paratoner test cihazı portatiftir. Bu portatif cihazla, aktif paratonerin çalışırlılığı istenilen anda test edilebilir ve buna göre çalışır durumda olup olmadığına karar verilir. Arızalı ise paratoner ünitesi yenilenir böylece tesisatın güvenirliği sağlanır.Sonuç olarak, paratoner tesisatı bakımları sınıfına göre zamanında yaptırılmalı ve bu bakımlarda aktif paratonerler test edilmelidir. Aktif paratonerler, bakım zamanları haricinde belirli aralıklar da ve yıldırım düştükten sonra da mutlaka çalışıp çalışmadığı test edilmelidir. Eğer

kontroller yapılmazsa ve yıldırım sonucu aktif paratoner başlığı zarar görmüş ise biz sadece korunduğumuzu zannederiz. Bu nedenle, aktif paratonerler test cihazları ile belirli aralıklarla kontrol edilmelidir.

Aşırı gerilim korunmasına ek olarak, özellikle veri merkezi ve sistem odalarında elektrostatik yüke karşı gerekli önlemler alınmalıdır. Bu odalarda bulunan zemin kaplamalarının direnci 10 – 100 megaohm arasında olmalıdır. Veri merkezi ve sistem odası içerisinde bulunan, yangına sebep olacak veya yangının büyümesine katkıda bulunacak tüm unsurlar bir yangın yükü (tehdidi) yaratır. Zemin kaplamaları en az elektrik kabloları kadar yangın tehlikesi oluşturmaktadır. Malzemelerin alev alması veya yanmazlığı hakkında TS EN 13501-1+A1 (EN 13501-1+A1, DIN 4102-1) standartları içerisinde detaylı bilgiler bulunmaktadır. Zemin kaplama için kullanılacak malzemenin, DIN 4102-1 standardına göre en az "B1 Zor Alevlenici - yangın geciktirici" sınıfında olması önerilmektedir. Bu durum yükseltilmiş zeminler için de geçerlidir.

Aşırı gerilim korunma tasarımı, boyutu ne olursa olsun, aşırı gerilim korunmasına dahil edilen tüm ekipmanların, kapsamlı potansiyel dengeleme/topraklama sistemlerine ihtiyacı bulunmaktadır. Aşırı gerilim nedeniyle BT bileşenleri üzerinde meydana gelen hasarın büyük bir bölümü yanlış uygulanmış (veya uygulanmamış) topraklamadan kaynaklanır. Veri merkezi içerisinde yer alan BT bileşenleri için farklı topraklama sistemlerinin kullanılması, elektriksel potansiyel farkının oluşmasına neden olur. Bu veri merkezi içerisinde çok istenmeyen bir durumdur. Elektriksel potansiyel farkını ortadan kaldırmak, potansiyel dengelemeyi oluşturmak amacı ile veri merkezi içerisinde tüm cihazların ortak bir topraklama sistemini kullanmaları önerilmektedir.

VRM.2.U16 Veri merkezi iklimlendirme

BT bileşenlerinin sürekli olarak güvenilir bir şekilde çalışabilmesi için çevresel koşulların, üretici tarafından belirtilen sınırlar dahilinde olmasının sağlanması gerekir. Bu bağlamda kullanılan "iklimlendirme" terimi, aşağıdaki iklimlendirme parametresinin düzenlenmesinden oluşur:

- Hava sıcaklığı,
- Nem,
- Temiz hava oranı,
- Asılı parçacıklar.

Sıcaklığı önceden belirlenen sınırlar dahilin de tutmak iklimlendirme sisteminin en önemli görevidir. BT'ye verilen elektrik enerjisinin neredeyse tamamı, ısıya dönüşür ve odanın dışına çıkarılması gereklidir. Bir odadaki normal ısı ve hava dolaşımı BT bileşenlerinin

sağlıklı bir biçimde çalışması için yeterli değilse, ek soğutma için bir sistem kurulması gerekecektir.

Sıcaklığa ek olarak, elektrostatik yüklerden (nem çok düşükse) veya oksitlenme ve küften (nem çok yüksekse) kaçınmak için nem çoğu zaman belirli sınırlar dahilinde tutulmalıdır.

Havadaki asılı parçacıklar, genellikle klima sistemlerinde kullanılan filtreler nedeniyle zaten yeterince düşüktür. Ek filtreleme, genellikle özel donanım kullanıldığında veya ortamdaki havanın yüksek oranda parçacığa sahip olması durumunda gereklidir. Gerekli hava akışının sağlandığını garanti etmek için, iklimlendirme sistemi filtreleri düzenli olarak kontrol edilmeli ve gerektiğinde uygun biçimde değiştirilmelidir.

Üçüncü iklim parametresi, BT operasyonları ile direk ilgili değildir. İklimlendirme sistemlerinin temiz hava sağlayarak, çalışanlar için (ilgili işyerleri yönetmeliklerine göre) uygun çalışma alanları oluşturmalıdır.

İklimlendirme sisteminin birincil amacına hizmet edebilmesi için yeterli kapasiteye sahip olması gereklidir. Tüm BT bileşenlerinin güç tüketiminde karşılaşılan bazı farklılıklar göz önüne alındığında, her kilovolt-amper (kVA) elektrik enerjisinin 0.8kW ila 1kW arasında ısı üreteceği düşünülebilir.

Bu sistemin soğutma kapasitesi, termal yük hesaplamasına ve bu değere eklenen yedek kapasiteye dayandırılmalı ve kolayca genişletilebilir olmalıdır. Soğutulan alanlara yerleştirilen üniteler, düzenli aralıklarla (her 12 ila 24 ayda bir) ölçülmeli, ayrıca BT donanımı üzerinde yapılacak büyük değişikliklerden sonra ölçümler tekrarlanmalıdır. Günün farklı saatlerinde yapılan ölçümler ile (nem miktarına göre) nemlendirme gereksinimi daha doğru şekilde belirlenebilir.

Yapılan hesaplamalarda özellikle, veri merkezinin bulunduğu bölgedeki yaz aylarında yaşanan sıcaklıklar (45-50°C'ye çıkan sıcaklıklar) dikkate alınmalıdır. Yüksek sıcaklıklar aynı zamanda yüksek soğutma gereksinimleri anlamına gelmektedir. Diğer taraftan modern BT bileşenlerinin, 30 ° C ve hatta daha yüksek sıcaklıklarda çalışabileceği de düşünülmelidir. Bu durum gerek duyulan toplam soğutma kapasitesini düşürebilir.

İklimlendirme sistemi, gerekli iklimlendirme koşullarını sağlayabilmek için çok yüksek miktarda güç harcarlar ve bu nedenle hiçbir zaman; BT bileşenlerini besleyen kesintisiz güç kaynaklarına (UPS) bağlanmamaları önerilir. İklimlendirme sistemi, kısa elektrik kesintilerinde bile UPS'in rezerv enerjisini hızlı şekilde tüketip kendini kapatmasına neden olacaktır. Fakat iklimlendirme sisteminin UPS'e bağlı olmaması, kısa süreli elektrik kesintilerinde dahi iklimlendirme sisteminin devre dışı kalması anlamına gelecektir. Yaşanan kesinti sonrası jeneratör devreye girerek, iklimlendirme sistemine gerekli enerjiyi

kısa süre içerisinde sağlayabiliyor olsa da, teknik nedenlerden dolayı (örneğin, buzlanmayı önlemek için) iklimlendirme sistemi birkaç aşamada devreye girer. Tam soğutma kapasitesi ile çalışmaya devam edebilmesi için 10-15 dakika süre gerekebilir.

Kesinti süresince (iklimlendirme sistemi çalışamasa da) BT bileşenleri genellikle UPS veya jeneratör tarafından beslenmeye ve ısı üretmeye devam eder. Oluşan ısı dışarı atılmadığı veya havanın yeterince soğutulmadığı takdirde, aşırı ısınma nedeniyle ciddi hasarlar meydana gelebilir.

İklimlendirme sisteminin çalışmadığı ve havanın soğutulmadığı durumlarda, oda sıcaklığı yalnızca 3 dakika içerisinde 60 ° C'nin üzerine çıkabilir! Bu kısa süre BT bileşenlerinin büyük bir kısmını düzgün bir şekilde kapatmak için bile yeterince uzun değildir. Bu nedenle her durumda iklimlendirme sisteminde yaşanan kesintinin ne kadar süreceği, böyle bir kesintinin sonuçlarının neler olabileceği ve hangi önlemlerin alınması gerektiği incelenmelidir.

İklimlendirme sisteminde oluşan kesintilerde, soğuk depolama sistemi kullanmak yaygın bir metottur. Bu sistem, normal operasyon sırasında oluşan ek soğutma kapasitesinin depolanarak ileride kullanılmasına dayanır. Bu sayede iklimlendirme sistemi tam kapasite çalışmaya başlayana kadar gerekli soğutma sağlanabilecektir.

Erişilebilirlik gereksinim çok yüksek olan kurumlar, elektrik şebekesinde yaşanacak kesintilerden, iklimlendirme sisteminin etkilenmemesini sağlamak için, iklimlendirme sistemine özel UPS kurulumunu da değerlendirmektedir.

Modern veri merkezlerinin enerji yoğunluğu sürekli olarak artmaktadır. 1980'lerde, 500 W / m²'lik bir enerji yoğunluğu yaygın iken, bugün 5 ila 10 kW / m² ve daha yüksek enerji yoğunluklarına sahip veri merkezlerine sıkça rastlanılmaktadır.

Geleneksel veri merkezlerinde, odanın soğutulması, soğutulmuş havanın yükseltilmiş zeminin altından taşınması, oda boyunca dolaştırılarak, kabin önlerinde yer alan mazgaldan kabinlere aktarılması ile sağlanır. Yüksek enerji yoğunluklarına sahip veri merkezlerinde, bu geleneksel yöntem artık yeterli olmamaktadır. Günümüzde piyasada mevcut gereksinimleri karşılayan, yüksek performanslı kabin içi veya kabin tipi iklimlendirme sistemleri bulunmaktadır.

İklimlendirme sisteminin işlevine devam edebilmesini güvence altına alabilmek için düzenli bakımı gerçekleştirilmelidir. Bu sistemin izlenebilmesi için ek bir izleme ünitesi kullanılması veya iklimlendirme sisteminin merkezi izleme ve alarm sistemine entegre edilmesi önerilir.

İklimlendirme sisteminden kaynaklı olabileceği düşünülen BT kesintilerinde (yetersiz soğutma, yüksek nem, vb.), detaylı analiz yapılması gereklidir. Bu gibi şüpheli durumlarda

yaşanan kesinti hakkında bilgi edinebilmek ve kesintinin gerçek nedenini anlayabilmek amacıyla sıcaklık ve nem değerlerinin en az bir hafta boyunca 15 dakikalık aralıklarla kaydedilmesi önerilir. Bu değerleri mümkünse elektronik ortamda saklayarak grafikler oluşturarak incelemeler gerçekleştirilebilir. Tamamen elektronik olarak grafikler oluşturmak mümkün değilse, en az 7 günlük termograf (sıcaklık ve nem değerlerinin tutulduğu rapor) hazırlanmalıdır.

Bir iklimlendirme sisteminin dış soğutma üniteleri, yıldırıma karşı korunmalıdır. Yüksek erişilebilirlik hedeflerine sahip, kritik veri merkezlerinde iklimlendirme sistemi (ve üniteleri) herkes tarafından erişilebilir olmamalı ve gerekirse sabotaja karşı korunmalıdır.

Acil durum planlarında klima sistemi de dikkate alınmalıdır.

VRM.2.U17 Erken yangın algılama

BT bileşenlerinde, yangınları olabildiğince erken bir aşamada tespit edebilmek için erken yangın algılama sisteminin kullanılması gereklidir. Bu tür sistemler genellikle, duman girişlerinden, havada dolaşan az sayıda ve ince duman parçacıklarını tespit edebilir, ayrıca iklimlendirme sisteminin hava dolaşım kanalını analiz edebilir.

Farklı BT bileşenleri üzerinde, bileşene dayalı izleme uygulanabilir. Konvansiyonel yangın alarmı teknolojisine (geometrik oda izleme) ek olarak, bileşen izleme ek bir algılama seviyesinin oluşmasını sağlar. Bu dedektörler, yangından etkilenen cihazın elektriğini kapatmanın yanı sıra, tek tek bileşenlerdeki yangınları söndürmek için de kullanılabilir.

Yangının gelişiminde güç kaynağını kapatmak, yangını geciktirmek veya söndürmek için yeterli olabilir.

Ek yangın söndürme sistemlerinin gerekli görülmesi durumunda, gerek maddi nedenlerle gerekse veri merkezinde çalışan personeli korumak için her bir kabin için ayrı gazlı söndürücüler kullanmak mantıklı olabilir. Bileşen koruma sistemleri, planlama, yangın algılama, söndürme gibi üreticinin sağladığı kurulum, işletme ve bakım talimatları açısından VDS 2304 kılavuzuna uygun standartlara dayandırılmalıdır.

Optik duman dedektörleri, BT birimindeki kritik odaları izlemek için kurulabilir. Yükseltilmiş zemin de optik duman dedektörleri tarafından izlenmelidir.

Bir veri merkezi veya sistem odasının yüksek erişilebilirlik hedefleri var ise veya bu alanlarda maliyeti yüksek ve değiştirmesi yüksek maliyet getirecek BT bileşenleri yer alıyorsa, otomatik söndürme sistemleri kullanılarak, atıl gazlar aracılığı ile söndürme (karbondioksit, nitrojen, argon, azot, FM 200 vs.) sistemi kurulması düşünülmelidir.

Yangın söndürme gazları sadece alevleri bastırmakla kalmaz, ayrıca havadaki oksijen miktarını azaltarak boğulma gibi durumların yaşanmasına neden olabilir. Örneğin, hacimce yüzde 8'den büyük karbondioksit konsantrasyonu hayatı tehdit eder boyuttadır. Boğulma risklerinin azaltılması ve giderilmesi için bu tür gazların kullanımı öncesinde, personelin alanı boşaltması için gerekli bir süre tanınması, görsel ve işitsel sinyaller ile gerekli uyarıların yapılması gerekmektedir.

Gazlı yangın söndürme sistemlerinin planlanması ancak uzman bir planlayıcı tarafından yapılmalıdır.

VRM.2.U18 Su sızıntısına karşı koruma

Sunucular gibi merkezi fonksiyonlara sahip BT bileşenlerinin bulunduğu oda veya alanlarda, su taşıyan her türlü borudan kaçınılmalıdır. Kesinlikle gerekli ise, soğutma suyu boruları, yangın söndürme suyu boruları ve ısıtma boruları bu alanlarda bulunabilir. Radyatör besleme hatları, mümkünse odanın veya alanın dışında kapama vanaları ile donatılmalıdır. Isıtma zamanları dışında bu vanalar kapalı olmalıdır.

Kritik alanlarda yer alan su boruları, alan dışına alınamıyorsa, olumsuz sonuçların en aza indirilmesi için su sızıntılarının olabildiğince erken tespit edilmesine yönelik önlemler alınmalıdır. Asgari koruma sağlamak için, suyu odanın dışına atan bir su toplama tavası veya su boşaltma oluğu borunun altına monte edilebilir. Su borularının oda yerine koridorlara kurulması önerilmektedir. Bu sayede borulardaki herhangi bir hasar hızlı tespit edilebilir. Tecrübeler, tavanları hafif renklerle boyamanın büyük su sızıntılarını ve su sızdıran boruları tespit etmeyi kolaylaştırdığını göstermektedir. Mevcut su borularını, herhangi bir sızıntı olup olmadığını anlamak amacıyla düzenli görsel denetime tabi tutmak gerekmektedir.

Su dedektörleri kullanılarak, tüm su borularının izlenmesi sağlanmalıdır. Boruların altına özel alarm kabloları takılarak, kablolar su sızıntısı algılama sistemlerine entegre edilebilir. Bu sayede sızıntılar hızlı bir şekilde tespit edilebilir ve sızıntının oluştuğu bölge, oldukça hassas bir biçimde belirlenebilir. Kullanılacak bu tarz bir su sızıntısı algılama sisteminin ürettiği alarm mesajları, sürekli bir personelin bulunduğu merkezi birime aktarılmalı, bu mesajlar doğrultusunda hızlı bir biçimde harekete geçmek mümkün olmalıdır. Bir seçenek olarak, özellikle kısa sürede bir personelin ulaşamayacağı alanlarda, sızıntıyı algıladığı anda, borudan su akışını engelleyecek, otomatik selenoid valflı su dedektörleri kullanılabilir. Selenoid valflerin, suyu oda veya alan dışında bloke edebilmesi (oda veya alanın dışında kurulması) sağlanmalıdır.

Otomatik drenaj sistemi, ilave veya alternatif koruma tedbirleri olarak da önerilir (bkz. VRM.1.U24 Otomatik drenaj).

BT birimindeki çalışanlar ve/veya bina hizmetleri/teknisyenleri, su borularının ne tür sorunlara neden olabileceği, nelere dikkat edilmesi konularında bilgilendirilmelidir. Su sızıntısı durumunda gerçekleştirilmesi gereken faaliyetleri, alınması gereken önlemleri detaylı bir biçimde açıklayan müdahale planları hazırlanmalı ve ilgili tüm çalışanların kullanımına sunulmalıdır.

VRM.2.U19 Teknik altyapı fonksiyonel testler

Kurumlarda, teknik altyapı ile ilgili gerçeği yansıtan fonksiyonel testler nadiren gerçekleştirilmektedir. Bu örneğin, acil durum güç kaynağının düzgün çalışıp çalışmadığının veya iklimlendirme sistemi ile yangın alarm sisteminin entegre çalışıp çalışmadığının yeterince test edilmediği anlamına gelir. Birçok durumda, arızalara karşı oldukça fazla zaman harcanmasına rağmen, arızaların oluşmasını engelleyebilecek önlemlerinin etkinliği ve yeterliliği, testlerin hasara neden olabileceği korkusuyla, test edilmez. Hâlbuki herhangi bir arıza ile operasyon sırasında karşılaşmaktansa, önceden yapılan fonksiyonel testler sırasında bunları fark etmek, bir yandan oluşan arızayı giderirken, diğer taraftan dersler çıkarmak daha doğru bir yaklaşım olarak görülmektedir.

Az da olsa kurumlar tarafından gerçekleştirilen testler, daha çok incelenen bileşenlerin istenilen fonksiyonu sağlayıp sağlayamadığı ile sınırlı kalıp, gerçek hayatta yaşanabilecek bir durumu yansıtmamaktadır. Örneğin birçok veri merkezinde, herhangi bir şebeke kesintisi yaşanması durumunda, jeneratörün devreye girebileceği şekilde elektrik tasarım yapılır, buna uygun bir biçimde sistem kurulur. Fakat veri merkezi işletilirken, yaşanabilecek bir şebeke kesintisinde jeneratör devreye girebilecek mi test edilmez. Birçok kurum bu durumu test etmek amacıyla önce jeneratörü devreye alır, daha sonra jeneratör çalışırken, şebeke elektriğini keserek testi gerçekleştirir. Hâlbuki gerçek hayatta şebeke kesintisi yaşandığında jeneratörün çalışır durumda olmayacaktır! Aslında gerçekleştirilmiş olan test jeneratörün istenilen beslemeyi sağlayıp sağlamadığının testidir. Şebeke kesintisine reaksiyon olarak gerçekleşecek işlevler zinciri bu tür bir test ile güvence altına alınamaz.

Genel olarak fonksiyonel testler, karmaşık reaksiyon senaryolarının düzgün şekilde çalışacağına dair güvence sağlamaz. Her bir bileşenin optimum şekilde incelenmesine ve korunmasına rağmen, bir arıza meydana geldiğinde genel sistem planlandığı gibi çalışmadığı durumlar da ortaya çıkabilir.

Bu nedenle, reaksiyon zincirlerini de teste tabi tutmak önemlidir. Tek bir bileşenin işlevinin test edilmesi yerine, gerçek hayatta yaşanabilecek durumlar göz önünde bulundurularak, bileşenin içinde yer aldığı ve etkileşimi bulunduğu diğer bileşenler ile birlikte bir bütün olarak test edilmesi sağlanmalıdır. Bu tür testlerin amacı yalnızca genel sistemde

saptanabilir hataların bulunması ve giderilmesidir. Bu tür testler sırasında çalışmakta olan BT bileşenlerinde kesintiler yaşanması da söz konusu olabilir.

Bu nedenle, gerek fonksiyonel ve gerekse gerçek hayatta yaşanabilecek durumların benzeştirildiği reaksiyon zincir testleri, BT bileşenlerinin yoğun olarak kullanıldığı mesai saatleri içerisinde gerçekleştirilmemeli ve olası hatalar durumunda, sonuçların kontrol altına alınabilmesi için önlemler alınmalıdır. Ayrıca bu uygulama, acil durum hazırlığının bir parçası olmalıdır.

VRM.2.U20 Altyapı ve inşaat planlarının düzenli güncellenmesi

Veri merkezinin içerisinde bulunduğu binaya ait inşaat planları, yerleşim planları; veri merkezi altyapı planları, yangın çıkış güzergah planları, elektrik devre şemaları, itfaiye yolları, vb. planlar ve dokümanlar her değişiklik veya yeni kurulum sonrası güncellenmelidir. Herhangi bir yenilik, değişiklik olmaması durumunda dahi tüm ilgili planların güncelliği ve doğruluğu belirli aralıklar ile kontrol edilmelidir.

Güncel planlar ile:

- Tanımlanan güvenlik seviyesinin korunması,
- Acil durumlara en uygun şekilde yanıt verilebilmesi,
- Denetimlerin, testlerin ve incelemelerin daha kolay gerçekleştirilebilmesi,
- Koruma önlemlerinin tamamen ve yeterli bir şekilde planlanıp uygulanmasına olanak tanıması sağlanır.

Örneğin sadece bina yönetimiyle ilgili planların sorumluluğunu üstlenmek yeterli değildir. Hasar veya acil durumlarda (örneğin kablo hasar gördüğünde veya bir su borusu patladığında), hatanın nerede oluştuğunun tespiti için ciddi zaman kayıpları yaşanabilir, bu durum sorunun giderilmesini geciktirebilir. Planlar, bina hizmetleri ve teknisyenler tarafından da erişilebilir, okunabilir olmalıdır. Gerekirse personel buna göre eğitilmeli, bilinçlendirilmeli ve uygun durumlarda bu planlardan yararlanma talimatı verilmelidir.

2.3 3.SEVİYE UYGULAMALAR

1. ve 2. seviye uygulamalar sonrasında, veri merkezleri ve/veya sistem odalarında artan koruma koşullarında dikkate alınması gereken uygulamalar aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun uygulamalardan faydalanmaları önerilir. Uygulama kapsamında öncelikli koruma sağlanan prensip, parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.2.U21 Felaket Kurtarma Merkezi

Herhangi bir felaket durumunda BT hizmetlerinin devamlılığını sağlamak isteyen kurumların, mevcut veri merkezinden coğrafi olarak ayrılmış bir felaket kurtarma merkezi (FKM) kurması ve kullanması önerilir. FKM, kurum için **kritik iş süreçlerini** destekleyecek BT hizmetlerinin felaket durumunda çalışabilmesini sağlayacak biçimde boyutlandırılmalıdır. Gerektiğinde kullanıma hazır olmasını sağlamak amacı ile gerekli planlar hazırlanmalıdır. Kurum tarafından kritik tüm verilerin düzenli olarak FKM'ye aktarılmasının sağlanması önerilmektedir.

Felaket kurtarma merkezinin fiziksel olarak kurulumu ve kullanıma hazır hale getirilmesi, iklimlendirme sistemleri, yapısal kablolama, enerji alt yapısı, yangın algılama ve söndürme sistemleri, ısı ve nem takip sistemleri, aydınlatma, fiziksel geçiş kontrol sistemleri, kamera sistemleri, izolasyon ve yükseltilmiş zemin, vb. faaliyetlerin veri merkezi rehberlerinde yer alan standartlara uygun yapılması gerekmektedir (FKM'ler veri merkezleri gibi düşünülmelidir).

Felaket kurtarma merkezi kurulumu aşamasında detaylı mimari (örneğin kabinelerin yerleşimi UPS, jeneratör yerleştirilmesi gibi), inşası (yükseltilmiş zemin, yangın kapısı gibi), elektrik (şebeke ve UPS elektrik kablolaması, topraklama), güvenlik (yangın algılama, kapı geçiş ve kamera sistemleri) ve mekanik projelerin hazırlanması (yangın ve klima sistemlerinin borulaması), yapısal kablolama altyapısının projelendirilmesi gerekmektedir. Bu proje çizimleri üzerinden kurulumların yapılması ve projelendirilmesi uygulamada bir bütünlük oluşturması açısından önem arz etmektedir.

Felaket kurtarma merkezi avantajları

- Yedekli bir ortam sunularak, olası kesintiler durumunda iş sürekliliğinin garanti altına alınması,
- İş süreçlerinin olası afetlerden en az şekilde etkilenmesinin sağlanması,
- Geriye dönük bilgi ve verilerin güvende tutulması,
- Yaşanabilecek herhangi bir doğal afet durumunda verilerin (ve veri güvenliğinin) güvence altına alınması,
- Esnek ve ölçeklenebilir bir yedeklilik sağlanmasıdır.

VRM.2.U22 Veri merkezi operasyonu sırasında inşaat projeleri

Ekonomik nedenlerden ötürü, genellikle veri merkezini/sistem odasını yeniden inşa etmek yerine, bitişik alanları birleştirerek mevcut veri merkezinin/sistem odasının genişletilmesi tercih edilir. Bu gibi alan büyütmeleri, duvarların değiştirilmesi veya yeniden inşa edilmesi, mevcut yapıyı önemli ölçüde değiştirir. Ayrıca, genişleme alanlarının yeni donanımlar için

uygun altyapıya (yükseltilmiş zemin, elektrik temini, klima, güvenlik teknolojisi, vb.) sahip olması gerekmektedir. Bu durum ciddi miktarda iş yükünü beraberinde getirir.

Kurum işleyişinin aksamaması için, inşaat çalışmaları sırasında, mevcut BT bileşenlerinin çalışmaya devam etmesi gereklidir. Aynı zamanda devam etmekte olan BT operasyonu, inşaat işlerini mümkün olduğunca kısıtlamamalı veya proje maliyetlerini gerekli seviyenin üzerine çıkaracak gereksinimler sunmamalıdır.

Güç kaynağı, iklimlendirme sistemleri, izleme ve alarm teknolojisi gibi veri merkezinin destekleyen altyapı unsurlarının, inşaat çalışmalarından etkilenmemeleri ve işlevselliklerini sürdürebilmeleri için gerekli planlamalar ve hazırlıklar gerçekleştirilmelidir. Ayrıca BT bileşenlerinin barındırıldığı alan toza, kire ve yetkisiz erişime karşı korunmalıdır. Aynı zamanda inşaat sahasına giriş/çıkış gereksiz yere engellenmemelidir. Kirlenmeye ve tozlanmaya karşı korunmak için aşağıdaki önlemler alınabilir:

- Folyo veya plastik toz koruma duvarı(toz bariyeri) oluşturulması,
- Alçıpan toz koruma duvarının oluşturulması,
- Yapıda bulunan (kir ve toz geçişini kolaylaştıracak) boşlukların doldurulması,
- Hava temizleyicilerin kullanımı,
- İnşaat alanında düşük basınç koşullarının oluşturulması,
- Özel iş prosedürlerinin uygulanması.

Plastik toz koruma duvarları, daha az miktarda toz üretecek, kısa süreli projelerde tercih edilmelidir. Plastik toz koruma duvarları kolaylıkla hasar görebilir. Ayrıca fiziksel anlamda BT bileşenleri için bir koruma sağlamaz, yetkisiz veya kötü niyetli kişilerin BT bileşenlerine kolaylıkla erişebilmelerine imkân sunar. Bu yüzden uzun süreli projelerde tercih edilmemeleri gerekir.

Uzun süreli projelerde alçıpan toz koruma duvarları tercih edilmektedir. Çift kat alçıpan kullanılarak oluşturulacak toz koruma duvarı, toza karşı daha etkin bir koruma sağlamaktadır.

Oluşturulan toz koruma duvarları üzerinde herhangi bir açıklık ve delik olmamasına dikkat edilmeli, mevcut açıklıklar ve delikler uygun sızdırmazlık malzemeleri kullanılarak kapatılmalıdır. Tozdan mümkün olan en üst düzeyde koruma sağlanmalıdır.

Alçıpan toz koruma duvarlarına kapıları monte etmek mümkündür, fakat dikkat edilmeksizin yerleştirilen kapılar tozdan korunma açısında ciddi sorunlar yaratabilir. Tozdan koruma duvarına, hava geçirmez kapılar monte edilmeli, bu sayede BT bileşenlerinin yer aldığı alana toz ve kir geçişi engellenmelidir. Mümkünse hava geçirmez

şantiye kapıları kullanılabilir. Kullanılan kapılarda yer alabilecek büyük boşluklar kauçuk contalar kullanılarak kapatılabilir.

Alçıpan toz koruma duvarları, şantiye alanı ile BT bileşenlerinin yer aldığı alanı fiziksel olarak ayırabileceği için inşaat sırasında BT bileşenlerinin bulunduğu alan içerisine yetkisiz/izinsiz kişilerin direk erişimi engellenmiş olacaktır.

İnşaat çalışması sırasında, yüksek miktarda toz oluşuyorsa, bir hava temizleyici kullanılması da önerilebilir. Bu durumda, havanın bir filtre ile temizlenmesi tercih edilmelidir. Havanın su bazlı bir yöntemle temizlenmesi durumunda, nem oranı artacak ve yüksek sıcaklıklarda çalışmayı daha zor hale getirecektir.

Toz korumaya yönelik:

- Özel ıslak sondaj veya kesim tekniklerinin kullanımı,
- Tozun doğrudan kalıcı olarak monte edilmiş veya hareketli ekstraksiyon sistemleri kullanılarak üretildiği yere çekilmesi (havanın dışarıya doğrudan üflenmesi veya havanın filtrelenmesi),
- Tozun endüstriyel bir vakumla çıkarılması,
- Yıkım malzemesinin vakum veya ilgili süpürme makineleri ile toplanması ve taşınması,
- Süpürgeler veya basınçlı hava ile temizleme işlemleri

ilave önlemler olarak düşünülebilir.

Gerçekleştirilen çalışmalar sırasında iş ve işçi sağlığı güvenliğine dikkat edilmesi sağlanmalıdır. Yönetmeliklere ve standartlara uygun bir biçimde önlemler alınmalı, çalışmaların uygun bir şekilde gerçekleştirilip gerçekleştirilmediği düzenli aralıklarla kontrol edilmelidir.

Toza karşı koruma sağlamanın yanı sıra, çalışma sırasında BT bileşenlerinin yeterince soğutulduğundan emin olmak gerekmektedir. Soğutma için hava kullanılıyorsa, inşaat sırasında üretilen ilave toz hesaba katılmalı, ek tozdan koruma filtrelerine ihtiyaç olup olmadığı değerlendirilmelidir.

Daha sonra yüklenici tarafından alınması gereken önlemlere ilişkin maliyetin kuruma yansıtılmamasını sağlamak için, ihale şartnamesinde çalışma sırasında yükleniciden beklenen tüm önlemlerin detaylı biçimde belirtilmesi önerilir.

İnşaat işleri sadece toz ve gürültü oluşturmaz, aynı zamanda dikkatsizlik veya hatalı planlama nedeniyle mevcut sistemler üzerinde hasarlar oluşmasına da neden olabilir (örneğin kabloların delinmesi veya zarar verilmesi). Buna ek olarak, inşaat çalışmaları sırasında sürekli değişecek yüklenici personelinin, aynı zamanda birçok farklı yerde

çalışması gerekebilir. Bu durumda, yüklenici personelinin yeterince izlenebileceği bir sistem kurulması veya BT alanlarının, yetkisiz erişimlere imkan tanınmayacak bir biçimde, inşaat alanlarından izole edilmesi sağlanmalıdır.

VRM.2.U23 Veri merkezi kablolama

Sistem odaları ve veri merkezlerinde, TS EN 50173-1 "Bilgi teknolojisi - Jenerik kablolama sistemleri - Bölüm 1: Genel kurallar" standardı içerisinde tanımlanmış, kablolama sistemlerine ilişkin temel ilkeler takip edilmelidir. TS EN 50173-5 “Bilgi teknolojisi – Genel kablolama sistemleri – Bölüm 5: Veri merkezleri” uzantısı, veri merkezlerine özel olarak geliştirilmiş ve yayımlanmıştır. Bu güncelleme standart gereksinimlerinin uygulanmasını kolaylaştırmıştır.

Kurumun mevcut veya planlanan ağ tasarımından ortaya çıkan gereksinimler, sistem odaları ve/veya veri merkezlerinde yapısal BT kablolamasının temelini oluşturmaktadır. Tasarım içerisinde, BT bileşenleri arasında nasıl bir ağ oluşturulacağı, bileşenlerin iç ağa (LAN), dış ağlara (WAN, MAN, vb.) ve sağlayıcılara (Internet, vb.) nasıl bağlanacakları tanımlanır. Tasarım sırasında, kurumda kullanılan veya kullanılması planlanan BT bileşenleri (sunucular, ağ bileşenleri, KVM anahtarları, depolama bileşenleri, vb.) göz önünde bulundurulmalıdır. Yapısal BT kablolamaya ilişkin erişim ve toplama alanlarının, bina ve kat dağılımlarına uygun bir şekilde tanımlanması gerekir.

Büyük kurulumlarda, sunucuların bulunduğu her bir kabin grubu, genellikle bir "ağ kabin “ine atanır ve kablolaması doğrudan belirlenmiş ağ kabini ile yapılır. Ağ kabininin ise bir (veya birden fazla) omurga ağ kabinine bağlanması sağlanır. Farklı kurulum gereksinimlerine göre ağ kabinleri kendi aralarında da bağlantılara ihtiyaç duyabilir.

Kablo taşınması sırasında, veri merkezi alanını mümkün olan en iyi şekilde kullanmak için, gereksinimleri karşılayan bir oda yerleşimi geliştirilmesi gereklidir. Bu oda düzeninde, kurumun faaliyet gösterdiği kabinler için gerekli alanlar (depolama sistemleri, aktif ve pasif bileşenler ve sunucular) ve de genişlemeler hesaba katılmalıdır. Kaçış ve ulaşım yolları ve iklimlendirme sistemi gibi unsurlar da dikkate alınmalıdır. Ayrıca oda düzeni kapsamında, elektrik güç kaynağının planlanması ve kablo taşıma sistemleri düşünülmelidir.

Veri merkezi veya sistem odaları için yükseltilmiş zemin kullanılması önerilmektedir. İklimlendirme sistemi, soğuk havayı odaya dağıtmak için yükseltilmiş zeminden faydalanıyorsa, kablo taşıma kanallarının iklimlendirmeyi etkilememesine dikkat edilmelidir. Kablo kanallarının hava akışını engellemesi, sunucuların ve aktif bileşenlerin ihtiyaç duydukları miktarda soğuk hava alamamalarına, aşırı ısınmalarına neden olmakta, bu durum arıza riskleri ortaya çıkmaktadır.

Buna ek olarak, yükseltilmiş zeminin temiz tutulması veya olası tozlanmanın kabinlere ulaşmasının engellenmesi gerekmektedir.

Mümkün olan yerlerde kabloların sabitlenmesi önerilir. Bu, kabloların yükseltilmiş zeminde veya tavanın altındaki tava sistemlerine düzgün biçimde kurulmasını gerektirir. Mümkünse "yama" kablolar kullanılmasından kaçınılmalıdır. Yüksek erişilebilirlik seviye gereksinimleri söz konusu olduğunda, veri merkezlerinde ikincil ve üçüncül kablolamanın yedekli olarak tasarlanması düşünülmelidir.

VRM.2.U24 Video gözetim sistemlerinin kullanımı

Video gözetleme sistemleri, bir binanın dış cephesini koruma (bkz. VRM.2.U12 Veri merkezi için çevre koruma tasarımı ve uygulanması) ve bir binaya erişimi kontrol altına alma önlemlerine ek olarak kullanılabilir. Video gözetim sistemleri yer alan koruma hedeflerine ulaşılması konusunda yardımcı olur:

- Caydırıcılık,
- Bina cephesinin izlenmesi,
- Kimlik,
- İzleme,
- Alarm,
- Tehditlerin tespiti ve yerinin belirlenmesi,
- Zararın önlenmesi,
- Kuralların ve düzenlemelerin ihlal edildiğinin belgelendirilmesi ve değerlendirilmesi.

Bir video gözetim sistemi planlarken, video gözetiminin genel bina güvenlik konseptine entegre olması sağlanmalıdır. Bu durum, özellikle video gözetim sistemlerine ilişkin izlemenin yapılacağı monitörlerin, korunması gereken alanın uzağında bulunduğu kurumlar için oldukça önemlidir. Bu amaçla öncelikle sürekli olarak izlenmesi gereken alanlar belirlenmeli, bu alanları eksiksiz bir biçimde takip edecek şekilde kamera sistemi seçilmelidir.

Herhangi bir izleme, değerlendirme ve alarm mekanizması olmaksızın video gözetim sistemi kurulması, caydırma amacı dışında herhangi bir anlam ifade etmemektedir. Video gözetim sistemi için merkezi bir ortam/oda belirlenmeli, gözlem için gerekli olan merkezi teknik bileşenler, uygun ortamlara kurulmalı ve korunmalıdır. Kameralar tarafından alınan görüntülerin bu merkezde kayıt altına alınması, bir görevli tarafından izlenmesi sağlanmalıdır.

Mümkün ise video gözetim sistemine ilişkin bileşenler UPS'e bağlanmalı, şebeke kesintilerinde jeneratör ile desteklenmelidir. Video gözetim sisteminin sağlıklı bir biçimde çalışmasını güvence altına almak için düzenli aralıklarla fonksiyonel testler gerçekleştirilmelidir.

Video gözetimi, giriş kontrol hizmeti için destek sağlamalıdır. Uygun kamera sistemi kullanılarak farklı durumlar izlenebilir ve kontrol edilebilir:

- Kameralar, diğer sistemler tarafından üretilen alarmları doğrulamak için kullanılabilir (örneğin, hırsızlık alarm sistemi). Böylece, güvenlik görevlisi yerinden ayrılmaksızın bir alarm mesajını değerlendirilebilir.
- Kameralar belirli bir kimliği doğrulamak için kullanılabilir (yüz tanıma, plaka tanıma yüz tanıma). Bu yolla, uzaktan giriş veya çıkışlar, merkezi giriş kapısından erişimler veya yollar izlenebilir ve kapılar yetkili kişiler için açılabilir.
- Kameralar, veri merkezleri gibi kritik bölgelere erişim doğrulaması için kullanılabilir,
- Kameralar, hareketleri veya değişiklikleri tespit etmek için kullanılabilir.

Video gözetiminin planlanması ve kurulum aşamalarında, veri koruma yetkilisi ve ilgili personel dâhil edilmelidir.

VRM.2.U25 Kesintisiz güç kaynaklarının (UPS) yedekli tasarımı

UPS, BT donanımı önünde elektrik kesilmesine karşı son kalelerden biridir ve erişilebilirliği sağlamak için oldukça önemlidir. Bu nedenle, UPS tarafından beslenen BT ile aynı koruma ihtiyaçlarına sahiptir. Kritik BT sistemlerinin yedeklenmesi gibi UPS'lerin de yedeklenmesi gerekebilir.

UPS sistemleri farklı biçimlerde tasarlanabilir. Genel olarak tasarımda beş farklı yaklaşımdan yararlanılır:

- Capacity System (Kapasite Sistem)
- Isolated (Blocked) Redundant (İzole(Bloke) Yedekli)
- Parallel Redundant (Paralel Yedekli)
- Distributed Redundant (Dağıtık Yedekli)
- System plus System Redundant (Sistem + Sistem Yedekli)

Bu beş temel tasarım yaklaşımından; Kapasite Sistem tasarım ***N sistem*** olarak, İzole, Paralel ve Dağıtık Yedekli tasarımlar ***N+1 sistem***, Sistem + Sistem Yedekli tasarım ***2N veya 2N+1 sistem*** olarak da bilinirler.

UPS tasarımlarında çokça "N" harfi kullanılır. Zaman zaman N, zaman zaman N+1 veya 2N gibi kavramlar ile karşılaşılabilir. Burada "N" ile veri merkezi içerisinde yer alan, enerji

kaynağından beslenecek cihazların sağlıklı bir şekilde çalışabilmesi için gerekli güç kapasitesi kastedilmektedir.

Çok kısa bir biçimde özetlenecek olursa, *N* tasarım, ihtiyaç duyulan güç kapasitesini sağlayacak sayıda ekipman veya sistem ile oluşturulur, herhangi bir yedeklilik içermez. *N + 1* tasarımda ek bir ekipman veya sistem aracılığı ile yedeklilik sağlanır. *2N veya 2(N+1)* tasarımda ise tüm ekipmanlar/sistemler yedeklidir, böylelikle en üst düzey koruma sağlanmış olur.

Kurumların erişilebilirlik ihtiyaçları, veri merkezinde yer alan BT bileşenlerinin kritiklik seviyelerine ve işin maliyeti tasarım yaklaşımlarından hangisinin seçileceği konusunda belirleyicidir.

Bu farklı tasarımlar arasında N tasarım en az elektriksel ekipmanın kullanıldığı, dolayısı ile en az maliyetli tasarımdır. Fakat herhangi bir elektrik kesintisi durumunda bir koruma sağlamaz, tüm BT bileşenleri elektrik kesintisinden etkilenecektir.

2N tasarım, kullanılan elektriksel ekipmanların bire bir yedeklendiği, en üst düzey korumanın sağlandığı tasarımdır. Her ne kadar BT bileşenlerinin elektrik kesintilerinden etkilenmemesi için en yüksek korunumu sağlasa da, gerek ekipman maliyeti açısından, gerekse bakım maliyeti açısından en yüksek maliyetli tasarımdır.

N+1 ise ek bir elektriksel ekipman ile yedekliliğin sağlanmasına yönelik bir tasarımdır. Maliyet açısından 2N tasarıma oranla daha uygun olduğu söylenebilir. N+1 tasarım için farklı topolojilerden yararlanılabilmektedir.

Kurumlarda en çok tercih edilen UPS tasarımı paralel yedekli tasarımdır. Bu tasarımda, birbirine paralel bir biçimde bağlı, ortak güç yolunu kullanan, aynı kapasitede (ve tercihen aynı modelde) UPS'ler yer alır. Sistemde yer alan tüm UPS'ler toplam enerji yükünü paylaşırlar, boş herhangi bir UPS bulunmaz. UPS'ler kendi aralarında senkronizasyonu sağlamak için haberleşirler. Herhangi bir UPS üzerinde sıkıntı yaşanması (veya bakım/onarım için UPS'in devre dışı bırakılması) durumunda, diğer UPS'ler yükü üzerlerine alarak operasyonun sürekliliğini sağlarlar.

Bu tarz bir tasarımda, ihtiyaç duyulduğunda sisteme UPS eklenerek kapasite artırılabilir. Aşağıdaki tabloda farklı sayıda UPS'in yer alabileceği durumlara örnekler verilmiştir.

Tablo 7. Örnek UPS Kullanımları

Paralel bağlı UPS'ler	Toplam UPS Kapasitesi	Veri Merkezine sağlanan enerji	UPS Modülü yükü (%)	Açıklama
2 x 240 kW	480 kW	240 kW	%50	*(N+1)* Herhangi bir UPS'in kesintiye uğraması durumunda diğer modül yükü üzerine alır.
3 x 120 kW	360 kW	240 kW	%66	*(N+1)* Herhangi bir UPS'in kesintiye uğraması durumunda diğer iki modül yükü üzerine alır.
4 x 80 kW	320 kW	240 kW	%75	*(N+1)* Herhangi bir UPS'in kesintiye uğraması durumunda diğer üç modül yükü üzerine alır.
3 x 240 kW	720 kW	240 kW	%33	*(N+2)* İki farklı UPS'in aynı anda kesintiye uğraması bile tolere edilebilir.

Paralel yedekli tasarım, gerektiğinde kapasitenin (belirli bir seviyeye kadar) artırılabilir olması, sistemde yer alan tüm UPS'lerin aynı anda kullanılabiliyor olması ve donanım konfigürasyonunun kolaylığı açısından tercih edilebilir.

Montaj ve devreye alma konularında UPS üreticilerinin tavsiyelerine uyulmalıdır. Ortam sıcaklığı, nem oranı, hava akışı, yanıcı ve patlayıcı maddelerden arındırılmış bir ortam kurulum için dikkate alınması gereken en önemli koşullardır.

VRM.2.U26 Yedekli jeneratör

Yüksek koruma gereksinimleri kapsamında, alternatif güç kaynağı olarak kullanılacak sistemlerin de yedekli tasarlanması önerilir.

BT'nin erişilebilirlik amacı gereğince, jeneratörler paralel bağlanarak birbirinin yedeği olarak kullanılabilir. Yedekli bir tasarım amaçlanıyorsa (N + 1) yedeklilik, ana jeneratörün arızalanmasına karşı, paralel bağlanan jeneratörün otomatik devreye girmesi ile kesinti yaşanmadan kritik sistemlerin beslenmesi sağlanmalı ve arıza halinde tüm kritik sistemleri taşıyabilecek kapasitede olmalıdır. Aynı şekilde, jeneratörün bakım esnasındaki yedekliliği isteniyorsa, 2(N + 1) şeklinde bir yapı düşünülmelidir.

Özellikle tamiri zaman alacak jeneratörün, yedeğinin bulunması önerilmektedir. Jeneratörün uzu süreler boyunca, sağlıklı biçimde çalışmasını sağlamak amacıyla, düzenli olarak periyodik bakımları yapılmalı ve testleri gerçekleştirilmelidir.

Yedeklilik, modülerlik ve ölçeklenebilirlik konu detayları “VRM.2.U29 Teknik altyapıda yedeklilik, modülerlik ve ölçeklenebilirlik” maddesinde açıklanmıştır.

VRM.2.U27 Felaket kurtarma ve yangın tatbikatları

Yangın durumunda alınması gereken önlemler, bir alarm planı içerisinde yazılı hale getirilmelidir. Böyle bir plan içerisinde:

- Hangi olaylar karşısında ne tip önlemlerin alınacağı,
- Bina tahliyesinin gerekip gerekmediği, gerekiyorsa tahliyenin nasıl gerçekleştirileceği,
- Böyle bir durumda kimlerin bilgilendirileceği,
- Hangi destek personeline ve acil servise (itfaiye, hastane, polis, vb.) bilgi verileceği,
- Yangın durumunda çalışanlardan beklenen davranış biçimleri gibi bilgilerin yer alması önerilmektedir.

Hazırlanan alarm planının yayımlanması, tüm çalışanlara duyurulması sağlanmalıdır.

Bununla birlikte en iyi alarm planı içerisinde yer alan önlemler, doğru ve uygulanabilir değilse çok faydalı olmayacaktır. Bu nedenle planın, uygulanabilirliği düzenli olarak kontrol edilmeli ve gerekli durumlarda güncellenmesi gereklidir.

Alarm planının kontrolünde yararlanılan yöntemlerden biri de yangın tatbikatlarıdır. Birçok kurumda, düzenli yangın tatbikatı gerçekleştirilmediği gibi yangın tatbikatlarının gerçekleştirildiği kurumlarda; örneğin çalışanların yangın söndürücünün nerede olduğu, nasıl kullanılacağı konusunda bilgi sahibi olmadıkları; acil çıkış/kaçış yolunun nerede olduğunu, en yakın merdiveni, çıkış kapılarının yerlerini bilmediklerinin ortaya çıktığı görülmüştür. Hatta kimi çalışanların, tatbikat sırasında normal çalışmalarına devam ettikleri ve tatbikatı göz ardı ettikleri de bilinmektedir. Acil durumlarda bu tip bilgi yetersizliği felaket ile sonuçlanabilir.

Özellikle yangın güvenliği tatbikatlarında insan hayatının ve BT bileşenlerinin korunması için doğru davranış eğitimlerinin verilmesi sağlanmalıdır. Bu tür tatbikatların uygulanması için öncelikle yetkili makamlar veya şirket üst yönetimi ile anlaşmaya varılmalı, tatbikat sonuçlarının üst yönetimin bilgisine sunulması düşünülmelidir.

Alarm planları dışında, herhangi bir felaket durumunda (yangın, su baskını, vb.) kurum tarafından işlerin sürdürülebilmesi için gerekli BT bileşenlerinin ve BT servislerinin alternatif yerlerde (tercihen Felaket Kurtarma Merkezlerinde) çalışır hale getirilmesi için felaket kurtarma planlarının hazırlanması da gereklidir.

Felaket kurtarma planları içerisinde, felaket durumunda ilk yapılacaklar, insan sağlığını güvence altına almak için gerekli önlemler, hasar tespit için gerçekleştirilecek faaliyetler, iletişim (ve gerekli ise halkla ilişkiler) planı, kurtarılacak BT bileşenleri, bu bileşenleri kurtarmak için gerçekleştirilmesi gereken kurtarma adımları (faaliyetler), sorumlu personel, vb. yer alır.

Her ne kadar felaket kurtarma planı en ince ayrıntısına kadar düşünülerek hazırlanmış olsa da, planın uygulanabilirliği düzenli olarak kontrol edilmeli ve gerekli durumlarda güncellenmesi sağlanmalıdır.

Felaket kurtarma planının uygulanabilirliğini kontrol etmek amacıyla:

- Fonksiyonel testler düzenlenebilir (felaket kurtarma merkezi içerisinde yer alan ekipmanların sağlıklı çalıştığını güvence altına alabilmek amacıyla),
- Bir felaket çıkması durumunda izlenecek yöntem (adım adım plan üzerinden geçilerek) tartışılabilir,
- Yangın tatbikatları düzenlenebilir,
- Bir felaket yaşanmış gibi tüm sistemler kapatılarak, felaket kurtarma merkezinin devreye alınması denenebilir.

Bu kontrollerden bir kısmı toplantılarda, sadece plan üzerinden geçerek; bazıları ise canlı ortamda gerçek hayatta yapılması gerekli faaliyetleri gerçekleştirerek felaket kurtarma işleyişinin geçerliliğini sınama fırsatı sağlar.

Testler veya kontrollerde elde edilen bulgular, test/kontrol sonuçları kayıt altına alınmalı ve felaket kurtarma planlarının iyileştirilmesi için gerekli faaliyetler belirlenmelidir. Planların gerekli durumlarda güncellenmesi sağlanmalıdır.

VRM.2.U28 Teknik altyapıda yedeklilik, modülerlik ve ölçeklenebilirlik

BT bileşenlerinin erişilebilirliğini sağlamak için en iyi yöntem, yedekliliktir. Bu, belirli bir görevi gerçekleştirmek için aslında gerekli olandan daha fazlasına sahip olmak demektir (Latince'den: "redundare", taşma, fazla olma). Bilgi Teknolojileri endüstrisinde yedeklilik,

bir teknik sistemin işlevsel olarak eşdeğer kaynaklarının varlığı anlamına gelir. Bu nedenle yedeklilik ile ilgili asıl soru: “Yedekliğe sahip olmak için ihtiyaçtan fazla kapasiteler oluşturmak gerekli midir?” sorusudur.

Modülerlik ise istenilen hizmetin bir veya daha fazla modül tarafından sağlanıp sağlanamadığını açıklar. Başarılı şekilde oluşturulan modül tasarımları sayesinde, gereken yedeklilikler ortadan kalkabilir. Değişen teknik gereksinimlere karşın en iyi planlanan modeller bile bir süre sonra yeniden ölçeklendirilmeye (boyutlandırılma) muhtaç kalabilir.

Teknik altyapı tasarımında, beş temel tasarım yaklaşımı ağırlıklı olarak kullanılır. Bu yaklaşımlar; Kapasite Sistem tasarım N sistem olarak, İzole, Paralel ve Dağıtık Yedekli tasarımlar N+1 sistem, Sistem + Sistem Yedekli tasarım 2N veya 2N+1 sistem olarak da bilinirler.

Veri merkezi teknik altyapı tasarımlarında çokça “N” harfi kullanılır. Zaman zaman N, zaman zaman N+1 veya 2N gibi kavramlar ile karşılaşılabilir. Burada “N” ile veri merkezi içerisinde yer alan, enerji kaynağından beslenecek cihazların sağlıklı bir şekilde çalışabilmesi için gerekli güç kapasitesi kastedilmektedir.

Çok kısa bir biçimde özetlenecek olursa, N tasarım, ihtiyaç duyulan güç kapasitesini sağlayacak sayıda ekipman veya sistem ile oluşturulur, herhangi bir yedeklilik içermez. N + 1 tasarımda ek bir ekipman veya sistem aracılığı ile yedeklilik sağlanır. 2N veya 2(N+1) tasarımda ise tüm ekipmanlar/sistemler yedeklidir, böylelikle en üst düzey koruma sağlanmış olur.

Kurumların erişilebilirlik ihtiyaçları, veri merkezinde yer alan BT bileşenlerinin kritiklik seviyelerine ve işin maliyeti tasarım yaklaşımlarından hangisinin seçileceği konusunda belirleyicidir.

Bu farklı tasarımlar arasında N tasarım en az elektriksel ekipmanın kullanıldığı, dolayısı ile en az maliyetli tasarımdır. Fakat herhangi bir elektrik kesintisi durumunda bir koruma sağlamaz, tüm BT bileşenleri elektrik kesintisinden etkilenecektir.

2N tasarım, kullanılan elektriksel ekipmanların bire bir yedeklendiği, en üst düzey korumanın sağlandığı tasarımdır. Her ne kadar BT bileşenlerinin elektrik kesintilerinden etkilenmemesi için en yüksek korunumu sağlasa da, gerek ekipman maliyeti açısından, gerekse bakım maliyeti açısından en yüksek maliyetli tasarımdır.

N+1 ise ek bir elektriksel ekipman ile yedekliliğin sağlanmasına yönelik bir tasarımdır. Maliyet açısından 2N tasarıma oranla daha uygun olduğu söylenebilir. N+1 tasarım için farklı topolojilerden yararlanılabilmektedir.

Veri Merkezi Seviyelendirme

1.Seviye Veri Merkezi

1.Seviye veri merkezleri genel anlamda küçük ölçekli işletmelere hizmet eden sistem odalarıdır. Hem planlanmış hem de planlı olmayan çalışmalar ile kesinti yaşanmasına açıktır. Soğutma sistemi bulunur ancak yükseltilmiş zemin, UPS veya bir jeneratör olmayabilir. UPS ve jeneratörün olduğu durumlarda ise tek modüle sahip olurlar ve birçok noktada kesinti yaşatma ihtimalleri yüksektir. Yıllık olarak yapılan bakım çalışmaları sırasında da bu veri merkezlerinin tamamen kapanması ve operasyona ara vermesi gerekmektedir.

2.Seviye Veri Merkezi

2.Seviye'ye sahip veri merkezlerinde yedekli bileşenler bulunmaktadır ancak bunlar tek hat üzerinden sağlanmaktadır. Güç ve soğutma sistemi de tek hat üzerinden sağlanır ancak dağıtım sırasında yedeklilik sağlayan bileşenlere sahiptir. Bir örnek ile açıklamak gerekirse; Enerji aynı hat üzerinden sistem odası panosuna kadar gelir, burada linye ve sigortalar ile iki ayrı hat üzerine ayrılıp kabinet üzerinde 2 ayrı PDU'yu besleyecek duruma ulaşırlar. Bunun avantajı, cihazda oluşabilecek bir arızanın enerji sistemini etkilemesi durumunda öncelikle bağlı olduğu PDU'nun sigortasını ya da kabinetin pano tarafındaki sigortasını etkilemesi olacaktır. Cihaz diğer power supply aracılığıyla çalışmasına devam edecektir. Dezavantajı ise, veri merkezi güç dağılım panosuna gelen enerji hattı üzerinde bir sorun oluşması durumunda sistemin tamamen kapanması olacaktır.

Bu seviyeye sahip veri merkezlerinde yedekli bileşenler bulunmaktadır ancak bunlar tek hat üzerinden sağlanmaktadır. Güç ve soğutma sistemi de tek hat üzerinden sağlanır ancak dağıtım sırasında yedeklilik sağlayan bileşenlere sahiptir. Bir örnek ile açıklamak gerekirse; Enerji aynı hat üzerinden sistem odası panosuna kadar gelir, burada linye ve sigortalar ile iki ayrı hat üzerine ayrılıp kabinet üzerinde 2 ayrı PDU'yu besleyecek duruma ulaşırlar. Bunun avantajı, cihazda oluşabilecek bir arızanın enerji sistemini etkilemesi durumunda öncelikle bağlı olduğu PDU'nun sigortasını ya da kabinetin pano tarafındaki sigortasını etkilemesi olacaktır. Cihaz diğer güç kaynağı aracılığıyla çalışmasına devam edecektir. Dezavantajı ise, veri merkezi güç dağılım panosuna gelen enerji hattı üzerinde bir sorun oluşması durumunda sistemin tamamen kapanması olacaktır.

3.Seviye Veri Merkezi

3.Seviye'ye sahip veri merkezlerinde, herhangi bir planlanmış çalışma, bakım, bileşenlerin onarımı ve değişimi, yeni kapasite sağlayacak ekipmanların eklenmesi, çıkarılması,

yapılacak olan testler, sistemin işleyişini bozmadan ve kesintiye uğratmadan yapılabilmektedir.

Bu seviye veri merkezlerinde soğutma ve enerji için birden fazla hat vardır ancak sadece bir tanesi aktif olarak çalışır. Kesinti, arıza ya da bakım sırasında yük diğer hat üzerinden sağlanabileceğinden operasyon aksamadan devam edebilecektir. Soğutma ve elektrik enerji sistemleri sadece veri merkezi özelinde kullanılabilir, veri merkezinin içinde bulunduğu yapı ya da diğer birimler için paylaşılma söz konusu olamayacaktır. 3.Seviye veri merkezlerinin ortalama yıllık kesinti süresi 1.6 saattir.

3.Seviye veri merkezlerinde de tam bir (N+1) yedekliliği vardır. Soğutma sistemi olarak CRAC ya da CRAH kullanılır. Günümüzde merkezi su soğutmalı chiller sistemleri (CRAH) yaygın olarak kullanılmaktadır.

Ayrıca bu sistemlerin bir avantajı da ülkemizde ki mevsim çeşitliliğinden yararlanılarak kış aylarında soğutma için enerji kullanımında yüzde 75 oranında(free cooling) tasarruf sağlanılmasıdır.

Kabinler içerisinde de enerji yedekliliği aktif şekilde kullanılmaktadır. Bir kabin birden fazla PDU tarafından beslenilmekte olup, enerji hattının bir kolunda oluşacak arıza nedeniyle diğer kol üzerinden süreklilik devam edecektir.

Jeneratörler için de herhangi bir kesinti de 72 saat yetecek kadar yakıt depolama zorunluluğu bulunmaktadır. Genellikle de bir petrol şirketiyle öncelikli teslimat edilmek üzere anlaşmaları bulunmaktadır.

Enerji, soğutma ve mekanik gibi yedekliliğin yanı sıra internet erişimi için de yedeklilik sağlanmaktadır. Ayrıca veri merkezi içerisinde meydana gelebilecek yangın durumları için VESDA(Very Early Smoke Detection System) bulunmakta olup oda içerisinde sirküle edilen havada herhangi bir duman belirtisi görülmesi durumunda alarm olarak düşmektedir. Yangın söndürme olarak da FM200 ya da NOVEC 1230 olarak bilinen gazlı söndürme sistemleri kullanılmaktadır. Operasyonun işleyişini aksatmadan oda içerisindeki oksijen seviyesini düşürerek yangın çıkma ihtimalini ortadan kaldırmaktadır. Sel ya da su soğutmalı sistemlerde meydana gelebilecek sızıntılara karşı da önlemler alınmıştır. Yükseltilmiş zemin tabanına döşen sızıntı algılayıcı kablolar en ufak bir sıvı temasında yine alarm verecek şekilde sisteme entegre edilebilmektedir.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

Veri merkezi ile ilgili detaylı konulara aşağıdaki referans ve kaynaklardan ulaşılabilir:

- TIA-942-A: Veri Merkezleri İçin Telekomunikasyon Altyapı Standardı
- ANSI/BICSI 002-2014: Veri Merkezi Tasarım ve Uygulama En İyi Pratikleri
- Enterprise Data Center Design and Methodology, Rob Snevely
- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri
- [DIN50600-1] DIN EN 50600-1
- [DIN62305-4] IEC 62305-4 (VDE 0185-305 / DIN EN 62305) – Yıldırımdan korunma ANSI - American National Standards Institute
- BICSI - Building Industry Consulting Service International
- BSI-Bundesamt für Sicherheit in der Informationstechnik, Umsetzungshinweise zum Baustein INF.2 Rechenzentrum sowie Serverraum https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_2_Rechenzentrum_sowie_Serverraum.html

VRM.3.U: ELEKTRİK KABLOLAMA

1 AÇIKLAMA

1.1 TANIM

Elektrik kablolaması, kuruma enerji sağlayan elektrik şebekesinin binaya giriş noktasından, BT bileşenlerinin ve elektrik ile çalışan tüm diğer ekipmanların elektrik bağlantılarına kadar tüm kablolarını ve iletim ağlarını içerir.

Uygun ve standartlara uyumlu bir kablolama, BT erişilebilirliğinin temelini teşkil eder. Elinizdeki rehber sadece elektrik kablolamaya özgü bilgileri içermekte olup, BT bileşenlerinin birbirleri ile haberleşmeleri için yararlanılan BT kablolaması ayrı bir rehber içerisinde detaylı olarak ele alınmaktadır (bkz. BT Kablolama Rehberi).

1.2 YAŞAM DÖNGÜSÜ

Elektrik Kablolama Uygulama Rehberi veri merkezinin ve veri merkezi içerisinde yer alan BT bileşenleri ve altyapı ekipmanlarının kurum ihtiyaçlarına uygun bir biçimde çalışabilmesini sağlamak amacıyla planlama, uygulama, işletme ve elden çıkarma aşamalarında kullanılabilecek uygulama maddelerini içermektedir. Bu uygulama maddeleri mevcut bir binanın elektrik tesisatının yenilenmesi sırasında kullanılabileceği gibi yeni bir binanın elektrik kablolama altyapısının oluşturulması sırasında da kurumlara yardımcı olacaktır.

Planlama ve Tasarım

Etkin, verimli ve güvenli bir kablolama altyapısının temelleri planlama aşamasında atılır. Bu amaçla, öncelikle bir ihtiyaç analizi yapılması gereklidir (**bkz. VRM.3.U4 Elektrik kablolama ihtiyaç analizi**).

Kabloların mekanik ve elektriksel özellikleri, kullanım için seçilen kablo tiplerine (**bkz. VRM.3.U1 Uygun kablo tiplerinin seçimi**), kablo güzergahlarına, kablo taşıma sistemlerine (kablo kanalları, kablo taşıyıcıları, vb.) ve çevresel koşullara (**bkz. VRM.3.U2 Kablo yönetimi**) göre belirlenir. Ayrıca planlama aşamasında, elektrik tesisatının çevresel tehlikelere karşı dayanıklı hale getirilmesi (**bkz. VRM.3.U6 aşırı gerilimden korunma** ve **VRM.3.U12 İkincil güç kaynağı**) ve bina içerisinde bulunan kabloların fiziksel olarak korunması düşünülmelidir (**bkz. VRM.3.U14 Elektrik kablolama malzeme güvenliği** ve **VRM.3.U15 Kabin sistemlerinin kullanımı**).

Devreye Alma/Yerine Getirme

Planlama ve tasarım sonrası, kablo tiplerine uygun bir biçimde kurulum gerçekleştirilerek (**bkz. VRM.3.U3 Profesyonel kurulum**) elektrik tesisatı kullanıma hazır hale getirilir.

Yangın kontrolü için önemli unsurlardan bir tanesi kablo taşıma sistemleridir. Korunmamış kablo kanalları, yangının ortaya çıkmasına ve yangın durumunda yangının daha hızlı yayılmasına neden olabilir (**bkz. VRM.3.U8 Kablo taşıma sistemlerinin yangından korunması**). Kabloların döşenmesi sırasında, ayrıntılı ve doğru bir dokümantasyon oluşturmak oldukça önemlidir. İlerleyen aşamalarda hangi kablonun nereden geldiğini, nereye gittiğini ve nereye bağlandığını belirlemek çok daha zor olacaktır (bkz. **VRM.3.U9 Elektrik kablolamanın dokümantasyonu ve etiketleme** ve **VRM.3.U10 Elektrik tesisatlarının ve bağlantıların kontrolü**). Gerçekleştirilen kurulumlar sonrası, tüm elektrik tesisatı, bir kabul/onay sürecinden geçmelidir (**bkz. VRM.3.U5 Elektrik kablolama iş kabulü**).

İşletme

Veri merkezi bünyesinde, enerji kullanımının risksiz ve sorunsuz bir biçimde gerçekleşebilmesi için elektrik tesisatı, tüm ekipmanlar ve bu ekipmanların kullanımları düzenli olarak kontrol edilmelidir (**bkz. VMR.3.U10 Elektrik tesisatlarının ve bağlantılarının kontrolü**). Ayrıca kablo taşıyıcı sistemlerin (kablo kanallarının) üzerinde gerçekleştirilecek tüm çalışmalara bir yangın güvenlik görevlisinin (acil eylem sorumlusu) katılımı sağlanmalıdır (**bkz. VRM.3.U11 Elektrikli cihazların ve elektrik altyapısının yangın çıkarma riski**).

Elden Çıkarma

Kullanılmayan, işlevini tamamlamış kabloların ortadan kaldırılmaları veya uygun şekilde elden çıkarılmaları sağlanmalıdır (**bkz. VMR.3.U7 Gereksiz kabloların çıkarılması ve devre dışı bırakılması**).

Acil durum planlama

Kurum (veya veri merkezi) yüksek erişilebilirlik gereksinimlerine sahipse, kullanılan harici bağlantılar da dahil olmak üzere tüm elektrik kabloları yedekli olarak tasarlanmalıdır.

2 UYGULAMALAR

Aşağıda yer alan maddeler, "Elektrik Kablolama" temel varlığına özel uygulama maddeleridir.

2.1 1.SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

VMR.3.U1 Uygun kablo tiplerinin seçimi

Kablo seçiminde, teknik gereksinimlerin yanı sıra kabloların yer alacağı ortam ve işletim koşulları da dikkate alınmalıdır. Bu tür gereksinimleri karşılayabilmek amacı ile kablo üreticileri farklı kablo çeşitleri sunarak ihtiyaca uygun çözümler geliştirirler.

Bina içinde veya dış alanlardaki kablo kurulumlarında, özellikle kablo kaplamaları/korumaları ile ilgili aşağıdaki kriterler dikkate alınmalıdır:

- Sıcaklık,
- Çevreleyen ortam (su, kanalizasyon, asit, gaz, ışık, toprak),
- Kemirgen koruması, çarpma dayanımı (stone-chip resistance), su basıncı direnci, vb.,
- Yangına yatkın alanlarda koruma seviyesi,
- Havadan (yukarıdan) hat kullanımlarında oluşabilecek özel gerilme kuvvetleri.

Buna ek olarak kablo taşımasında kullanılacak platformlar, kablo kanalları, kablo merdivenleri, kullanılacak döşemeler, tuğlalar, vb. unsurlar işin içerisine dahil edilmeli, ilgili yönetmelikler ve standartlar değerlendirilmelidir (IEC 60364, TS HD 60364, DIN VDE 0100, DIN 4102, vb.).

Elektrik kablolarının seçimi için gereksinimler, sadece BT ekipleri tarafından belirlenmemeli, işletim ortamı ile ilgili çevresel etkiler veya özel yapısal özellikler de göz önünde bulundurulmalıdır.

Özellikle bina işletimi, yapısal özellikler ve binaya özgü diğer özel koşullara aşina olan bina hizmetleri personelinin/teknisyenlerinin, kablo taşıma sistemlerinin belirlenmesi, uygun kablo tipinin seçimi gibi kablo tasarım çalışmalarına dahil olmaları sağlanmalıdır.

VMR.3.U2 Kablo yönetimi [BT Yöneticisi]

Kablo taşıma sistemleri planlanırken, öngörülebilir tehlike kaynaklarından kaçınmaya özen gösterilmelidir. Kablolar, sadece bina içerisinden erişilebilen kanallar aracılığıyla iletilmelidir. İyi tasarlanmış ve düzenlenmiş kablo kanalları kontrolü kolaylaştırır. Kablo kanalları ve kablolar, insanlar, taşıtlar ve makineler nedeniyle oluşabilecek hasara karşı korunacak şekilde döşenmelidir.

Elektrik kablosu bağlanacak cihazlar ve cihaza bağlı kablolar, kişilerin yürüme veya araçların geçiş alanlarında bulunmamasına dikkat edilmelidir. Eğer kabloların bu tür alanlar üzerinden taşınması bir zorunluluk ise, bunların gerekli ağırlığı kaldırabilecek şekilde yapılandırılacak kanal yolları içerisinde taşınarak korunmaları sağlanmalıdır. Cihazları elektrik prizine bağlarken, oluşan kablo gerginliğine dikkat edilmeli, kablo gerginliğinin azaltılması sağlanmalıdır. Hatta elektrik bağlantısı için kullanılacak fişlerin

vidalanmaması düşünülebilir. Böylelikle kablo gerginliğinin artması veya dış bir müdahaleden fişin etkilenmesi, sadece fişin prizden çıkmasına neden olacak, priz veya cihaz üzerindeki lehimlenmiş soket bir zarar görmeyecektir.

Yeraltında bulunan otoparklar, hasar azaltmaya yönelik kablo yönetimi için ciddi riskler içerir. Örneğin otopark giriş kapılarının uzun süreler açık kalması, üçüncü şahısların otoparklara erişimine olanak sağlayabilir. Düşük tavan yükseklikleri nedeniyle, genellikle tavanda yer alan kablo kanallarına basit aletler ile rahatlıkla ulaşılabilir. İzin verilen taşıt yüksekliğinin belirlenmesi sırasında, taşıt geçiş alanında bulunan kablo kanallarının göz önünde bulundurulmaması, kablo kanallarının (ve dolayısıyla kabloların) yüksek taşıtlar nedeniyle zarar görmelerine, elektrik kabloları üzerinde ciddi hasarlar oluşmasına neden olabilmektedir.

Farklı kurumlar ile ortak kullanılan binalarda kabloların, ortak olarak kullanılmakta olan zemin, tavan veya duvar gibi alanlardan geçmesini önlemek için özen gösterilmelidir. Tüm kablo taşıma sistemleri, diğer kurumlar tarafında kullanılmakta olan alanlardan fiziksel erişimi engellemek amacı ile, mekanik olarak kilitlenmelidir. Mümkün olması durumunda, alan sınırlarında, kabloların sonlandırılması sağlanmalıdır.

Yangın riski yüksek alanlardan mümkün olduğunca kablo geçirilmemesi önerilmektedir. Kabloların, yangına rağmen belirli bir süre operasyonu devam ettirebilmesi, devre bütünlüğü olarak tanımlanır. Kanallar içerisinde bulunan tüm kabloların devre bütünlüğünü sağlamak için kablo kanalının yangın riski yüksek alanda kalan parçası üzerinde, yangına dayanıklı özel maddeler kullanılarak yalıtım gerçekleştirilmelidir. Sadece belirli kablolar için devre bütünlüğü önemliyse, yangına dayanıklı bir kablo tipi ve sabitleme tertibatı kullanılmalıdır. Devre bütünlüğü sadece uygun tip kablolar ile sağlanamaz, kablo taşıma sisteminin; kablo kanalları, kablo merdivenleri, kablo kelepçeleri veya kanalet gibi bileşenler ile birlikte bir bütün olarak düşünülmesi gereklidir. Bununla birlikte yangın durumunda yukarıdan düşen parçaların, kablo taşıma sistemini tahrip edememelerini sağlamak da son derece önemlidir.

Zemin altında bulunan kablo kanalları için, kanalın yaklaşık 10 cm yukarısına bir risk uyarı etiketi yerleştirilmelidir. Kablo kanalı içerisinden taşınmayan tekli kablolar için özel kablo korumalarının kullanılması önerilebilir.

Kablolar, fırtınadan etkilenmeyecek şekilde taşınmalıdır. Örneğin, bina çatısı üzerinden geçirilecek kabloların, en azından her 5 metrede bir, uygun bir şekilde çatı yüzeyine bağlanması sağlanmalıdır. Fırtına nedeniyle oluşan kuvvetler, kablo veya kablo tellerini etkileyebilir. Buna ek olarak, bir fırtına durumunda, kablolar üzerine düşecek nesneler,

kabloları tahrip edebilir. Bu tür durumlara karşı da korunma gereklidir. Bu yüzden, çatı ve panjur yüzeyleri üzerinde bulunan kablolar, daima muhafaza boruları ile döşenmelidir.

Elektrik kablosu taşımak için kullanılan tüm kanalların (örneğin zemin kanalları, PVC kanalları, dış boru taşıma kanalları) uygun genişlikte olması sağlanmalıdır. Bir yandan, ek kablo ihtiyacını karşılayabilmek için yeterli alan olmalı, diğer taraftan kabloların birbirine karışmasını önlemek için asgari boşluklar bırakılmalıdır. Özellikle elektrik ve BT kabloları için ortak kanallar kullanılıyorsa, sinyal karışmasını, gürültü ve parazitleri önlemek için, bir ayırıcı aracılığı ile kabloların ayrı ayrı yönlendirilmesi sağlanmalıdır. Kablolar üzerinde oluşan parazitler çoğunlukla, elektrik ve BT kablolarının ayrı ayrı taşınması ile engellenebilir.

Yeterli genişlikte kablo kanal kurulumu mümkün değilse, kanal içerisinde en azından genişleme durumunda kullanılabilecek kadar alan bulundurulduğuna dikkat edilmelidir. Kablo kanallarının kurulumu sırasında, duvar ve tavan açıklıkları yeteri genişlikte planlanırsa, sonrasında oluşabilecek gürültülü, kirli ve masraflı genişletme işleri gerekmeyebilir. Geniş kurulan kablo kanalları içerisinde bulunan açıklıkların yangına dayanaklı malzeme (yangın bariyerleri) ile kapatılması, bu sayede yangına ve dumana karşı koruma sağlanması, genişleme durumunda bu malzeme yerine gerektiğinde ek kabloların kurulumunu kolaylaştıracaktır.

İçerisinden kabloların geçmesi planlanan duvarlar için, olası genişlemeler düşünülerek duvar açıklıklarının belirlenmesi, duvar açıklıklarının en fazla %60'a kadar kullanılması, kalan kısmın yangına dayanıklı malzemeler ile doldurularak yangın bariyerleri oluşturulması önerilmektedir. Açıklıkların, yangın koruma bariyerleri ve/veya yumuşak yangın koruyucular (köpük gibi) kullanılarak doldurulması, genişleme gerektiğinde daha pratik bir biçimde alan oluşturulmasına yardımcı olacaktır.

Kablo kanal boyutlarının, kullanılacak kablo tipleri göz önünde bulundurularak belirlenmesi sağlanmalıdır.

Kurulumda tasarlanan odaların elektrik bağlantı değerleri, bir süre sonra gerçek koşullara olan uygunluğunu yitirebilir. Özellikle elektrik tesisatının ilk kurulum aşamasında yanlışlıkla, üç fazdan birine daha fazla yüklenildiği durumlar ortaya çıkabilmektedir. Ayrıca odaların doluluk oranları ve elektrik kullanım değerleri, tasarım sırasında öngörülen değerler ile uyuşmayabilir. Kurulu elektrik tesisatının, güncel ihtiyaçları karşılayıp karşılamadığı, fazlar üzerinde yüklerin dengeli olup olmadığı düzenli olarak kontrol edilmeli, gerekli düzenlemelerin ve iyileştirmelerin yapılması sağlanmalıdır.

Düzenleme ve iyileştirme için odaların kullanımında değişikliklere gidilebileceği gibi gerekli durumlarda hatlar yeniden düzenlenerek, BT bileşenlerinin veya altyapı ekipmanlarının

farklı fazlardan beslenmelerini sağlamak da düşünülebilir. Bununla birlikte, bazı durumlarda mevcut tesisata ekler yapılabilir veya tamamen yeni bir tesisat da oluşturulabilir.

Gerekli kablo güzergahlarının, koridorların, kaçış ve kurtarma yollarının yanı sıra, duvarların içinde yer alan boru ve kablo kanallarında gerçekleştirilecek tüm çalışmalar ile ilgili yangın koruma görevlisinin bilgilendirilmesi önerilmektedir. Çalışma öncesi yapılacak bu tür bir bilgilendirme ile yangın güvenlik görevlisi, önleyici yangın korumasının işin uygulamasına dahil edilebilmesini sağlayabilecektir.

Yangın güvenlik görevlisinin (acil eylem sorumlusu) bu tür çalışmalara katılımı, çalışmalar öncesinde hazırlanan inşaat projesinin planlama ve kabul dokümanlarının yangın güvenlik görevlisi tarafından (yangın önlemleri açısından) değerlendirilmesi önerilmektedir. Çalışma kapsamında, yangın güvenlik görevlisi koordinasyonunda, yangın önleme tedbirlerinin alınması, düzgün bir biçimde işletilmesi, gerektiğinde güncellenmesi ve kontrol edilmesi sağlanmalıdır.

Kurumun yüksek erişilebilirlik gereksinimleri doğrultusunda, (genellikle veri merkezi içerisinde barındırılan) bina içerisinde bulunan kritik BT bileşenlerinin iki bağımsız elektrik hattı üzerinden beslenmesi sağlanmalıdır.

İmkanların uygun olması durumunda, kurum için kritik BT bileşenlerinin (merkezi depolama bileşenleri, merkezi ağ cihazları veya kritik sunucular) iki farklı elektrik hattı üzerinden veya birbirinden bağımsız iki farklı güç kaynağından beslenmesi önerilir. Bu sayede herhangi bir güç kaynağında sıkıntı yaşanması durumunda, diğer güç kaynağı kritik BT bileşenlerine enerji sağlamaya devam edebilecektir. Kritik olmayan BT bileşenleri tek güç kaynağından beslenebilir.

VMR.3.U3 Profesyonel kurulum

Elektrik kablolama kurulum çalışmaları, ilgili tüm standartlara uyumlu, dikkatli ve ustalıkla yapılmalıdır. Kurulumu gerçekleştirecek kişiler, konusuna hakim, tecrübeli uzmanlar arasından seçilmelidir. Elektrik kablolamanın belirlenen kriterlere uygun, profesyonel bir biçimde uygulandığını, yetkilendirilmiş kişiler tarafından her aşamada kontrol edilmelidir.

Ekipmanların teslimi sırasında, doğru kabloların ve bağlantı bileşenlerinin tedarik edilip edilmediği kontrol edilmelidir. Elektrik kabloları ve kablo kanalları döşenirken, kurulumun herhangi bir hasara neden olmadığına ve bina kullanımını etkilemediğine dikkat edilmelidir.

Ayrıca mümkün olduğunca BT kablolarının ve elektrik kablolarının ayrı kanallar içerisinden taşınması sağlanmalıdır.

2.2 2.SEVİYE UYGULAMALAR

1.Seviye uygulamalar sonrasında, elektrik kablolama altyapılarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar, aşağıdaki uygulama maddelerini dikkate alarak, iyileştirme/geliştirme faaliyetlerini planlayabilirler.

VMR.3.U4 Elektrik kablolama ihtiyaç analizi

Kablolama çalışmaları öncesinde, mevcut ve geleceğe yönelik ihtiyaçlar göz önünde bulundurularak, elektrik kablolama gereksinimleri oluşturulmalıdır. İhtiyaç analizinde öncelikle kurum kullanıcılarının, veri merkezi içerisinde bulunan tüm BT bileşenlerinin ve kullanılan altyapı ekipmanlarının kısa ve uzun vadeli elektrik tüketim profilleri çıkarılmalı; kısa vadede hangi kullanıcıların ne kadar elektrik tüketebileceği ve bu kullanımın daha uzun vadede ne kadar artacağı tahmin edilmelidir.

VMR.3.U5 Elektrik kablolamanın iş kabulü

Elektrik kablolama, kurulumun tamamlanmasından sonra bir muayene ve kabul sürecine tabi tutulmalı; işletim sırasında düzenli aralıklarla elektrik tesisatı ve kullanılan ekipmanlar muayene edilmelidir. Bu muayeneler sırasında bilgi güvenliği unsurları da (bkz. VRM.3.U11 Elektrikli cihazların ve elektrik altyapısının yangın çıkarma riski) dikkate alınmalıdır. İlk kurulum sonrası kabul aşamasında gerçekleştirilmesi gereken faaliyetler TS HD 60364-6 (IEC 60364-6, DIN-VDE 0100-610) “Alçak gerilim elektrik tesisleri – Bölüm 6: Doğrulama” standardında detaylı bir biçimde açıklanmaktadır.

Kabul, elektrik kablolama çalışmasına ilişkin tüm görevler tamamlandıktan, işi icra eden/yüklenici kabul aşamasına gelindiğini bildirdikten sonra ve işveren (kurum) tarafından yapılan muayenelerde kabul edilemez eksiklikler bulunmadığında yapılmalıdır. Yapılan incelemelerde kabul edilemez eksikliklerin bulunması durumunda, bu eksikliklerin giderilmesi için makul bir süre verilmeli, sonrasında yeni bir kabul tarihi seçilmelidir.

Muayene ve kabul sırasında:

- Kurulumların, üretici firmanın belirlediği koşullara uygun bir şekilde gerçekleştirilip gerçekleştirilmediği,
- Yangın yalıtımlarının uygun malzemeler ile doğru biçimde yapılıp yapılmadığı,
- Doğru tip ve miktar kablo kullanılıp kullanılmadığı,
- Elektrik tesisatının tasarıma uygun bir şekilde kurulup kurulmadığı,
- Gerekli uyarı işaretlerinin kullanılıp kullanılmadığı,
- İlgili dokümantasyonun hazırlanıp hazırlanmadığı,
- İletkenlerin doğru bir biçimde bağlanıp bağlanmadığı,
- Topraklamanın uygun bir biçimde yapılıp yapılmadığı,

ve benzeri unsurlar kontrol edilmeli, sonuçlar bir kabul tutanağı içerisinde kayıt altına alınmalıdır.

Kabul tutanağı için bir kontrol listesi hazırlanmalıdır. Kontrol listesi, işletme alanları için genel gereksinimleri de içermelidir. Kabul tutanağı, katılımcılar ve sorumlu kişiler tarafından yasal olarak bağlayıcı bir şekilde imzalanmalıdır. Tutanak, kablolama dokümanlarının bir parçası olmalıdır.

VMR.3.U6 Aşırı gerilimden korunma

Elektrik ileten ağlarda (güç veya veri iletimi olup olmadığına bakılmaksızın) her an aşırı gerilim oluşabilir. Çoğunlukla bu tür aşırı gerilimlere, aynı şebeke içerisinde bulunan diğer tüketiciler neden olur. Diğer taraftan, yıldırım nedeniyle oluşan aşırı gerilim daha az yaşanmakla birlikte, çok daha yüksek hasarlara sebebiyet verebilir.

Aşırı gerilimler, kullanılan (veri veya elektrik taşıyan) kabloların yanı sıra telefon hatları, su veya gaz boruları gibi elektriksel iletken hatlar ile de binaya ve BT bileşenlerine ulaşabilir, iç hatlara yansıyabilir.

BT bileşenlerini ve altyapı ekipmanlarını korumak için alınabilecek gerekli tedbirler, aşırı gerilimin oluşma nedenine bakılmaksızın esasen aynıdır. Yıldırım ve aşırı gerilimden korunma ile ilgili çeşitli standartlar bulunmaktadır. ISO 62305, IEC 61643-11, IEC 60634, UL 1449 bunlardan bir kısmıdır. Türkiye'de TS EN 62305-1/2/3/4 standardı yıldırıma ve aşırı gerilime karşı koruma oluşturmanın genel kurallarını açıklar. Standardın ikinci bölümü olan "Risk Yönetimi", yıldırım ve yıldırım sonucunda oluşabilecek aşırı gerilimin önlenmesinde risk odaklı bir yaklaşım sunmaktadır. Üçüncü bölüm, yapıların ve kişilerin fiziksel olarak korunmasını, dördüncü bölüm "Yapılarda Elektrik ve Elektronik Sistemler" ise bina içerisinde yer alan elektrik ve elektronik sistemler için uygulanabilecek önlemleri ele almaktadır.

Kurumların aşırı gerilimden korunabilmeleri için, TS EN 62305 standardına uygun bir aşırı gerilim koruma konsepti oluşturulmaları gereklidir.

Aşırı gerilim koruma konsepti içerisinde; elektrik dalgalanmalarından ve aşırı gerilimden korunma cihazları, alternatif güç kaynakları (jeneratör sistemleri) ve kesintisiz güç kaynakları (UPS'ler) dikkate alınmalıdır. UPS'ler, kendisine bağlı ekipmanlara bir miktar koruma sağlamakla birlikte hiçbir şekilde aşırı gerilim koruyucusu olarak kabul edilmemeli, aksine aşırı gerilimden korunması gereken bir elektronik cihaz olarak düşünülmelidir.

Aşırı gerilim korumasına ek olarak, özellikle veri merkezi ve sistem odalarında elektrostatik yüke karşı gerekli önlemler alınmalıdır. Bu odalarda bulunan zemin kaplamalarının direnci 10 – 100 megaohm arasında olmalıdır. Veri merkezi ve sistem odası içerisinde bulunan,

yangına sebep olacak veya yangının büyümesine katkıda bulunacak tüm unsurlar bir yangın yükü (tehdidi) oluşturur. Zemin kaplamaları en az elektrik kabloları kadar yangın tehlikesi oluşturmaktadır. Malzemelerin alev alması veya yanmazlığı hakkında TS EN 13501-1+A1 (EN 13501-1+A1, DIN 4102-1) standartları içerisinde detaylı bilgiler bulunmaktadır. Zemin kaplama için kullanılacak malzemenin, DIN 4102-1 standardına göre en az "B1 Zor Alevlenici - yangın geciktirici" sınıfında olması önerilmektedir. Bu durum yükseltilmiş zeminler için de geçerlidir.

Aşırı gerilimden korunma modelinde, boyutu ne olursa olsun aşırı gerilim korumasına dahil edilen tüm ekipmanların, kapsamlı potansiyel dengeleme/topraklama sistemlerine ihtiyacı bulunur. Aşırı gerilim nedeniyle BT bileşenleri üzerinde meydana gelen hasarın büyük bir bölümü yanlış uygulanmış (veya uygulanmamış) topraklamadan kaynaklanır. Veri merkezi içerisinde yer alan BT bileşenleri için farklı topraklama sistemlerinin kullanılması, elektriksel potansiyel farkının oluşmasına neden olur. Bu veri merkezi içerisinde istenmeyen bir durumdur. Elektriksel potansiyel farkını ortadan kaldırmak ve potansiyel dengelemeyi oluşturmak amacı ile veri merkezi içerisinde tüm cihazların ortak bir topraklama sistemini kullanmaları önerilmektedir.

BT bileşenlerinin düzgün biçimde çalışmasını engelleyen bazı arızalara, elektrik iletkenleri neden olur. Özellikle farklı kaynaklardan oluşan sinyallerin birbirine karışması (gürültü/parazit oluşumu), yıldırım veya anahtarlama operasyonlarının neden olduğu aşırı gerilimlerin BT bileşenlerine kadar taşınması önemli arıza kaynakları arasında görünmektedir. Bu tür sorunları ortadan kaldırabilmek için bozulmanın elektriksel yayılımını engellemek ve BT bileşenlerine kadar ulaşmasını engellemek gereklidir. Galvanik izolasyon (veya sadece izolasyon) ile elektriksel yayılım kesilebilir, bozulmanın BT bileşenlerini etkilemesinin önüne geçilebilir.

VMR.3.U7 Gereksiz kabloların çıkarılması ve devre dışı bırakılması

Gereksiz kablolar, kullanım değişikliği veya modernizasyon nedeniyle gerekliliğini yitiren kablolardır. Bina yangın yüklerini en aza indirmek ve mevcut kablo kanallarını gerektiği gibi kullanabilmek için bu kablolar tamamen kaldırılmalıdır. Kabloların çıkartılması sonrasında, kablo kanallarının ve yangın duvarlarının düzgün bir biçimde (yangına dayanaklı malzemeler ile bir yangın bariyeri oluşturacak biçimde) kapatılmış olduğundan emin olunmalıdır.

İhtiyaç duyulmayan ve kaldırılması gereken kablolar, yetkili bir ekip tarafından dikkatli bir inceleme sonrası belirlenmeli ve ekip tarafından alınan kararlar kayıt altına alınmalıdır.

Kablolama altyapısında yapılan değişiklikler çalışma saatlerinde yürütülüyorsa, operasyonel işleyişin aksamaması için gerekli tedbirler alınmalı ve kesintilerin en aza

indirilmesi sağlanmalıdır. Bu amaçla, çalışmaların hafta sonu ve gece geç saatlerde yapılacak şekilde bir takvim oluşturulması gerekir.

Kabloların yenilenmesi sırasında, kablo kanallarında mevcut kabloları ve yeni döşenecek kabloları barındırabilecek yeterli alan bulunmuyor ise, geçiş süresini en aza indirmek için, önce yeni kablolar için kanalların kurulması, yeni kabloların ve tesisatın döşenmesi, kullanıma hazır hale getirilmesi, daha sonra eski tesisatın (kablolar, kablo kanalları, vb.) devre dışı bırakılması düşünülmelidir. Eski tesisatta yer alıp, ileride kullanılabileceği düşünülen kablo kanalları ve kablolar uygun koşullarda saklanmalı, kullanılmayacak olan her türlü ekipman ise kurum varlık imha politika ve talimatlarına göre elden çıkarılmalıdır.

Kablolar ve kablo kanalları üzerinde gerçekleştirilen tüm değişiklikler, ilgili dokümanlar (veya kullanılan yazılımlar) içerisinde denetlenebilir bir şekilde kayıt altına alınmalıdır.

İşletim güvenliği sağlama amaçlı, düzenli aralıklar ile uzman bir kişi tarafından elektrik tesisatının denetlenmesi önerilmektedir. Ayrıca bina ve veri merkezi kullanımlarında yaşanan değişikliklerin, elektrik tesisatı üzerine olan etkileri değerlendirilmeli ve gerekli önlemler/iyileştirmeler planlanmalıdır.

VMR.3.U8 Kablo taşıma sistemlerinin yangından korunması

Elektrik kabloları genellikle kablo kanalları aracılığı ile taşınmakta, kablo kanalları ise bina içerisinde, kaçış ve kurtarma yolları üzerinde, yeraltı otoparklarında, depolarda, ziyaretçilerin bulunabildiği yerlerde ya da farklı kullanım alanlarında bulunabilmektedir.

Bina içerisinde kullanılan tüm elektrik kabloları (yangın bölgelerinden, duvarlardan, tavanlardan geçirilen veya trafik güzergahlarına döşenen vb.) yangın güvenlik yönetmeliklerine tabi olmalıdır. Özellikle kablo kanalları, yangın ikaz ve alarm sistemleri, yangın söndürme sistemleri veya acil durum aydınlatması için kullanılıyorsa, yangın durumunda elektrik kablolarının fonksiyonel bütünlüğünün bozulmaması için ek önlemler alınmalıdır. Bu nedenle, kablo kanalları ve taşıma güzergahları planlanırken, yangın güvenlik görevlisine (acil durum sorumlusu) danışılması önerilmektedir. Kablo kanallarının yangına dayanıklı malzemeler kullanılarak yalıtılması, düzgün bir biçimde kilitlenmesi gibi önlemler yardımıyla, kanalların gerek yangına, gerekse sabotaja karşı korunması sağlanmalıdır.

Elektrik kablolarının, yangın korumalı kablo kanallarında sıkı ve yoğun bir şekilde taşınması durumunda, kanal içerisinde yüksek sıcaklık artışı meydana gelebilir. Oluşan ilave ısı elektrik hattı direncinde de bir artışa neden olabilir. Bu durum kanaldan geçen kablo miktarının azaltılması veya kanalın uygun biçimde havalandırılması ile giderilebilir. Bu ve olası benzeri sorunlar nedeniyle elektrik tesisatının seçilmesi ve montajı sırasında,

TS HD 60364-5-52 (IEC 60364-5-52, DIN VDE 0100-520) "Binalarda elektrik tesisatı – Bölüm 5-52: Elektrik donanımının seçilmesi ve montajı – Çekilen hat sistemleri (iletkenler)" standardının dikkate alınması önerilmektedir.

Kablo döşenmesi sırasında zemin, duvar veya tavanda oluşan boşluk ve aralıklar, TS EN 13501-1+A1 (EN 13501-1+A1, DIN 4102-1) ve benzeri standartlar göz önünde bulundurularak, yangına dayanıklı uygun malzemeler ile doldurulmalı, yangın bariyerleri oluşturulmalıdır. Özellikle duvarlardaki açıklıkları kapatmak için yangın durdurucu yastık ve köpükler, mastikler kullanılabilir. Fakat kablo kanalları duvar içerisinden geçiyorsa, yangın durumunda ısınarak genişleyecek kablo kanalları, kullanılan bu yumuşak yangına dayanıklı malzemeyi yok edebilir, duvara zarar verebilir. Bu nedenle kablo kanallarının, duvarlara bitişik olmaması veya duvar içerisinden geçirilmemesi; her iki taraftan da kanal ile duvar arasında en az 10 cm mesafe bırakılması önerilmektedir.

Bir kablo kanalı genellikle farklı kablo tipleri barındırır (telefon hatları, yerel alan ağı kabloları, binanın teknik kabloları, vb.). Kablolama ile ilgili yapılacak bir değişiklik esnasında, yakın gelecekte diğer kablo sistemlerinin de değiştirilmesi gerekip gerekmediği planlama aşamasında hesaba katılmalıdır. Farklı kablo sistemlerinde yapılacak değişikliklerin birlikte projelendirilmesi ile kesintiler en aza indirilebilir ve tekrar tekrar uygulanması gerekecek yangın bariyerleri oluşturma masrafında da belirli bir oranda tasarruf sağlanacaktır.

Eğer planlama aşamasında öngörülen kablo kanal güzergahı, yangın koruma yönetmelikleri nedeniyle uygulanamıyorsa, alternatif bir güzergah belirlenmelidir. Buna ek olarak, montaj çalışmalarının tamamlanmasından sonra, oluşturulan yangın bariyerleri düzenli aralıklarla (örneğin yılda bir kez) kontrol edilmelidir.

VMR.3.U9 Elektrik kablolamanın dokümantasyonu ve etiketleme

Kablolamaya ilişkin iyi bir dokümantasyon ve içerisinde ilgili tüm bileşenlerin net bir şekilde tanımlanması, bakım, onarım, sorun giderme ve kontrol için oldukça önemlidir. Hazırlanan dokümantasyonun kalitesi, dokümanların eksiksizliği, güncelliği ve okunabilirliğine bağlıdır. Her durumda, kablolamaya ilişkin tüm bilgilerin doğru bir şekilde kayıt altına alınmasından ve dokümantasyonundan sorumlu bir kişinin atanması önerilmektedir.

Bir tesisatın boyutu genişledikçe, tüm bilgiler tek bir plan içerisinde tutulamaz hale gelebilir. Bu durumda bilgileri bölmek daha yararlı olacaktır. Gerçek konum bilgileri daima ölçekli planlarla çizilmelidir. Diğer bilgiler, tablolar veya şematik planlar halinde saklanabilir. Tüm bilgilerin açık ve net olarak, gerektiğinde erişilebilecek biçimde organize edilmesi önemlidir. Dolayısıyla dokümantasyon içerisinde tanımlayıcı belgeler, listeler ve planlar bulunmalıdır.

Tanımlayıcı belgeler (örneğin dokümantasyon rehberi, dokümantasyon yönetimi politikası, vb.) içerisinde, dokümantasyon yönetimi için kullanılan prosedürler, tanımlama ve etiketleme kuralları gibi bilgiler bulunur. Bu belgeler arasında, örneğin, hangi durumlarda ne tür liste ve planların oluşturulması gerektiği ve oluşturulan dokümanların nasıl denetime uygun bir biçimde yönetilmesi gerektiği anlatılmalıdır.

Oluşturulan listeler ve planlar, kablolama için önemli tüm unsurlara ilişkin bilgileri içermelidir. Bu bilgiler arasında:

- Tedarikçi ve bileşen bilgileri,
- Kullanılan kablo tipleri,
- Kablo etiketleri,
- Merkezi dağıtım noktalarının yerleri,
- Bina ve odalar için sorumlu kişiler ve iletişim bilgileri,
- Ekipman yerleşim planları,
- Kablo kullanım bilgileri,
- Yerleşke ve kablo taşıma kanallarının boyutlandırılmış saha planları,
- Bina bölümlerinin şematik planları,
- Tam konuma sahip boyutlandırılmış kat planları,
- Panoların konumları,
- Odalara ait prizler vs.,
- Teknik oda planları, yükseltilmiş zemin planları, sunucu kabinlerinin pozisyonları, bina elektrik iletim planları ve klima sistemleri,
- Tehlike bölgeleri,
- Mevcut önlemleri

gibi birçok detayı içerebilir.

Hazırlanan dokümantasyon aracılığı ile kablolamaya ilişkin genel resim, hızlı ve kolay şekilde elde edilebilmelidir.

Dokümantasyonun güncelliğinin sağlanması amacı ile kablolama ile ilgili tüm çalışmalar, dokümantasyon yönetiminden sorumlu kişilere zamanında bildirilmeli, bu kişilerin gerekli değişiklikleri dokümanlara yansıtması sağlanmalıdır.

Dokümantasyonlar hassas (ve kimi zaman kritik) bilgiler içerdiğinden, güvenli bir şekilde saklanmaları ve dokümanlara erişimin kontrol altında tutulması gerekir.

Hazırlanan prosedürlere göre, kablolar (her iki uçlarından) etiketlenmelidir. Bu amaçla özel etiketler kullanılmalı ve silinmeyen kalemler kablolar ile işaretlenmelidir. Kabloların

etiketlenmesi sırasında, kablonun kritikliğini, önemini belirten kısaltmalardan ve renklerden kaçınılması, sadece kablo tanımlama bilgisine yer verilmesi önerilmektedir.

Dokümanların planlama aşamasından itibaren bir yazılım yardımıyla oluşturulmaya başlanması ve işletim aşamasında da aynı yazılım aracılığı ile doküman yönetiminin devam ettirilmesi önerilmektedir. Bu şekilde aynı doküman üzerinde gerektiğinde birden fazla kişinin çalışabilmesini sağlamak, dokümanlar üzerinde değişiklikleri takip etmek, dokümanları güncel tutmak daha pratik olabilecektir.

VMR.3.U10 Elektrik tesisatlarının ve bağlantıların kontrolü

Elektrik tesisatının ilk montajı ve kabulü sonrası, düzenli aralıklarla elektrik tesisatları ve kullanılan ekipmanlar kontrol edilmelidir. Bu muayeneler sırasında bilgi güvenliği unsurları da dikkate alınmalıdır. İlk kurulum sonrası, kabul aşamasında gerçekleştirilmesi gereken faaliyetler TS HD 60364-6 (IEC 60364-6, DIN-VDE 0100-610) “Alçak gerilim elektrik tesisleri – Bölüm 6: Doğrulama” standardında detaylı bir biçimde açıklanmaktadır.

Kontroller deneyimli, sertifika sahibi bir uzman tarafından gerçekleştirilmelidir. Kontrolü gerçekleştiren uzman, kurulumları ve tesisatın çalıştırılmasını denetlemeli; ayrıca test ölçümleri yapmalıdır. Çalışma sırasında,

- İmalatçının teknik özelliklerine göre elektrik tesisatının kurulup işletildiği,
- Yangın bariyerlerinin doğru kurulduğu,
- İletim hatlarının mevcut taşıma kapasitesi, koruyucu ekipmanın seçimi ve planlamaya uygunluğu,
- Elektrik devre planlarının doğru ve bütünsel olduğu,
- İkaz ve uyarı bilgilendirmelerinin yapıldığı,
- Tüm iletim hatlarının düzgün şekilde bağlandığı

kontrol edilmelidir. Ayrıca elektrik tesisatının yalıtım direncinin ölçülmesi, otomatik kapanma ile korunmanın doğrulanması önerilmektedir. Gerçekleştirilen tüm kontrollerin sonuçları, ölçüm sonuçları ile birlikte test raporları olarak kayıt altına alınmalı ve uygun bir şekilde saklanmalıdır.

İşletim güvenliğinin sağlanabilmesi için düzenli aralıklar ile uzman bir kişi tarafından elektrik tesisatının muayene edilmesi (denetlenmesi) önerilmektedir. Ayrıca bina, veri merkezi kullanımlarında yaşanan değişikliklerin elektrik tesisatı üzerine olan etkisi değerlendirilmeli, gerekli önlemler/iyileştirmeler planlanmalıdır.

VMR.3.U11 Elektrikli cihazların ve elektrik altyapısının yangın çıkarma riski

Yapısal yangın koruma önlemlerinin büyük bir kısmı, genişleyen yangınların sınırlandırılmasının yanı sıra kişilerin tahliye edilmesi ve kurtarma ekiplerinin gerekli

alanlara erişimlerini sağlamayı amaçlamaktadır. Bu önlemlerin genellikle yangın kaynağı veya çıkış nedeni üzerinde etkileri son derece azdır, yangının başlamasını durduramazlar.

Yangının başlamasını engellemek için çalışanların ve diğer kişilerin dikkatli ve gözlemleyici olmaları beklenmektedir. Özellikle çalışanlar günlük çalışma ortamlarında kül tablaları, kağıt bulunan çöpe sigara veya izmarit atılması gibi yangına neden olabilecek potansiyel kaynaklara dikkat etmelidir.

Elektrikli cihazlar

Kurum tarafından yeni bir cihaz satın alındığında, hala çalışmakta olan eski cihazlar bir şekilde kullanılmaya devam eder. Kurum içerisinde farklı bir iş birimine devredilebilir, farklı bir kuruma gönderilebilir fakat çalışan cihazlar genellikle atılmaz. Oysa ki, eskiyen elektrikli cihazların yeni cihazlara göre, hasar yaşama olasılığı daha fazladır. Dolayısıyla bu tür cihazların daha yüksek yangın tehlikesi içerdiği göz ardı edilmemelidir.

Bu nedenle, kurum içinde "eski" elektrikli cihazların kullanımı için bir düzenlenme getirilmesi önerilmektedir. Eski elektrikli cihazların, uzman bir elektrikçi tarafından kontrol edilmesi ve emniyetli olduğunun belirlenmesi durumunda kullanımına izin verilmesi sağlanmalıdır. Onaylanmış cihazlar özel bir etiket ile işaretlenmeli, eski ve kontrolden geçmemiş cihazlardan ayrışmaları sağlanmalıdır.

Özellikle sürekli çalıştırılan buzdolapları ve genellikle saatlerce açık çalıştırılan kahve makineleri, BT bileşenleri ile birlikte bulundurulmamalı, bu amaç için tasarlanan (küçük mutfak, vb.) odalarla çalıştırılmalıdır.

Grup prizler / Uzatma kabloları

Bir alanda ne kadar fazla elektrik prizi olursa olsun, her zaman ya yetersizdir ya da yanlış yerde bulunurlar. Bu eksikliği gidermek için genellikle grup prizler veya uzatma kabloları kullanılır. Kalitesiz veya yanlış bir biçimde kullanılan grup prizleri / uzatma kabloları son derece tehlikeli bir ateşleme (yangın) kaynağı oluşturur.

Grup prizlerin / uzatma kablolarının kullanımından mümkün olduğunca kaçınılması önerilmektedir. Gerekli durumlarda, uzman bir elektrik teknisyeni tarafından var olan elektrik tesisatı üzerinden yeni prizler açılmalı ve duvara monte edilmelidir.

Yeni prizlerin açılması mümkün değilse ve grup prizlerin / uzatma kablolarının kullanılması kaçınılmaz ise aşağıdaki hususlara dikkat edilmesi gerekir:

- Sadece uzman bir elektrik teknisyeni tarafından kontrol edilmiş ve güvenli olduğu tespit edilen, yüksek kaliteli grup prizler / uzatma kabloları kullanılmalıdır,

- Fazla sayıda, küçük grup prizleri / uzatma kabloları kullanmak yerine geniş ve çoklu grup prizler / uzatma kabloları tercih edilmelidir,
- Grup prizleri / uzatma kabloları asla birbirine bağlanmamalıdır,
- Grup prizlere / uzatma kablolarına aşırı yüklenilmemelidir (genellikle sınır 3500 watt'tır),
- Grup prizleri / uzatma kabloları yürüyüş alanlarında veya ayak altlarında bulundurulmamalıdır.

Elektrik Dağıtım

Elektrik tesisatında kullanılan tüm ekipman (özellikle kullanılan elektrik sigortaları, bağlantı bileşenleri ve noktaları) teknik cihazlarda olduğu gibi yaşlanmaya tabidir. Bu nedenle tüm ekipmanların sağlıklı bir biçimde çalıştıklarına dair, DIN VDE 0105-100: 2005-06 "Elektrik sistemlerinin işletimi" standardına uygun bir biçimde, düzenli aralıklarla denetlenmelidir. Denetimler sonucu, elektrik tesisatının ve ekipmanların işletim emniyeti ve etkinliği güvence altına alınır.

Gerçekleştirilen tüm kontrollerin sonuçları, ölçüm sonuçları ile birlikte test raporları olarak kayıt altına alınmalı ve uygun bir şekilde saklanmalıdır. Herhangi bir hasar durumunda yetkili kişi, ilgili kurum ve kuruluşlara (ticaret denetim makamları, meslek kuruluşları, sigorta şirketleri, vb.) elektrik tesisatı üzerinde gerçekleştiren test raporlarını sunabilmelidir.

Havalandırma fanları

Kir ve toz tarafından bloke edilmiş fanlar, gerekli soğutmayı sağlayamadıkları için, BT bileşenlerinin aşırı ısınmalarına sebebiyet verebilir. Aynı zamanda fanların kendileri de bir yangın kaynağı olabilir.

Bu sebeple, fanların toz birikintileri açısından düzenli aralıklarla (yılda en az bir kere) kontrol edilmesi ve temizlenmesi gerekir.

Kayıt Altına Alma

Gerçekleştirilen tüm incelemelerin sonuçları kayıt altına alınmalı ve uygun bir şekilde saklanmalıdır.

2.3 3.SEVİYE UYGULAMALAR

1. ve 2. seviye uygulamalar sonrasında, artan koruma koşullarında dikkate alınması gereken önlemler aşağıda yer almaktadır. Kurumların ve organizasyonların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun uygulamalardan faydalanmaları önerilir. Uygulama kapsamında öncelikli koruma sağlanan prensip

parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VMR.3.U12 İkincil güç kaynağı (E)

Elektrik şebekesi, üretilen elektrik enerjisini kullanıcılara iletmek için oluşturulmuş bir ağdır. Ülkemizde veri merkezinin (veya sistem odasının) bulunduğu yere bağlı olarak, elektrik şebekesi aracılığıyla, elektrik hizmeti o bölgede dağıtım işini üstlenmiş şirket tarafından sunulur.

Elektrik dağıtım şirketleri her zaman, yerleşim birimlerine kesintisiz enerji sağlamayı garanti edemezler. Erişilebilirlik gereksinimi yüksek olan veri merkezleri, şebekede yaşanacak olası bir kesinti durumunda veri merkezine enerji sağlayacak ikincil (acil durum) bir güç kaynağı ile desteklenmelidir.

Elektrik şebekesinde yaşanan kesintilerin veri merkezini etkilememesini sağlamak için kullanılan UPS sistemi, şebekede meydana gelebilecek olası dalgalanmalara karşı BT bileşenlerini koruyabilir veya sahip oldukları aküler yardımıyla geçici bir süre (genellikle 30 dakika kadar) BT bileşenlerini besleyebilir.

UPS sistemi ile kısa süreli kesintilerin veri merkezini etkilememesi sağlanabilir fakat uzun süreli kesinti durumunda UPS sistemi yeterli olamaz. Bu yüzden şebekede yaşanacak olası bir kesinti durumunda veri merkezine enerji sağlayacak yedek sistemler, ikincil (acil durum) güç kaynakları düşünülmelidir. Bu amaçla genellikle jeneratörlerden yararlanılır. Veri merkezi erişilebilirlik gereksinimleri doğrultusunda, yerel koşullar izin veriyorsa, jeneratör yerine ikinci bir elektrik şebekesinden gelen elektrik hattı ile de yedekleme sağlanabilir.

Enerji konusunda yedekli yapılar ve modülerlik konularında daha detaylı açıklamalar “VMR.2 Veri merkezi ve Sistem odası” uygulama rehberinde yer almaktadır.

Şebekede uzun süreli kesinti yaşanması durumunda, ikincil (acil durum) güç kaynağı devreye girerek BT işletiminin sürdürülmesini sağlar. İkincil (acil durum) güç kaynağının bulunduğu ortamın da yönetilmesi gerekir. Bunların yerleştirileceği odanın kendine ait bir yangın söndürme sistemine sahip olması sağlanmalı, içeride ısınan havanın dışarı atılması ve soğutmanın gerçekleştirilmesi için gerekli iklimlendirme sistemi kurulmalıdır. Bu kaynaklar yangın ve suya karşı korunmalı, ayrıca yetkisiz kişilerin erişimleri engellenmelidir.

İkincil (acil durum) güç kaynağı olarak kullanılacak sistemlerin, doğru ve sorunsuz çalışmasını sağlamak için düzenli olarak bakıma tabi tutulması gerekir. Bunun için üreticinin sağladığı bakım aralıklarına dikkat edilmeli, bakım esnasında yük ve fonksiyon

testleri yapılmalıdır. Buna ek olarak, ikincil (acil durum) güç kaynağı olarak kullanılacak sistemlerin en az iki yılda bir, gerçek koşullar altında, test amaçlı çalıştırılması sağlanmalıdır.

VMR.3.13 A-B ("Dual bus") yedekli sistem (E)

Erişilebilirlik gereksinimleri yüksek ve kritik BT bileşenlerine, enerjinin farklı hatlar üzerinden sağlanması önerilmektedir.

A-B yedekli sistemlerde; enerji BT bileşenlerine iki farklı dağıtım hattı üzerinden iletilir. En ideal durumda, her dağıtım hattı (yedekli olarak çalışıp birbirini destekleyen UPS'lerin oluşturduğu) bir UPS sistemi ve şebeke kesintisi halinde yeteri kadar elektrik üretebilecek jeneratörler ile desteklenir. Kritik BT bileşenleri, iki farklı dağıtım hattından (enerji yükü kanallar arasında %50 oranında paylaştırılacak şekilde) beslenebilecek şekilde yapılandırılır. Böylece enerji yükü dengeli olarak ikiye bölünmüş olur. Çift güç besleme ünitesine sahip BT bileşenlerinde, her bir güç besleme ünitesi farklı bir dağıtım hattından enerji ihtiyacını karşılayabilir. Üzerinde tek güç besleme ünitesi bulunan BT bileşenlerinin ise uygun bir transfer anahtarı (STS/ATS) üzerinden beslenmesi sağlanır.

Dağıtım hatları, tek başına bütün enerjiyi tüketen BT bileşenlerine gerekli enerjiyi sağlayabilecekleri biçimde planlanmalıdır. Böylece dağıtım hatlarından herhangi birinde sorun yaşanması durumunda, diğer dağıtım hattı tek başına bütün bileşenler için gerekli enerjiyi sağlayabilir.

Kurulan yedekli sistemin işlevselliği yetkili kişiler tarafından ve uygun ekipmanlar kullanılarak düzenli aralıklarla izlenmelidir. İki güç besleme ünitesine sahip cihazlarda hangi besleme ünitesinde arıza verdiği izlenebilir. Ayrıca farklı dağıtım hatları aracılığı ile A-B enerji iletiminin erişilebilirliği izleme araçları ile de takip edilebilir.

A-B yedekli sistem aracılığıyla, en etkin, verimli ve güvenli bir biçimde enerjinin iletilebilmesi için, her bir dağıtım hattı için kullanılan kabloların farklı kablo kanalları aracılığıyla taşınması önerilmektedir.

VMR.3.14 Elektrik kablolamanın malzeme güvenliği (E)

Ziyaretçilerin kullandığı odalarda veya binanın izlenemeyen alanlarında yer alan kabloların (kablo kanalları) ve dağıtım panolarının yetkisiz erişime karşı korunması sağlanmalıdır. Korunma için çeşitli yöntemlerden yararlanılabilir:

- Kabloların veya kablo kanallarının sıva altına döşenmesi,
- Kabloların zırhlı borular içinden geçirilmesi,
- Kabloların mekanik olarak güçlü ve kilitlenebilir kanallara döşenmesi,
- Panoların kilitlenmesi,

- Kablo kanallarının ve panoların izlenmesi.

Prensip olarak kabloların yetkisiz kişilerin erişebileceği yerlerden geçirilmemesi, korunması gerekli kablo uzunluğunun mümkün olduğunca kısa tutulması önerilir.

Kablo güvenliğinin sağlanabilmesi için kablo kanallarının güzergahı boyunca, karşılaşılabilecek tehdit unsurları da göz önünde bulundurulmalı, alınması gereken önlemler planlanmalıdır. Koridor veya yeraltı otoparkı gibi ulaşım yolları olarak kullanılan alanlarda yer alan kablolar, kazara meydana ve gelebilecek mekanik hasarlara, gerekli durumlarda sabotaja karşı korunacak şekilde sağlam bir biçimde kapatılmalıdır.

Kilitli tutulan dağıtım panoları ve kablo kanallarına ilişkin anahtarların dağıtımını, kullanımını ve (panolara, kanallara) erişim yöntemlerini belirleyen düzenlemelerin oluşturulması gereklidir. Ayrıca kablolar, kablo kanalları veya panolarda yapılacak değişikliklerin nasıl yönetileceği, değişiklik öncesinde ve sonrasında nelere dikkat edileceği belirlenmelidir. Değişikliklerin koordine edilmesi, yetkili kişiler tarafından onaylanması ve kayıt altına alınması (ilgili diğer dokümanların güncellenmesi) sağlanmalıdır.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

Elektrik kablolama ile ilgili detaylı konulara aşağıdaki referans ve kaynaklardan ulaşılabilir:

- DIN 4102:2016-05
- IEC 60364 Electrical Installations for Buildings
- ANSI - American National Standards Institute
- BICSI - Building Industry Consulting Service International
- IEC 62305 – Lightning protection standard
- DIN VDE 0100 – Voltage electrical installation

VRM.4.U: BT KABLOLAMA

1 AÇIKLAMA

1.1 TANIM

BT kablolaması, kurum tarafından veri iletimi için kullanılan tüm iletişim kablolarından ve pasif bileşenlerden (bağlantı kutuları, dağıtım panoları (patch panel), vb.) oluşur. Aynı zamanda kurum iletişim ağının fiziksel temelidir. BT kablolaması, harici ağların bağlantı noktalarından (örneğin, telekomünikasyon sağlayıcısının ISDN bağlantısı veya internet sağlayıcısının DSL bağlantısı), ağ terminal noktalarına (son kullanıcı cihazlarının, sunucuların, vb. ağ bağlantılarına) kadar uzanır.

Bina teknik altyapısının bir parçası olan BT kablolaması, yapılandırılmış kablolama sistemleri için kurulan yaklaşımlara ve prosedürlere göre **üç farklı alan içerisinde** incelenebilir.

Birincil alan, binaları birbirine bağlayan kablo taşıma sistemlerinden oluşur. Genellikle uzun mesafeleri birbirine bağlayan birincil alan içerisinde yer alan kablolar üzerinden, az sayıda bulunan bağlantı noktaları arasında yüksek oranlarda veri iletir. Bu nedenle, sadece büyük işletme veya kurumlar kendi birincil kablolamalarını işletmektedir. Kurumun tek bir binada çalışması durumunda, bina içerisinde (genellikle veri merkezi veya sunucu odası) yer alan omurga ağ (ana dağıtım ağı) birincil alan olarak kabul edilir.

İkincil alan, merkezde bulunan omurga ağı (ana dağıtım ağı) ile binanın farklı katları veya alanları arasındaki kablo bağlantılarını ifade eder. Özellikle farklı katlara dağılmış kurumların birçoğunda bu tür alanlar mevcuttur.

Üçüncül alan kablolama, terminal cihazlarını (son kullanıcı cihazları, yazıcılar, sunucular, vb.) o alanda yer alan (örneğin aynı katta) merkezi bir dağıtım noktasına bağlayan kabloları içerir.

Yapısal kablolamada, terminal cihazlarının (doğrudan ağ altyapı bileşenlerinin barındırıldığı) veri merkezi ve/veya sistem odasına bağlanması durumuna sıkça rastlanılır. Bu durumda ikincil alan, kablolama anahtarları (switches) arasındaki bağlantı kablolarından oluşur. Üçüncül kablolama ise binadaki merkezi dağıtım noktasından odalarda yer alan bağlantı soketlerine kadar uzanır.

1.2 YAŞAM DÖNGÜSÜ

BT Kablolama Uygulama Rehberi, veri merkezinin ve veri merkezi içerisinde yer alan ve veri iletim ağına bağlanacak tüm BT bileşenlerinin ve altyapı ekipmanlarının, kurum ihtiyaçlarına uygun bir biçimde iletişim kurabilmesini sağlamak amaçlı planlama,

uygulama, işletme ve elden çıkarma aşamalarında yararlanılabilecek uygulama maddelerini içermektedir. Bu uygulama maddeleri mevcut bir binanın BT kablolama altyapısının yenilenmesi sırasında kullanılabileceği gibi yeni bir binanın BT kablolama altyapısının oluşturulması sırasında da kurumlara yardımcı olur.

Geçmiş tecrübeler, yeni bir bina içerisinde BT kablolama altyapısının sıfırdan oluşturulmasının/değiştirilmesinin, mevcut bir bina içerisinde yer alan BT kablolama altyapısının değiştirilmesine göre çok daha düşük maliyetli olduğunu göstermektedir.

Planlama ve Tasarım

Yüksek performanslı ve korunumlu kablolama altyapısının temelleri planlama aşamasında atılır. Başlangıç olarak, mevcut durumun ve yakın gelecekte gerçekleşmesi beklenen gelişmeler göz önünde bulundurularak ihtiyaç analizi yapılmalıdır (**bkz. VRM.4.U4 BT kablolama ihtiyaç analizi**).

İhtiyaç analizi sonrasında oluşturulan ağ yapısı doğrultusunda, kabloların mekanik ve elektriksel özellikleri, kullanım için seçilen kablo tipleri (**bkz. VRM.4.U1 Uygun kablo tiplerinin seçimi**), kablo güzergahları ve kablo taşıma sistemleri (kablo kanalları, kablo taşıyıcıları, vb.) (**bkz. VRM.4.U2 Kablo yönetimi**) belirlenmelidir.

Ayrıca planlama aşamasında, bina içerisinde bulunan kabloların ve dağıtım panolarının, kötü niyetli kullanıma karşı fiziksel olarak korunması sağlanmalıdır (**bkz. VRM.4.U11 BT kablolamanın fiziksel güvenliği** ve **VRM.4.U13 Kabin sistemlerinin kullanımı**).

Uygulama

Planlama ve tasarım sonrası, erişilebilirliğin ve sorunsuz bir operasyonun sağlanabilmesi için doğru bir biçimde kurulum gerçekleştirilerek (**bkz. VRM.4.U3 Profesyonel kurulum**) BT kablolama altyapısı kullanıma hazır hale getirilmelidir. Yangın kontrolü için önemli unsurlardan bir tanesi de kablo taşıma sistemleridir. Korunmamış kablo kanalları ve yangın bariyerlerinin bulunmaması, yangının ortaya çıkmasına (yangın durumunda yangının daha hızlı yayılmasına) neden olabilir (**bkz. VRM.4.U7 Kablo taşıma sistemlerinin yangından korunması**). Kabloların döşenmesi sırasında, ayrıntılı ve doğru bir dokümantasyon oluşturmak oldukça önemlidir. İlerleyen aşamalarda hangi kablonun nereden geldiğini, nereye gittiğini ve nereye bağlandığını belirlemek çok daha zor olacaktır (**bkz. VRM.4.U8 BT kablolamanın dokümantasyonu ve etiketleme**).

Kurulumlar sonrasında ve BT kablolama altyapısının işletimine başlamadan önce, veri merkezinin tüm BT kablolama altyapısı bir kabul/onay sürecinden geçmelidir (**bkz. VRM.3.U5 BT kablolama muayene (kabul)**).

İşletim

BT bileşenlerine yetkisiz erişimin önlenmesi için, sadece ihtiyaç duyulan bağlantıların ve soketlerin etkinleştirilmesi sağlanmalıdır. Bununla birlikte, veri iletiminin güvenli ve sorunsuz bir biçimde gerçekleşebilmesi için tüm etkinleştirilen bağlantıların ve soketlerin kullanımları düzenli olarak kontrol edilmelidir (**bkz. VRM.4.U9 Mevcut bağlantıların kontrolü**). Ayrıca ağ dokümantasyonun güncelliği güvence altına alınmalıdır (**bkz. VRM.4.U6 Ağ dokümanlarının gözden geçirilmesi ve güncellenmesi**).

Sonlandırma/elden çıkarma

Kullanılmayan, işlevini tamamlamış BT kablolarının ve bileşenlerinin ortadan kaldırılmaları veya uygun şekilde elden çıkarılmaları sağlanmalıdır.

Acil Durum Planlaması

Yüksek erişilebilirlik gereksinimleri kapsamında, kullanılan harici bağlantılar da dahil olmak üzere tüm BT kablolama altyapısının yedekli olarak tasarlanması düşünülmelidir. Böylelikle BT kablolama altyapısında belirli bir bölümde/bölgede meydana gelebilecek bir arızanın, tüm sistem erişilebilirliğini etkilemesi engellenebilecektir (**bkz. VRM.4.U10 Ağ yedekliliği**).

2 UYGULAMALAR

Aşağıda yer alan maddeler, "BT Kablolama" temel varlığına özel uygulama maddeleridir.

2.1 1.SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

VRM.4.U1 Uygun kablo tiplerinin seçimi [Bina hizmetleri yöneticisi]

Kablo seçiminde, teknik gereksinimlerin yanı sıra kabloların yer aldığı çevre ve işletim koşulları da dikkate alınmalıdır. Bu tür gereksinimleri karşılama amaçlı, kablo üreticileri farklı kablo çeşitleri sunarak ihtiyaca uygun çözümler geliştirirler.

Bina içinde veya dış alanlardaki kablo kurulumlarında, özellikle kablo kaplamaları/korumaları ile ilgili aşağıdaki kriterler dikkate alınmalıdır:

- Sıcaklık,
- Çevresel ortam (su, kanalizasyon, asit, gaz, ışık, toprak),
- Kemirgen koruması, çarpma dayanımı (stone-chip resistance), su basıncı direnci, vb.,
- Yangına yatkın alanlarda koruma seviyesi,
- Havadan (yukarıdan) hat kullanımlarında oluşabilecek özel gerilme kuvvetleri.

Buna ek olarak kablo taşımasında kullanılacak platformlar, kablo kanalları, kablo merdivenleri, döşemeler, tuğlalar, vb. unsurlar işin içerisine dahil edilmeli, ilgili yönetmelikler ve standartlar değerlendirilmelidir (IEC 60364, TS HD 60364, DIN VDE 0100, DIN 4102, vb.). Uluslararası standart ISO/IEC 14763-2 kablolama için kurulum, planlama, yönetim ve bakım kurallarını tanımlar.

Kablo seçimi, sadece BT ekipleri tarafından belirlenmemeli, işletim ortamı ile ilgili çevresel etkiler veya özel yapısal özellikler de göz önünde bulundurulmalıdır.

Özellikle bina işletimi, yapısal özellikler ve binaya özgü diğer özel koşullara aşina olan bina hizmetleri personelinin/teknisyenlerin, kablo taşıma sistemlerinin belirlenmesi, uygun kablo tipinin seçimi gibi kablo tasarım çalışmalarına dahil olmaları sağlanmalıdır.

Veri iletişimi veya haberleşme açısından, ihtiyaç duyulan veri transfer hızının (tam olarak doğru olmasa da bant genişliği olarak da nitelendirilir) ve veri iletimi gerçekleştirecek iletim veya aktarma birimleri arasındaki mesafenin göz önünde bulundurulması gereklidir. Kullanılabilecek farklı kablo tiplerine ilişkin avantajlar ve dezavantajlar aşağıda açıklanmıştır.

Kablolu veri iletiminde, genellikle elektrik veya optik ara bağlantılar (interface) kullanılmaktadır. Elektrik iletimi genellikle bakır teller gibi metal iletkenler aracılığı ile sağlanırken, optik (ışık ile) iletim için sentetik veya cam fiber kablolardan yararlanılmaktadır.

Bakır ve fiber optik kablolar, sektördeki kısaltmaları ile aşağıda ayrıntılı olarak ele alınmaktadır.

Bakır Kablolar – Bükümlü Çift (Twisted Pair) Kablo

BT kablolamada kullanılan bakır kablolar, bükümlü çift tipi kablolardır. Bu tipte, iki bakır telin birbirine geçirilmesi (bükülerek) ile bir çift oluşur. Dört farklı bükülmüş çift bir araya getirilerek, bir yalıtım malzemesi (örneğin plastik) ile giydirilir ve kabloyu meydana getirir. Bükümlü çift kablolarda veriler, bakır teller üzerinden analog sinyaller halinde gönderilir. Bükümlü çift tipi kablolar telefon sistemlerinde de kullanılır.

İki telin birbirine geçirilmesi ile oluşturulan basit bükümler,

- Çıplak kablonun ürettiği elektromanyetik alanın etkisini sınırlayıp diğer kablolarda parazit oluşumunu önleyerek,
- Kablo çiftini elektromanyetik alanın etkisine karşı daha az duyarlı yapıp diğer kablolardan kaynaklanan paraziti önleyerek,

kabloyu ağda kullanıma uygun hale getirir.

Bükümlü çift kablonun koruyucu ile sarılmış haline Korumalı Bükümlü Çift Kablo (Shielded Twisted Pair – STP) denir. İzole edilmiş bükümlü çiftlerin etrafına sarılmış metal koruyucu ile kablo elektromanyetik alandan daha iyi korunmakta ve sinyalin bozulmadan uzun mesafelere iletilmesine olanak sağlamaktadır. Korumasız Bükümlü Çift Kablo (Unshielded Twisted Pair), BT kablolamada çok rastlanılan ve Ethernet protokolünün fiziksel katmanında en çok kullanılan kablo türüdür. 4 Mbps ile 1 Gbps arasında değişen bant genişliği sağlar. Geçmişte tüm BT bileşenlerinin veri iletim ağına erişimlerini sağlamak ile birlikte geniş alan ağlarının omurgasını oluşturmak için de kullanılan bu tür kablolar, günümüzde yerini yavaş yavaş fiber optik kablolara bırakmaktadır.

Kurumların değişen güvenlik ihtiyaçlarına uygun farklı tipte bükümlü çift kablolar bulunmaktadır.

Örneğin:

- Korunmasız bükümlü çift kablo (U / UTP),
- Korunmasız, tüm tel çiftleri için ortak korunumlu bükümlü çift kablo (F / UTP veya SF / UTP),
- Her tel çiftinin ayrı ayrı korunduğu bükümlü çift kablo (U / FTP),
- Her tel çiftinin ayrı ayrı korunduğu, ortak korunuma da sahip bükümlü çift kablo (F / FTP, S / FTP ve SF / FTP).

Standartlar (özellikle ISO/IEC 11801) ile kablolar ve bağlantı bileşenleri, iletim özelliklerine göre kategori ve sınıflara ayırılmaktadır.

Kategoriler, kablolama altyapısı bileşenlerinin gereksinimlerini ve sınırlarını (örneğin belirli mesafe ve süre içerisinde kablo üzerinden iletilebilecek veri miktarı) tanımlamaktadır. Artan kategori ile birlikte, kabloların belirli bir mesafe için üzerinden geçirebilecekleri veri miktarı da yükselir. Veri iletim hızını

- **Kategori 1 (CAT 1):** 1985'te ortaya çıkmıştır. Telefon hatlarında kullanılır.
- **Kategori 2 (CAT 2):** 4 Mbps (Megabit / saniye) hızında veri transferi sağlar. Geçmişte kullanılan, günümüzde fazla görülmeyen token-ring tipi veri iletim ağlarında ve bazı telefon sistemlerinde kullanılmıştır.
- **Kategori 3 (CAT 3):** 10 Mbps hızında veri transferi sağlar. Token-ring ağlarda ve 10BaseT sistemlerde kullanılmıştır ve bazı telefon sistemlerinde hala kullanılmaktadır.
- **Kategori 4 (CAT 4):** 16 Mbps hızında veri transferi sağlar. Token-ring ağlarda, 10BaseT ve 10BaseT4 sistemlerde kullanılmıştır.

- **Kategori 5 (CAT5 ve CAT5e):** Yerel ağ bağlantıları için kullanılır. Günümüzde neredeyse tüm yerel ağ bağlantıları Kategori 5 kablolar ile yapılmaktadır. 100 metrelik mesafe aşılmadığı müddetçe (100 MHz frekans ile) 100 Mbps'lik veri aktarım kapasitesine sahiptir. Bu nedenle 100 Mbps hızını destekleyen Ethernet kartı ile çalışabilecek en uyumlu kablodur. Gelişmiş kategori 5 (CAT5e) tipi kablo ile 1 Gbps'lik (1000 Mbps) veri taşıma kapasitesine ulaşılabilir.
- **Kategori 6 (CAT 6):** Kategori 5 kablosuna göre daha yüksek frekans geçişlerine (250 MHz) elverişli olup, 1 Gbps hızında veri iletimine imkan tanır. CAT6a tipi kablo ile 10 Gbps'lik veri taşıma kapasitesine ulaşılabilir. Gigabit Ethernet kartlarıyla birlikte kullanılır.
- **Kategori 7 (CAT 7):** Kategori 6 kablosuna göre daha yüksek frekans geçişlerine (600 MHz) elverişli olup, 10 Gbps'lik veri taşıma kapasitesine ulaşabilirler. Gigabit veya 10 Gigabit Ethernet kartlarıyla birlikte kullanılır.

Yüksek kalitede veri iletimi ancak, uyumlu kablo ve bağlantı bileşenleri ve profesyonel bir kurulum ile elde edilebilir. BT bileşenleri kablo uzunluğunu algılayamazlar, sadece gelen elektrik sinyallerine tepki verebilirler. Bu nedenle, standartlar ile belirtilen kablo elektriksel sınır değerlerine önem verilmelidir. ISO / IEC 11801'e göre, bakır kablolar için maksimum uzunluk 90 m. (ek ve bağlantı kabloları ile birlikte 100 m.) olarak belirlenmiştir. Bununla birlikte azami uzunluk, gerekli elektrik iletim parametreleri karşılanırsa veya elektrik sinyal güçlendirici cihazlar kullanılırsa artabilir.

Bükümlü çift kablolar aşağıdaki avantajlara sahiptir:

- Düşük veri aktarım kapasitesinin (bant genişliğinin) yeterli olduğu durumlarda, bükümlü çift kabloların metre başına düşen maliyeti fiber kablolara göre daha azdır,
- Bükümlü çift kablolar nispeten daha kolay döşenebilir ve yönlendirilebilir,
- Bükümlü çift kablolar, evrensel kablolama (universal cabling) olarak düşünülebilir, diğer hizmetler için çok fazla teknik çaba sarf etmeden kullanılabilir (örneğin telefon hatları ile),
- Kablolama altyapısı kolayca kontrol edilebilir,
- Duvarlar arasından geçebilen esnek ve ince bir kablodur,
- Birden fazla hat aynı kablo sistemi üzerinden çalıştırılabilir.

Bunlara karşılık aşağıdaki dezavantajları bulunmaktadır:

- Veri iletimi sırasında kablolar üzerinden iletilen alternatif akımlar ortamda (dışarıdan) algılanabilir (kötü niyetli kişilerin veri iletimini dinleme riski),
- Veri iletimi sırasında kablolar üzerinden iletilen alternatif akımlar diğer sistemleri (ve kabloları) rahatsız edebilecek elektromanyetik alanlar üretebilir,

- Çift bükümlü kablolar elektromanyetik alanlara karşı duyarlıdır, gürültü/parazit oluşabilir,
- Uzun mesafelerde, yüksek hızlı veri iletişimi için uygun değillerdir.

Fiber Optik Kablolar

Fiber optik kablolar, ince ve hassas bir cam (ya da plastik) hat üzerinden ışığın iletilmesi prensibiyle çalışan bir sistemdir. Fiber optikte sinyaller, kızılötesi ışıklar ile iletilir. İletim için öncelikle fiber kablo girişinde, elektrik sinyali lazer (veya LED) diyotlar aracılığı ile optik sinyale (ışın demeti) dönüştürülür. Optik, sinyal alıcı tarafa iletilir. Alıcı tarafta sinyal, yarı iletken elemanlar kullanılarak tekrar elektriksel sinyal oluşturulur.

İletim için kullanılan fiber optik kablo (fiber de denir), ışığın hareket ettiği bir çekirdek (core) bölge ve çekirdeği çevreleyen, optik malzemeden üretilmiş, çekirdekten yansıyan ışığı tekrar çekirdeğe geri gönderen bir kaplama malzemeden oluşur. Binlerce fiberin bir araya gelmesi ile oluşan bu kabloların en dış kısmında da kabloyu darbelere ve neme karşı koruyan kılıf bulunur. Uzun mesafelere veri aktarımı için tasarlanmış olan fiber optik kablolar, teoride en yüksek bant genişliğine sahiptirler.

Fiber optik kablolar, yapıldıkları malzemeye, çekirdek çaplarına ve ışığın kırılma şekline göre tek modlu ve çok modlu fiber optik kablolar olarak ikiye ayrılırlar. Tek Mod Fiberler (Single Mode Fiber- SMF) :

- Çekirdek çapı küçüktür,
- Işığın tek bir mod ya da tek bir yolda ilerlemesine olanak tanırlar,
- Işığı uzun mesafe taşıyabilirler,
- Düşük sinyal kayıplarının olduğu ve yüksek veri iletişim hızının gerektirdiği durumlarda kullanılırlar.

Çok Modlu Fiberler (Multi Mode Fiber- MMF) :

- Çekirdek çapı daha büyüktür,
- Birden çok ışık çekirdeğe alınıp iletilebilir,
- Işıklar daha kısa mesafe taşınabilir,
- Işın çarpışmaları meydana gelebileceğinden kısa mesafeler için kullanılır.

Bunun dışında, fiber optik kablolar aşağıdaki alanlarda kullanılmaktadır:

- Uzak yerleşim birimlerini birbirine bağlayan geniş ağ bağlantılarında (WAN - Wide Area Network),
- Yerleşke ağ bağlantılarında (MAN - Metropolitan Area Network),

- Yerleşim olarak birbirine yakın olan ağların bağlanmasında (LAN - Local Area Network),
- Yüksek düzeyde elektromanyetik parazit bulunan alanlarda,
- Veri merkezlerinde, yüksek veri hızıyla veri depolama için kullanılan BT bileşenlerinin ağ bağlantısını sağlamak için (SAN - Storage Area Network).

Fiber optik altyapısında kullanılan bağlantı elemanları, bağlantı kalitesi için belirleyici unsurlardandır.

Fiber optik kabloların kullanımı aşağıdaki avantajları sağlar:

- Fiber optik kablolar, bakır kablolarla karşılaştırıldıklarında, verinin daha uzak mesafelere yüksek bant genişliklerinde iletilmesine izin verir,
- Fiber optik kablolar, elektromanyetik alanlara duyarsızdır (Elektromanyetik bağışıklık),
- Elektrik iletkenlerde olduğu gibi sinyal karışma etkisi yoktur,
- Fiber optik kablolar üzerinden iletilen veri, kötü niyetli kişiler tarafından ancak pahalı ekipmanlar kullanılarak dinlenebilir,
- Fiber optik kablolar, kabloların uçları arasındaki eş potansiyel dengelemeyi ortadan kaldırır,
- Küçük boyutlu ve hafiflerdir.

Bununla birlikte, fiber optik kullanımı aşağıdaki dezavantajlara sahiptir:

- Fiber optik kabloların kurulum maliyetleri bakır kablolardan daha yüksektir,
- İşçilik gereksinimleri nedeniyle özel ekipman ve personel ihtiyacı vardır,
- Fiber optik kablolar, bakır kablolara kıyasla daha kırılgandır; özellikle iş bilgisayarlarında (ve diğer son kullanıcı BT ekipmanlarında) bakır, bükümlü çift kablo kullanılarak LAN bağlantısı gerçekleştirilmesi daha pratiktir,
- Özellikle tek modlu fiber için bakım ve işletme maliyetleri, diğer sistemlere kıyasla daha yüksektir.

Gerek fiber optik kabloların, gerekse bakır kabloların kurulumu sırasında, kullanılan kablo tipine göre asgari standart uzunluklara dikkat edilmelidir. Standartlarda belirtilen uzunluklar, genellikle kurulum kablosu, ek ve bağlantı kabloları (patch kablolar) göz önünde bulundurularak belirlenmiştir. Örneğin asgari kablo uzunluğu 100m. olarak verilen 1000Base-T için kurulum kablosunun uzunluğu, ek ve bağlantı kablolarına yeterli alanı sağlamak için 90 m'yi geçmemelidir.

Özet

Özellikle WAN ve MAN tipi ağlarda, tek modlu fiber optik kablolama bir standart haline gelmiş durumdadır. Ayrıca bu tür kabloların binalar arası bağlantılar ve kat dağıtımlarında, LAN kablolama için de kullanılması önerilmektedir.

İş bilgisayarları (ve diğer son kullanıcı BT ekipmanları) için fiber optik kabloların kullanılması ve katlarda bakır kabloların yerini alması, genel bir bakış açısıyla/bütünsel olarak değerlendirilmelidir.

Fiber optik kablo kullanımını destekleyen unsurlar:

- Yangın yükü bakımından daha uygun olması,
- Veri iletiminin dinlenmesinin daha zor olması,
- EMC nötr olması (EMC - Elektromanyetik Uyumluluk),
- Kapladığı alan nedeniyle kablo taşıma sistemi kurulumunda tasarruf,
- Gerekli dağıtım oda sayısının azalması nedeniyle yer tasarrufu ve dolayısı ile elektrik kablolama maliyetlerinin düşmesi,
- Daha basit UPS ve topraklama konseptleri.

Karşı unsurlar:

- Terminal cihazlarda (iş bilgisayarları, diğer son kullanıcı BT ekipmanları, vb.) ve ağ bileşenlerinde daha yüksek maliyetli arabirim kartları,
- Telefon kablolamanın bakır kablolama üzerinden kurulum gerekliliği,
- Bazı ekipmanlar için (örneğin IP Telefonlar) veri ve elektrik iletiminin aynı kablo üzerinden yapılması ihtiyacıdır.

Bu yüzden, özellikle yeni kurulum ve/veya modernizasyon çalışmaları sırasında, işin deneyimli uzmanlar tarafından, teknik, güvenlik ve ekonomik açılardan değerlendirilmesi, kullanılacak kablo tipinin bu değerlendirme sonrasında belirlenmesi önerilmektedir.

VRM.4.U2 Kablo yönetimi [BT Yöneticisi]

Kablo taşımak için kullanılan tüm kanalların (örneğin zemin kanalları, PVC kanalları, dış boru taşıma kanalları) uygun genişlikte olması sağlanmalıdır. Bir taraftan, ek kablo ihtiyacını karşılayabilmek için yeterli alan olmalı, diğer taraftan kabloların birbirine karışmasını önlemek için asgari boşluklar bırakılmalıdır. Özellikle elektrik ve BT kabloları için ortak kanallar kullanılıyorsa, sinyal karışmasını, gürültü ve parazitleri önlemek için, bir ayırıcı aracılığı ile kabloların ayrı ayrı yönlendirilmesi sağlanmalıdır. BT kabloları üzerinde oluşan parazitler ve gürültüler çoğunlukla, elektrik ve BT kablolarının ayrı yerlerden taşınması ile engellenebilir.

Yeterli genişlikte kablo kanalları kurmanın mümkün olmaması durumunda, kanal içerisinde en azından genişleme durumunda kullanılabilecek kadar alan bulundurulduğuna dikkat edilmelidir. Kablo kanallarının kurulumu sırasında, duvar ve tavan açıklıkları yeteri genişlikte planlanırsa, sonrasında oluşabilecek kirli, gürültülü ve masraflı genişletme işleri gerekmeyebilir. Geniş kurulan kablo kanalları içerisinde bulunan açıklıkların yangına dayanaklı malzeme (yangın bariyerleri) ile kapatılması, bu sayede yangına ve dumana karşı koruma sağlanması, genişleme durumunda bu malzeme yerine gerektiğinde ek kabloların kurulumunu kolaylaştıracaktır.

Kablo kanal boyutlarının, kullanılacak kablo tipleri göz önünde bulundurularak belirlenmesi sağlanmalıdır. Örneğin, ortak güzergâh boyunca çok sayıda (tek çekirdekli) tek mod fiber kablo kullanmak yerine, tek bir (çok çekirdekli) çok modlu fiber kablo kullanılarak alandan tasarruf sağlanabilir. Belirli bir düzene göre korumalı kılıflar ve/veya fiber kablo kullanımı çapraz (sinyal) karışma sorunlarını önleyebilir. Bu şekilde dar bir alana sahip kablo kanallarında bile sorunsuz bir çalışma ortamı oluşabilir.

Kablo taşıma sistemleri planlanırken, öngörülebilir tehlike kaynaklarından kaçınmaya özen gösterilmelidir. Kablolar, sadece bina içerisinden erişilebilen kanallar aracılığıyla taşınmalıdır. İyi tasarlanmış ve düzenlenmiş kablo kanalları kontrolü kolaylaştırır. Kablo kanalları ve kablolar, insanlar, taşıtlar ve makineler nedeniyle oluşabilecek hasara karşı korunacak şekilde döşenmelidir.

BT kablosu bağlanacak cihazlar ve cihaza bağlı kabloların kişilerin yürüme veya araçların geçiş alanları üzerinden geçmemesine dikkat edilerek yerleştirilmelidir. Eğer kabloların bu tür alanlar üzerinden taşınması bir zorunluluk ise, bunların gerekli ağırlığı kaldırabilecek şekilde yapılandırılacak kanal yolları içerisinde taşınarak korunmaları sağlanmalıdır.

Yeraltında bulunan otoparklar, hasar azaltmaya yönelik kablo yönetimi için ciddi riskler içerir. Örneğin otopark giriş kapılarının uzun süreler açık kalması, üçüncü şahısların otoparklara erişimine olanak sağlayabilir. Düşük tavan yükseklikleri nedeniyle, genellikle tavanda yer alan kablo kanallarına basit aletler ile rahatlıkla ulaşılabilir. Otopark içerisinde izin verilen taşıt yüksekliğinin belirlenmesi sırasında, taşıt geçiş alanında bulunan kablo kanallarının göz önünde bulundurulmaması, kablo kanallarının (ve dolayısıyla kabloların) yüksek taşıtlar nedeniyle zarar görmelerine ve elektrik kabloları üzerinde ciddi hasarlar oluşmasına neden olabilir.

Farklı kurumlar ile ortak kullanılan binalarda, kabloların ortak olarak kullanılmakta olan zemin, tavan veya duvar gibi alanlardan geçmesini önlemek için özen gösterilmelidir. Tüm kablo taşıma sistemleri, diğer kurumlar tarafında kullanılmakta olan alanlardan fiziksel

erişimi engellemek amacı ile mekanik olarak kilitlenmelidir. Mümkün olması durumunda alan sınırlarında, kabloların sonlandırılması sağlanmalıdır.

Yangın riski yüksek alanlardan mümkün olduğunca kablo geçirilmemesi önerilmektedir. Kabloların, yangına rağmen belirli bir süre iletişimi devam ettirebilmesi, devre bütünlüğü olarak tanımlanır. Kanallar içerisinde bulunan tüm kabloların devre bütünlüğünü sağlamak için kablo kanalının yangın riski yüksek alanda kalan parçası üzerinde, yangına dayanıklı özel maddeler kullanılarak yalıtım gerçekleştirilmelidir. Taşıma kanalları yerine ihtiyaç tek tek kablolar ile giderilebiliyorsa veya sadece belirli kablolar için devre bütünlüğü önemliyse, yangına dayanıklı bir kablo tipi ve sabitleme tertibatı kullanılmalıdır. Devre bütünlüğü sadece uygun tip kablolar ile sağlanmaz. Kablo taşıma sisteminin kablo kanalları, kablo merdivenleri, kablo kelepçeleri veya kanalet gibi bileşenler ile birlikte bir bütün olarak düşünülmesi gereklidir. Bununla birlikte yangın durumunda yukarıdan düşen parçaların, kablo taşıma sistemini tahrip etmemesini sağlamak da son derece önemlidir.

Zemin altında bulunan kablo kanalları için, kanalın yaklaşık 10 cm yukarısına bir risk uyarı etiketi yerleştirilmelidir. Kablo kanalı içerisinden taşınmayan, tekli kablolar için özel kablo korumalarının kullanılması önerilir.

Kablolar, fırtınadan etkilenmeyecek şekilde taşınmalıdır. Örneğin, bina çatısı üzerinden geçirilecek kabloların, en azından her 5 metrede bir uygun şekilde çatı yüzeyine bağlanması sağlanmalıdır. Fırtına nedeniyle oluşan kuvvetler, kablo veya kablo tellerini etkileyebilir. Buna ek olarak, bir fırtına durumunda, kablolar üzerine düşecek nesneler kabloları tahrip edebilir. Bu tür durumlara karşı da korunma gereklidir. Bu yüzden, çatı ve panjur yüzeyleri üzerinde bulunan kabloların döşenmesinde daima muhafaza boruları kullanılmalıdır.

VRM.4.U3 Profesyonel kurulum [Bina hizmetleri yöneticisi]

BT kablolama kurulum çalışmaları, ilgili tüm standartlara uyularak, dikkatli ve ustalıkla yapılmalıdır. Kurulumu gerçekleştirecek kişiler, konusuna hakim ve tecrübeli uzmanlar arasından seçilmelidir. Kablo ve pasif bileşen üreticileri yasal asgari sınırları aşan garantiler sunuyorsa, konu ile ilgili sertifikalı bir şirket tarafından kurulumun gerçekleştirilmesi sağlanmalıdır. BT kablolamanın belirlenen kriterlere uygun, profesyonel bir biçimde uygulanma durumu, yetkilendirilmiş kişiler tarafından her aşamada kontrol edilmelidir.

Ekipmanların teslimi sırasında, doğru kabloların ve bağlantı bileşenlerinin tedarik edilip edilmediği kontrol edilmelidir. Temin edilip kullanılmayan kablolar ve ilgili malzemeler, uygun bir şekilde depolanmalıdır. Depo alanı kuru olmalı ve hava değişikliklerinden

etkilenmemelidir. Kullanım öncesi, depolanan malzemenin orijinal ambalajında bırakılması önerilir.

BT kabloları ve kablo kanalları döşenirken, kurulumun herhangi bir hasara neden olmadığına ve bina kullanımını etkilemediğine dikkat edilmelidir. Ayrıca mümkün olduğunca, BT kablolarının ve elektrik kablolarının ayrı kanallar içerisinden taşınması sağlanmalıdır.

Kablolamaya ilişkin ilk olarak 1995 yılında, iletişim bağlantılarının topolojisini ve sınıflandırmasını tanımlayan "EN 50173 - Genel Kablolama Sistemleri" standardı yayımlanmıştır. Avrupa Birliği içerisinde, kablolama ile ilgili standartlardan CENELEC (European Committee for Electrotechnical Standardization - Avrupa Elektrik Standardizasyon Komitesi) sorumludur. CENELEC sorumluluğunda, ISO/IEC (Uluslararası Standart Komiteleri) ile koordineli bir biçimde ilgili standartlar izlenir, gerekli görülürse geliştirilir ve güncellenir. Ülkemizde ise Türk Standartları Enstitüsü (TSE) standartların oluşturulması, yayımlanması ve güncel tutulması ile ilgili kurumdur.

BT ve iletişim kablolamaya ilişkin standartlar ile bina planlaması, kablolama tasarımı, planlama, uygulama ve işletim aşamalarında ilgili kişilerin desteklenmesi hedeflenmektedir.

Bu standartlar arasında, en yaygın kullanılanlardan biri, EN 50173 serisi içerisinde farklı kurulum alanlarındaki bakır ve fiber optik yapısal kablolama sistemleri için tasarım gereksinimleri tanımlanmaktadır. EN 50174 serisi ise bakır ve fiber optik yapısal kablolama sistemleri için pratik kurulum gereksinimlerini içerir.

Aşağıda yer alan standart alt başlıkları, farklı BT kablolama yaşam döngüsü fazları ile ilişkilendirilebilir:

Bina planlaması

- TS EN 50310 – Eş potansiyel kuşaklama ve topraklama uygulaması – Bilgi teknolojisi donanımı bulunan binalarda:
    - 5.2: Bir binada ortak potansiyel dengeleme sistemi (CBN)
    - 6.3: AC dağıtım ve koruyucu iletken bağlantısı (TN-S)

Kablolama tasarımı

- TS EN 50173-1: Bilgi teknolojisi – Jenerik kablolama sistemleri – Bölüm-1: Genel kurallar:
    - 4: Topoloji
    - 5: İletim hatlarının performansı
    - 7: Kablolar için gereksinimler

- 8: Kablo bağlantılarının gereksinimleri
- A.1: Kablo kanallarının sınır değerleri

Planlama

- TS EN 50174-1: Bilgi teknolojisi – Kablo döşeme – Bölüm 1: Teknik şartlar ve kalite güvencesi:
  - 4: Tespit yönetimi
  - 5: Kalite kontrolü
  - 7: Kablolama yönetimi
- TS EN 50174-2: Bilgi teknolojisi – Kablo döşeme – Bölüm 2: Döşeme planlaması ve bina içi uygulamalar:
  - 4: Güvenlik gereksinimleri
  - 5: Bakır ve fiber optik kablo kurulum genel şartnameler
  - 6: Bakır kablo kurulumu için ek gereksinimler
  - 7: Fiber optik kablo kurulumu için ek özellikler
- TS EN 50174-3: Bilgi teknolojisi – Kablo döşeme – Bölüm 3: Tesisat planı ve bina dışı uygulamalar
- TS EN 50310 – Eş potansiyel kuşaklama ve topraklama uygulaması – Bilgi teknolojisi donanımı bulunan binalarda:
  - 5.2: Bir binada ortak potansiyel dengeleme sistemi (CBN)
  - 6.3: AC dağıtım ve koruyucu iletken bağlantısı (TN-S)

Uygulama

- TS EN 50174-1: Bilgi teknolojisi – Kablo döşeme – Bölüm 1: Teknik şartlar ve kalite güvencesi:
  - Dokümantasyon
  - Kablolama yönetimi
- TS EN 50174-2: Bilgi teknolojisi – Kablo döşeme – Bölüm 2: Döşeme planlaması ve bina içi uygulamalar:
  - 4: Güvenlik gereksinimleri
  - 5: Bakır ve fiber optik kablo kurulum genel şartnameler
  - 6: Bakır kablo kurulumu için ek gereksinimler
  - 7: Fiber optik kablo kurulumu için ek özellikler
- TS EN 50174-3: Bilgi teknolojisi – Kablo döşeme – Bölüm 3: Tesisat planı ve bina dışı uygulamalar
- TS EN 50310 – Eş potansiyel kuşaklama ve topraklama uygulaması – Bilgi teknolojisi donanımı bulunan binalarda:

- 5.2: Bir binada ortak potansiyel dengeleme sistemi (CBN)
- 6.3: AC dağıtım ve koruyucu iletken bağlantısı (TN-S)

- TS EN 50346 – Bilgi teknolojisi – Kablolama kurulumu-Kurulu kablolamanın test edilmesi:
  - 4: Genel gereksinimler
  - 6: Fiber optik kablolama için test parametreleri

İşletim

- TS EN 50174-1: Bilgi teknolojisi – Kablo döşeme – Bölüm 1: Teknik şartlar ve kalite güvencesi
  - 5: Kalite kontrolü
  - 7: Kablolama yönetimi
  - 8: Onarım ve bakım

2.2 2.SEVİYE UYGULAMALAR

1.seviye uygulamalar sonrasında, BT kablolama altyapılarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar, aşağıdaki uygulama maddelerini dikkate alarak, iyileştirme/geliştirme faaliyetlerini planlayabilirler.

VRM.4.U4 BT kablolama ihtiyaç analizi

BT kablolamaya ilişkin ihtiyaç analizi sırasında, BT kablolama tesisatının ekonomik etkinliğini ve kabiliyetini etkileyebilir tüm mevcut ve gelecekteki gereksinimleri karşılayabilmek için çeşitli unsurların ele alınması gerekir.

Genellikle en çok önem verilen soru, ihtiyaç duyulan veri iletim miktarıdır. Bu soruya cevap verebilmek için kullanıcıların mevcut kullanımları göz önünde bulundurularak, önce kısa vadede planlanan kullanım ihtiyaçları belirlenmeli, bu bilgi üzerine daha uzun vadeli ve geleceğe yönelik kullanım gelişimleri tahmin edilmelidir.

Bu konuda iki farklı tipte gelişim göz önüne alınmalıdır:

İlk olarak, bant genişliği maliyetleri gün geçtikçe daha uygun hale gelmektedir. Bu durum BT kablolama kapasitesinde, her zamankinden daha yüksek talep baskısının ortaya çıkmasına neden olmaktadır. E-Posta ve Internet gibi tipik BT hizmetlerinin yanı sıra günümüzde hızla yaygınlaşan yüksek kaliteli ses, görüntü, dijital TV içeriklerinin BT ağ alt yapısındaki payı gün geçtikçe artmaktadır. Bu nedenle, BT kabloların tipini ve kalitesini seçerken artan bant genişliği talepleri dikkate alınmalıdır.

Diğer yandan, BT ağları giderek daha fazla uygulamaya hizmet vermektedir. BT protokollerini ve standartlarını kullanan tüm uygulamalar yaygın bir şekilde bu ağları

kullanacaktır. Bu aslında BT ağlarının ve dolayısıyla BT kablolamanın gelecekte sadece bilgisayarlar arasındaki iletişiminde kullanılmayacağı anlamına gelmektedir. Örneğin, geçmişte kendi özel ağını kullanan telefon, günümüzde BT ağlarından yararlanmaktadır (IP Telefon). Buna benzer birçok uygulamanın, BT teknolojisini ve BT ağlarını gelecekte daha çok kullanacağı tahmin edilmektedir. Bu tür öngörülebilir gelişmeler, BT kablolama altyapısı ve bileşenlerinin planlanmasında dikkate alınmalıdır. Buna ek olarak, ileride yaşanabilecek oda veya bina kullanım değişikliklerinin kablolama değişikliklerine neden olabileceği düşünülmelidir. Bu değişikliklerin, sorunsuz ve az maliyetli bir şekilde gerçekleştirilebilmesini sağlamak için, bina iç kabloların ve kablo kanallarının esnek ve genişletilebilir şekilde tasarlanması önerilmektedir.

Teknolojide gözlemlenen standartlaşmaya rağmen, bazen belirli uygulamalar için farklı kablolama tasarımları veya ayrı kabloların kullanılması gerekebilir. Özellikle alarm sistemleri gibi özel güvenlik gerektiren durumlarda veya hassasiyet gerektiren makine ve üretim kontrol uygulamalarında ayrı kabloların ve iletim tekniklerinin kullanılması gerekli olacaktır. Farklı koruma gereksinimleri bulunan ve başka herhangi bir şekilde (örneğin VPN'ler kullanarak) korunamayan uygulamalar için kabloların ayrılması önerilmektedir.

Erişilebilirlik

Kablo taşıma sistemlerinin dikkatli bir biçimde planlanması ve inşa edilmesi, erişilebilirliğin sağlanması için büyük önem taşımaktadır. Erişilebilirlik gereksinimleri yüksek kurumlarda, yaşanabilecek arızalara rağmen veri iletiminin kesintisiz bir biçimde sürdürülebilmesini sağlamak amacıyla yedekli hatlar kullanılması önerilmektedir.

Bütünlük

Kablo üzerinden taşınmakta olan verinin bütünlüğü açısından dış etkenlere karşı koruma sağlamak öncelik taşımaktadır. Bu her şeyden önce, BT kablolarının elektrik kablolarından belirli bir uzaklıkta, ayrı olarak taşınması gerektiği anlamına gelir. Buna ek olarak, uygulama gereksinimlerine uygun kablo tiplerinin belirlenmesi gereklidir.

Gizlilik

Kurum için kablo üzerinden taşınan verilerin gizliliğinin sağlanması (kabloların dinlenmesine yönelik önlemler, vb.) önemli ise, ilk tercih fiber optik kabloların kullanımı olmalıdır. Fiber optik kabloların dinlenmesi, bakır kablo hatlara göre çok daha fazla teknik çaba gerektirir.

Kullanılan kablo türü ne olursa olsun, kötü niyetli kişilerin BT bileşenlerini yerel ağa dinleme amaçlı yetkisiz bağlamalarını önlemek için, tüm dağıtım panoları ve ağ bağlantı soketleri korunmalıdır.

Birçok durumda, taşınan verilerin gizliliğini ve bütünlüğünü (veri ileten terminalleri (BT bileşenleri) ve kullanılan iletim protokolleri desteklediği sürece), şifreleme yöntemlerinden yararlanarak (iletilen veriyi şifreleyerek) sağlamak mümkündür. Buna karşın şifreleme yöntemleri erişilebilirliğin korunmasına yalnızca özel durumlarda yardımcı olabilir.

Ek Gereksinimler

IP telefonları veya WLAN erişim noktaları gibi bazı aktif bileşenlerin, enerji ihtiyaçlarını BT kablolama üzerinden karşılayabilecekleri (POE – Power Over Ethernet – Ethernet üzerinden Enerji) unutulmamalıdır. Bu tür aktif bileşenlere enerji iletimi sadece bakır kablolar aracılığı ile mümkündür. Bu tür uygulamalarda bakır kablo kullanımı zorunlu hale gelir, fiber optik kablolar tercih edilemez.

VRM.4.U5 BT kablolama muayene (kabul) [Bina hizmetleri yöneticisi]

BT kablolama, bilgi güvenliği unsurları da dahil olmak üzere kurulumun tamamlanmasından sonra bir muayene ve kabul sürecine tabi tutulmalıdır.

Kabul, BT kablolama çalışmasına ilişkin tüm görevler tamamlandıktan, işi icra eden/yüklenici kabul aşamasına gelindiğini bildirdikten sonra ve işveren (kurum) tarafından yapılan muayenelerde kabul edilemez eksiklikler bulunmadığında verilmelidir. Yapılan incelemelerde kabul edilemez eksikliklerin bulunması durumunda, bu eksikliklerin giderilmesi için makul bir süre verilmeli, sonrasında yeni bir kabul tarihi seçilmelidir.

Aşağıdaki hususlar kabule hazırlık açısından yararlıdır:

- Kuruluma ait tüm belgelerin eksiksiz olarak hazırlanıp hazırlanmadığı kontrol edilmelidir,
- Ölçüm değerleri incelenmeli, olağan dışı değerler için ölçümlerin tekrarlanması sağlanmalıdır.

Muayene ve kabul sırasında:

- Yerleşke, kat ve kabin planlarındaki gereksinimlerin, kabul sırasında yerine getirilip getirilmediği kontrol edilmeli,
- Teslimat, nicelik ve nitelik bakımından kontrol edilmeli,
- Hizmetlerin profesyonel olarak yürütüldüğü denetlenmelidir. Örnekleme yöntemiyle bileşenlerin tasarıma uygun, doğru biçimde kurulup kurulmadığı yoklanmalı, ölçülerin tutturulup tutturulmadığı ve kablo taşıma kanallarının standarda uygun döşenip döşenmediği tespit edilmeli,
- Kabul öncesinde tespit edilen olağan dışı ölçüm sonuçları, kabul esnasında tekrar test edilmeli,

- Bulgular ve çözüm çalışmaları kayıt edilmeli,
- Bulgular için kesin çözüm tarihleri üzerinde anlaşılmalı ve yüklenici firmanın takvime uyması sağlanmalı,
- Garanti süreleri ve benzeri unsurlar kontrol edilmeli, tüm sonuçlar bir kabul tutanağı içerisinde kayıt altına alınmalıdır.

Kabul tutanağı için bir kontrol listesi hazırlanmalıdır. Kontrol listesi, işletme alanları için genel gereksinimleri de içermelidir. Kabul tutanağı, katılımcılar ve sorumlu kişiler tarafından yasal olarak bağlayıcı bir şekilde imzalanmalıdır. Tutanak kablolama dokümanlarının bir parçası olmalıdır.

Kabul sonrası, kabul sırasında ortaya çıkan bulguların düzeltilmesi ve kalan işlerin kontrol edilmesi (sözleşmeye dayalı ve yasal olarak izin verildiği ölçüde) gerekmektedir. Faturaların ancak bundan sonra ödenmesi sağlanmalıdır.

VRM.4.U6 Ağ dokümanlarının gözden geçirilmesi ve güncellenmesi

İhtiyaçlar doğrultusunda, ağlar ve BT kablolama altyapısı üzerinde değişiklikler yapılması gerekebilir. Ek kabloların kurulması, kablolama üzerinde gerçekleşebilecek yapısal değişiklikler, genişlemeler, aktif ağ bileşenlerinin güncellenmeleri (update) ve yükseltilmeleri (upgrade) bu tür değişikliklere örnek olarak gösterilebilir. BT kablolamaya ait dokümantasyon, ağ ve kablolamaya ilişkin herhangi bir değişikliğin ayrılmaz bir parçası olarak kabul edilmeli ve dikkate alınmalıdır. Değişikliklerin değerlendirilmesi sırasında bu dokümantasyonlardan yararlanılmalıdır. Ayrıca değişiklik ancak dokümantasyon gerekli biçimde güncellendikten sonra tamamlanmalıdır.

Genel işletim güvenliğinin ve izlenebilirliğinin desteklenmesi yanında, BT kablolama dokümantasyonu aşağıda yer alan amaçlara da hizmet eder:

- Ağ değişiklik çalışmalarında daha hızlı hareket imkanı,
- Arızaların daha kolay tespiti ve giderilmesi,
- Arıza oluşması durumunda daha kısa sürede arızayı giderebilme şansı,
- Bakım sözleşmelerinin ekonomik verimliliğinin artması.

Değişiklikten etkilenen dokümantasyon alanlarının kolayca güncellenebilmesi ve uyarlanabilmesi önemlidir. Dokümantasyon kılavuzları hazırlanarak ilgili dokümantasyonun yönetimi herkes tarafından uygulanabilir hale getirilmelidir. Dokümantasyon kılavuzları içerisinde dokümantasyon yönetimi için kullanılan süreçler, dokümantasyon alanları ve özellikleri tanımlanmalı (adlandırma ve numaralandırma alanları gibi), bu kılavuzlar ilgili kişilerin kullanımına sunulmalıdır.

Ayrıca, ağ ve BT kablolama dokümantasyonu için bir doküman yönetimi sisteminin kullanılması değerlendirilmelidir. Doküman yönetimi uygulaması aşağıdaki hususlarda doküman yönetimini kolaylaştırabilir:

- Planlama aşamasından itibaren değişikliklerin kayıt altına alınabilmesi,
- İlgili tüm kişilerin değişiklikler (ve planlamalar) hakkında bilgilendirilmesi,
- Onay ve devreye alma süreçlerinin entegrasyonu,
- Eski belgelerin arşivlenmesi.

Günümüzde ağ yönetimi için kullanılan bazı uygulamalar, kablo ve ağ bileşenlerine ilişkin dokümantasyonu (bağlantılar ile birlikte) desteklemekte, entegre olarak kullanabilmektedir. Hatta pasif bileşenlerin (kablo dağıtım panoları ve kablolar gibi) aktif olarak izlenebilmesini sağlayan araçlar bile bulunmaktadır.

VRM.4.U7 Kablo taşıma sistemlerinin yangından korunması [Bina hizmetleri yöneticisi]

Elektrik ve BT kabloları genellikle kablo kanalları aracılığı ile taşınmakta, kablo kanalları ise bina içerisinde, kaçış ve kurtarma yolları üzerinde, yeraltı otoparklarında, depolarda, ziyaretçilerin bulunabildiği yerlerde ya da farklı kullanım alanlarında bulunabilmektedir.

Bina içerisinde kullanılan tüm elektrik ve BT kabloları, başta yangın bölgelerinden, duvarlardan, tavanlardan geçirilen veya trafik güzergahlarına döşenen tüm kablolar olmak üzere, yangın güvenlik yönetmeliklerine tabi olmalıdır. Özellikle kablo kanalları, yangın ikaz ve alarm sistemleri, yangın söndürme sistemleri veya acil durum aydınlatması için kullanılıyorsa, yangın durumunda elektrik ve BT kablolarının fonksiyonel bütünlüğünün bozulmaması için ek önlemler alınmalıdır. Bu nedenle, kablo kanalları ve taşıma güzergahları planlanırken, yangın güvenlik görevlisine (acil durum sorumlusu) danışılması önerilmektedir. Kablo kanallarının yangına dayanıklı malzemeler kullanılarak yalıtılması ve düzgün bir biçimde kilitlenmesi gibi önlemler yardımıyla, kanalların gerek yangına, gerekse sabotaja karşı korunması sağlanmalıdır.

BT kablolarının, yangın korumalı kablo kanallarında çok sıkı bir şekilde taşınması durumunda, kanal içerisinde yüksek sıcaklık artışı meydana gelebilir. Özellikle elektrik kabloları ile BT kablolarının birlikte taşındıkları kablo kanallarında oluşan ilave ısı, elektrik hattı direncinde de bir artışa neden olabilir. Bu durum kanaldan geçen kablo miktarının azaltılması veya kanalın uygun biçimde havalandırılması ile giderilebilir. Bu ve olası benzeri sorunlar nedeniyle elektrik tesisatının seçilmesi ve montajı sırasında, TS HD 60364-5-52 (IEC 60364-5-52, DIN VDE 0100-520) "Binalarda elektrik tesisatı – Bölüm 5-52: Elektrik donanımının seçilmesi ve montajı – Çekilen hat sistemleri (iletkenler)" standardının dikkate alınması önerilmektedir.

Kablo döşenmesi sırasında zemin, duvar veya tavanda oluşan boşluk ve aralıklar, TS EN 13501-1+A1 (EN 13501-1+A1, DIN 4102-1) ve benzeri standartlar göz önünde bulundurularak, yangına dayanıklı uygun malzemeler ile doldurulmalı, yangın bariyerleri oluşturulmalıdır. Özellikle duvarlardaki açıklıkları kapatmak için yangın durdurucu yastıklar, yangın durdurucu köpükler ve mastikler kullanılabilir. Fakat kablo kanalları duvar içerisinden geçiyorsa, yangın durumunda ısınarak genişleyecek kablo kanalları, kullanılan bu yumuşak yangına dayanıklı malzemeyi yok edebilir, duvara zarar verebilir. Bu nedenle kablo kanallarının, duvarlara bitişik olmaması veya duvar içerisinden geçirilmemesi; her iki taraftan da kanal ile duvar arasında en az 10 cm mesafe bırakılması önerilmektedir.

Bir kablo kanalı çoğunlukla farklı kablo tipleri barındırır (telefon hatları, yerel alan ağı kabloları, binanın teknik kabloları, vb.). Kablolama ile ilgili yapılacak bir değişiklik esnasında, yakın gelecekte diğer kablo sistemlerinin de değiştirilmesi gerekip gerekmediği planlama aşamasında açıklığa kavuşturmalıdır. Farklı kablo sistemlerinde yapılacak değişikliklerin birlikte projelendirilmesi ile kesintiler en aza indirilebilir ve tekrar tekrar uygulanması gerekecek yangın bariyerleri oluşturma masrafında belirli bir oranda tasarruf sağlanır.

Eğer planlama aşamasında öngörülen kablo kanal güzergâhı, yangın koruma yönetmelikleri nedeniyle uygulanamıyorsa, alternatif bir güzergâh belirlenmelidir. Buna ek olarak, montaj çalışmalarının tamamlanmasından sonra oluşturulan yangın bariyerleri düzenli aralıklarla (örneğin yılda bir kez) kontrol edilmelidir.

VRM.4.U8 BT kablolamanın dokümantasyonu ve etiketleme [Bina hizmetleri yöneticisi]

Kablolamaya ilişkin iyi bir dokümantasyon ve içerisinde ilgili tüm bileşenlerin net bir şekilde tanımlanması; bakım, onarım, sorun giderme ve kontrol için oldukça önemlidir. Hazırlanan dokümantasyonunun kalitesi; dokümanların eksiksizliğine, güncelliğine ve okunabilirliğine bağlıdır. Her durumda, kablolamaya ilişkin tüm bilgilerin doğru bir şekilde kayıt altına alınmasından ve dokümantasyonundan sorumlu bir kişinin atanması önerilmektedir.

Bir BT ağının boyutu genişledikçe, tüm bilgiler tek bir plan içerisinde tutulamaz hale gelebilir. Bu durumda bilgileri bölerek birden fazla kablolama planı oluşturmak daha yararlı olacaktır. Gerçek konum bilgileri daima ölçekli planlarla çizilmelidir. Diğer bilgiler tablolar veya şematik planlar halinde saklanabilir. Tüm bilgilerin açık ve net olarak, gerektiğinde erişilebilecek şekilde organize edilmesi önemlidir. Dolayısıyla dokümantasyon içerisinde tanımlayıcı belgeler, listeler ve planlar bulunmalıdır.

Tanımlayıcı belgeler (örneğin dokümantasyon rehberi, dokümantasyon yönetimi politikası, vb.) içerisinde; dokümantasyon yönetimi için kullanılan prosedürler, tanımlama ve

etiketleme kuralları gibi bilgiler bulunur. Bu belgeler arasında örneğin, hangi durumlarda ne tür liste ve planların oluşturulması gerektiği, oluşturulan dokümanların denetime uygun bir biçimde nasıl yönetilmesi gerektiği açık ve net bir biçimde tarif edilmelidir.

Oluşturulan listeler ve planlar, kablolama için önemli tüm unsurlara ilişkin bilgileri içermelidir. Bu bilgiler arasında:

- Tedarikçi, teslimat ve bileşen bilgileri,
- Kullanılan kablo türleri (fiber optik kablo türü ve kalitesi vs.),
- Kullanıma yönelik kablo etiketleme,
- Ana ve tali ağ dağıtım panolarının konum bilgileri,
- Kullanılan tesisatlar ve onlara bağlı bileşenlerin bilgileri,
- Bağlantı noktalarının teknik verileri,
- Tehlikeli noktalar,
- Mevcut ve test edilmesi gereken koruyucu önlemler gibi birçok detay bulunabilir.

Ayrıca envanter planları içerisinde:

- Yerleşke ve kablo taşıma kanallarının boyutlandırılmış saha planları,
- Bina bölümlerinin şematik planları, tam konuma sahip boyutlandırılmış kat planları, dağıtım panolarının konumları, odalarda bulunan ağ bağlantı soketleri, vb.,
- Teknik oda planları, yükseltilmiş zemin planları, sunucu kabinlerinin pozisyonları, bina elektrik iletim planları ve klima sistemleri,
- Ağlara ilişkin fiziksel ve mantıksal bağlantı diyagramları bulunur.

Hazırlanan dokümantasyon aracılığı ile kablolamaya ilişkin genel resim hızlı ve kolay şekilde elde edilebilmelidir.

Dokümantasyonun güncelliğinin sağlanması amacı ile kablolama ile ilgili tüm çalışmalar, dokümantasyon yönetiminden sorumlu kişilere zamanında bildirilmeli, bu kişilerin gerekli değişiklikleri dokümanlara yansıtması sağlanmalıdır.

Dokümantasyonlar hassas (ve kimi zaman kritik) bilgiler içerdiğinden, güvenli bir şekilde saklanması ve dokümanlara erişimin kontrol altında tutulması gerekir.

Hazırlanan dokümantasyona uygun bir biçimde, kullanılan kablolar (her iki uçlarından) etiketlenmelidir. Bu amaçla özel etiketler kullanılmalı, silinmeyen kalemler ile kablolar işaretlenmelidir. İhtiyaç halinde farklı renklerde kablolar kullanılarak, kablo taşıma yolları boyunca kabloların izlenilebilirliği kolaylaştırılabilir. Malzemeye bağlı olarak kabloların etiketlenmesinde değişik yazıcılar kullanılabilir. Kablo kalemleri (marker, vb.) ile etiketleme genellikle yeterli ve sağlıklı olmamaktadır. Kablo uzunluğuna bağlı olarak, kablo uçları dışında belirli aralıklarla etiketleme yapılması da düşünülebilir. Kabloların etiketlenmesi

sırasında, kablonun kritikliğini, önemini belirten kısaltmalardan ve renklerden kaçınılması, sadece kablo tanımlama bilgisine yer verilmesi önerilmektedir.

BT kablolarının yenilenmesi veya modernizasyonu planlanıyorsa, kablolamaya ilişkin dokümantasyon yönetimi konusunda, kurum ve işi üstlenecek yükleniciler (ağ planlayıcıları, tedarikçileri ve kurulum teknisyenleri) anlaşmalıdır. Kurum, devreye alma işlemi çalışmalarının başında, iç ve dış kablolama dokümantasyonuna sahip olmalıdır.

İç dokümantasyon, BT kablolarının kurulumu ve işletilmesi ile ilgili tüm kayıtları ve çizimleri kapsar. Bu dokümanlar, işletim ve gelişim unsurlarını en iyi şekilde destekleyecek biçimde hazırlanmalı ve muhafaza edilmelidir.

Dış dokümantasyon ise gerekli işletim desteğini sağlayabilmek için bağlantıların etiketlenmesini içerir. Sabotaj ve diğer kötü niyetli tehlikelere karşı, kabloların dışarıdan görülebilen alanlarında (örneğin, elektrik prizleri ve kablo uçlarının etiketlenmesi, insan geçiş alanları) etiketlemenin mümkün olduğunca az tutulması önerilir. Burada amaç, potansiyel bir saldırgana mümkün olduğunca az ipucu vermek, aynı zamanda BT personeline doğru ve izlenebilir ağ için gerekli işaretleri sağlamaktır.

Orta ve geniş kapsamlı kablolama projeleri, uygun dokümantasyon yazılımının kullanılmasını gerektirir. Bu nedenle planlama aşamasında, doküman yönetimi için kullanılacak program ve sürümü, dosya formatları, vb. özellikler belirlenmeli, projede çalışacak yüklenicilere (ve ilgili tüm taraflara) gerekli bilgilendirmeler yapılmalıdır. Dosya adı ve dosya içerisinde kullanılacak tüm bileşenler için geçerli olacak isimlendirme kuralları oluşturulmalı, dosya sürümünün dosya adında görülebilmesi sağlanmalıdır (örneğin dosya adı, dosyanın oluşturulduğu tarih ile başlayabilir).

Benzer şekilde kullanılacak etiketler ve işaretler için de isimlendirme kuralları belirlenmelidir. Örneğin, yönlendirilen farklı sınıf bakır kabloların çizimlerde nasıl ayırt edileceği konusu netleştirilmelidir (örnek: Hat 123 - bakır = H123-ba6a , CAT 6a).

Ortaya çıkan sorunlardan biri, bina odalarının ve bölümlerinin numaralandırılması ile ilgilidir. Mimarlar genellikle numaralandırmayı planlama aşamasında belirlemekte ve tasarım sırasında belirlenen bu numaralar, BT kablolarının planlaması ve işletiminde de kullanılmaktadır. Binayı kullanacak kurumun çeşitli nedenlerle tasarlanandan farklı bir numaralandırma sistemini kullanmayı tercih etmesi durumunda, bu yeni durum işletim sırasında tutarsızlıklara, karışıklıklara, işletimin bozulmasına ve hatta çeşitli güvenlik sorunlarının meydana gelmesine neden olabilir. Örneğin, oda numaralamasındaki bu tür tutarsızlıklar, yanlış odalar arasında ve dolayısıyla yanlış BT bileşenleri arasında kablo bağlantıları yapılmasına neden olabilir.

BT kablolamaya ilişkin ilk olarak planlama ve kurulum dokümanları oluşturulmalıdır. Öncelikle planlanan ağ topolojisi yazılı hale getirilmeli, kablo ve kablo kanal güzergahları, ağ bağlantı noktaları, bina ve oda planlarına eklenmelidir. Daha sonra kurulumu icra edecek kişilerden (yüklenici), gerçekleştirilecek kablolama çalışmasının detaylarını içeren gerekli dokümanların hazırlanması beklenir.

BT kablolama dokümantasyonu aşağıdakilerden oluşur:

- Bina bölümlerindeki kablo kanal ve tava güzergahları ve kullanımı,
- Her bir katta bulunan ağ bağlantı noktaları, kablo kanal ve tava güzergahları,
- Veri merkez ve sistem odası gibi BT bileşenlerini barındıran tüm odalara ilişkin oda planları (kabin yerleşimleri ve bağlantı kurulacak dış ağların giriş noktaları ile birlikte),
- Kabin (içinde kurulu sunucular) ve kullanılacak ek ve bağlantı kablolarına ilişkin tahmini genişleme/büyüme planı,
- Yürütme ile ilgili uygunluk belgeleri,
- Tedarikçi ve teslimat bilgileri, ölçüm kayıtları ve kabul testleri.

BT kablolama dokümantasyonun, kurumun gerçekleştirilen işi kabul etmesi için temel ve önemli bir parça olması sağlanmalıdır.

BT ağının ve kablolama altyapısının işletilmesi sırasında, mevcut durum için bir doküman tutulması ve ayrıca gerçekleştirilecek güncelleme çalışmaları için ayrı doküman oluşturulması önerilmektedir. Bilgisayar destekli tasarım yazılımları (CAD) ile oluşturulan bina/oda planları genellikle kurulum/yapım aşamaları sırasında kullanılacak dokümanlar olarak görülebilir.

İşletim sırasında, bina/oda planlarında bulunan yapısal unsurlar yerine, BT ağına ilişkin mantıksal ve BT'ye özgü bilgileri içeren dokümanlar daha kullanışlı olacaktır. Bu amaçla CAD yazılımları yerine "BT'ye yakın" yazılım uygulamaları seçilmeli, BT kablolama işletiminde görev alacak çalışanların bu tür uygulamalardan destek almaları sağlanmalıdır.

Dokümanların planlama aşamasından itibaren bir yazılım yardımıyla oluşturulmaya başlanması, işletim aşamasında da aynı yazılım aracılığı ile doküman yönetiminin devam etmesi önerilmektedir. Bu şekilde aynı doküman üzerinde gerektiğinde birden fazla kişinin çalışabilmesini sağlamak, dokümanlar üzerinde değişiklikleri takip etmek, dokümanları güncel tutmak daha pratik olabilecektir.

VRM.4.U9 Mevcut bağlantıların kontrolü

BT kablolama altyapısının ilk montajı ve kabulü sonrası düzenli aralıklarla, kullanılan tüm kablo kanalları, dağıtım panoları ve kablo çıkışları (en azından örnekleme yoluyla belirli örnekler seçilerek) görsel denetime tabi tutulmalıdır.

Görsel denetim sırasında:

- Kilitli dağıtım panolarında izinsiz açma girişimlerinin tespiti,
- Pano belgelerinin güncelliği,
- Kablolamanın dokümanlara uyumluluğu (gerçekleştirilen çalışmaların dokümanlarda ki güncelliği),
- Gereksiz hatların topraklanması,
- İzinsiz değişiklikler

gibi hususlar dikkate alınmalıdır.

Görsel denetime ek olarak düzenli aralıklarla ve sertifika sahibi bir uzman tarafından, fonksiyonel bir kontrolün ayrıca gerçekleştirilmesi de önerilmektedir. Kontrolü gerçekleştiren uzman, kurulumları ve tesisatın çalıştırılmasını denetlemeli, ayrıca test ölçümleri yapmalıdır. Çalışma sırasında,

- Tüm BT kablolama altyapısının belirlenen teknik özelliklere göre kurulup işletildiği,
- Yangın bariyerlerinin doğru kurulduğu,
- İletim hatlarının mevcut taşıma kapasitesi ve planlamaya uygunluğu,
- BT kablolama dokümantasyonunun doğru ve güncel olduğu,
- Tüm ağ bağlantılarının düzgün şekilde bağlandığı

kontrol edilmelidir. Özellikle nadir kullanılan ve kötü niyetli kullanımların hemen ortaya çıkarılamayacağı bağlantılar ile hassas bilgilerin iletildiği bağlantılar için kontrollerin daha sık aralıklarla gerçekleştirilmesi düşünülmelidir.

Görsel veya işlevsel kontroller sırasında saptanan usulsüzlükler derhal kayıt altına alınmalı ve gerekli diğer adımların zamanında alınabilmesi için ilgili birimlere raporlanmalıdır. Bulunan düzensizliklerin ortadan kaldırılmasının yanı sıra nedenlerinin tespit edilmesi de önemlidir. Ayrıca gerçekleştirilen tüm kontrollerin sonuçları, ölçüm sonuçları ile birlikte test raporları olarak kayıt altına alınmalı ve uygun bir şekilde saklanmalıdır.

2.3 3.SEVİYE UYGULAMALAR

1. ve 2. seviye uygulamalar sonrasında, BT kablolama altyapıları için artan koruma koşullarında dikkate alınması gereken uygulamalar aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun uygulamalardan

faydalanmaları önerilir. Uygulama kapsamında öncelikli koruma sağlanan prensip parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

VRM.4.U10 Ağ yedekliliği (E)

Çoğu zaman kampüs içerisinde birden fazla binaya dağılmış kurumlarda, yıldız topolojisine uygun biçimde, binaların veri merkezine bağlandığı gözlenir. Veri merkezine bağlı bulunan kritik binaların kesintisiz olarak ağ hizmetlerinden yararlanabilmesi için, farklı kablo kanalları kullanılarak yedekli kablolama gerekliliği incelenmelidir.

Ayrıca, BT veya telekomünikasyon sağlayıcılarıyla olan bağlantıların yedekli tasarlanıp tasarlanmadığı da kontrol edilmelidir. Gerçek bir yedeklilik için, kablo yollarının farklı noktalardan sağlayıcının ağına bağlantı oluşturulması sağlanmalıdır.

BT kablolamanın yedeklenmesi veya sağlayıcılar ile yapılan bağlantıların yedekli olup olmayacağı, kurumun erişilebilirlik gereksinimlerine bağlıdır.

Tam yedekli işletim (Paralel İşletim)

Veri merkezi ve/veya sistem odalarında, uygun aktif ağ bileşenlerinin kullanımı ile yedekli hatların aynı anda paralel olarak çalışması sağlanabilir. Bu sayede yedeklilik ile birlikte kapasite de artırılmış olur. Arıza nedeni ile hatlardan birinin çalışmaması durumunda, diğer hat üzerinden iletim devam eder fakat bu durumda iletim kapasitesinin düşeceği de unutulmamalıdır. Düşük kapasite miktarı, acil duruma hazırlık kapsamında dikkate alınmalıdır.

Kısmı yedekli işletim (Aktif/Pasif İşletim)

Kullanılan teknoloji veya kablolama yoluyla uygulanan hizmetler tam yedekli işletime (paralel işletim) izin vermiyor ise, kullanılan (aktif) hattaki arıza durumunda yedekte bekleyen (pasif) hat devreye alınarak iletim devamlılığı sağlanır. Bu geçiş (devreye alma işlemi) otomatik veya manuel gerçekleşebilir.

Paralel işletimin mümkün olmadığı ve kısmi yedekli işletimin kullanıldığı ağlarda, fiili bir arıza olmasa bile yedek (pasif) hatlar belirli aralıklar ile aktif hale getirilmelidir. Bu şekilde kısmi yedekleme işlevi düzenli olarak test edilmiş olur. Kontrol aralıkları, erişilebilirlik gereksinimleri doğrultusunda belirlenmelidir.

İzleme

İletişim hatlarındaki yedekli yapı, ancak (işlevsellik açısından) izlenir ve denetlenirse, erişilebilirlik seviyesini etkili bir şekilde artırabilir. İzleme ile arızaların, darboğazların ve diğer düzensizliklerin erken bir aşamada tespit edilerek, sorunların hızlıca giderilmesi

(mümkünse ortaya çıkmadan önlenmesi) amaçlanır. Yetersiz izleme ile hat arızalarının tespit edilememe riski artar, yedeklilik görünürde kalabilir, istenen erişilebilirlik seviyesi sağlanamayabilir.

Yüksek erişilebilirlik seviye gereksinimleri söz konusu olduğunda, ilgili binalarda ve/veya veri merkezlerinde ikincil ve üçüncül kablolamanın fazladan olarak tasarlanması düşünülmelidir.

VRM.4.U11 BT kablolamanın fiziksel güvenliği (E)

Ziyaretçilerin kullandığı odalarda veya binanın izlenemeyen alanlarında yer alan kabloların (kablo kanalları) ve dağıtım panolarının yetkisiz erişime karşı korunması sağlanmalıdır. Korunma için çeşitli yöntemlerden yararlanılabilir:

- Kabloların veya kablo kanallarının sıva altına döşenmesi,
- Kabloların zırhlı borular içinden geçirilmesi,
- Kabloların mekanik olarak güçlü ve kilitlenebilir kanallara döşenmesi,
- Panoların kilitlenmesi,
- Kablo kanallarının ve panoların izlenmesi.

Prensip olarak kabloların yetkisiz kişilerin erişebileceği yerlerden geçirilmemesi ve korunması gerekli kablo uzunluğunun mümkün olduğunca kısa tutulması önerilir. Kabloların mümkün olduğunca görünmeyecek biçimde (örneğin sıva altına, yükseltilmiş zemin altına, vb.) kablo kanalları veya kablo tavaları ile döşenmesi sağlanmalıdır. Kablolar ancak insan geçişleri ve diğer türlü hasar verebilecek sebepler ortadan kaldırıldığı takdirde açık bırakılmalıdır.

Kablo güvenliğinin sağlanabilmesi için kablo kanal güzergâhı boyunca, karşılaşılabilecek tehdit unsurları da göz önünde bulundurulmalı ve alınması gereken önlemler planlanmalıdır. Koridor veya yeraltı otoparkı gibi ulaşım yolları olarak kullanılan alanlarda yer alan kablolar, kazara meydana gelebilecek mekanik hasarlara, gerekli durumlarda sabotaja karşı korunacak şekilde sağlam bir biçimde kapatılmalıdır.

Kilitli tutulan dağıtım panolarına ve kablo kanallarına ilişkin anahtarların dağıtımını, kullanımını ve (panolara, kanallara) erişim yöntemlerini belirleyen düzenlemelerin oluşturulması gereklidir. Ayrıca kablolar, kablo kanalları veya panolarda yapılacak değişikliklerin nasıl yönetileceği, değişiklik öncesinde ve sonrasında nelere dikkat edileceği belirlenmelidir. Değişikliklerin koordine edilmesi, yetkili kişiler tarafından onaylanması ve kayıt altına alınması (ilgili diğer dokümanların güncellenmesi) sağlanmalıdır.

VRM.4.12 Korumalı (shielded) kablo kullanımı ile elektromanyetik alandan korunma

BT altyapısı için standartlar (TS EN 50173, TS EN 50174-2) hem korumalı, hem de korumasız veri kablolarını, bu sistemler için topraklama ve koruma gereksinimlerini tanımlamaktadır. Korumalı kablo kullanımına ilişkin BT bileşenlerinin barındırıldığı odalar (örneğin Sistem odaları ve veri merkezleri) ile genel BT kullanımı olan odalar arasındaki standartlarda farklılıklar bulunmaktadır. BT bileşenlerinin barındırıldığı odalar için, korumanın kablonun her iki ucunda uygulanması, sistemlerin ve bileşenlerin sıkıca birbirine geçirilmesi önerilmektedir. Binalarda genel kullanım için oluşturulan kat kablolamaları gibi uygulamalarda, standartlar korumanın kablonun tek ucuna uygulanmasını şart koşmaktadır (çift taraflı seçeneğe/mimariye bağlı).

Elektromanyetik alan nedeniyle oluşan parazitler, elektromanyetik girişim (EMI – Electromagnetic Interference) olarak da adlandırılır. Korumalı kablo kullanılmasına rağmen elektromanyetik girişim oluşuyor ve kablodan iletilen sinyallerin bozulmasına neden oluyor ise, öncelikle elektromanyetik girişimin oluşum sebepleri analiz edilmelidir. BT iletim yöntemlerinde kullanılan frekansların gittikçe artmasından dolayı, sistemler yüksek frekanslı girişimlere (parazitlenmeye) karşı oldukça hassas hale gelmektedir. Buna ek olarak, belirli koşullar altında, BT bileşenlerinin kendileri, bir elektromanyetik alan kaynağı haline gelerek, kendilerini çevreleyen sistemler için yüksek frekanslı elektromanyetik girişimlerin oluşmasına neden olabilirler. Çok farklı nedenlerden dolayı oluşabilecek bu tür arızalara karşı doğru çözümün üretilmesi uzmanlık gerektirir. Bu nedenle, bu durumu değerlendirmek ve analiz etmek, çözüm bulmak ve sonuçlandırmak için uzman bir şirket ile birlikte çalışılması önerilir.

Binalar ve veri merkezleri kablolama hatlarını, korumalı kablo kullanımı ile elektromanyetik alandan koruma TT, TN veya TN-C, TN-CS sistemleri ile sağlayabilmektedir.

VRM.4.13 Kabin sistemlerinin kullanımı (BE)

Özellikle bilgi işlem merkezleri ve sistem odalarında kabin sistemleri; veri depolanan, işlenen ya da iletişimi sağlayan BT donanımlarının (sunucu, aktif ve pasif ağ bileşenleri, depolama birimleri, vb.) organize bir şekilde yerleştirilmesini sağlayan ve onları dış etmenlere karşı koruyan yapılardır. Genellikle içerisinde yer alacak donanımların türüne bağlı olarak farklı biçimlerde (örneğin 19 inç rack kabin, sunucu kabini, ağ kabini, vb.) tanımlanırlar.

Kabin sistemleri, IEC 60297 ve DIN 41494 standartlarına göre üretilir. Standartlara uygun kabinlerin kullanılması, herhangi bir üretici firma tarafından üretilen donanımın (standartlar ile uyumlu olduğu takdirde) kabine kolaylıkla monte edilmesini sağlayacaktır. Yukarıda

belirtilen standartlarda, kabin sistemlerinin genişliği 19 inç (yaklaşık 48.3 cm) olarak belirlenmiştir. Standartlara uygun BT donanımları için “19 inç kurulum” tabiri kullanılır.

Genişlik olarak 19 inç standart olarak kabul edilse de, farklı uzunluklarda ve derinliklerde kabin sistemleri bulunmaktadır. BT ve ağ bileşenleri için genellikle 42U yüksekliğe sahip kabinler tercih edilir. Kabin sistemlerinde yükseklik birimi olarak U (rack unit – yaklaşık 44,45 mm.) kullanılır. Kabin içerisine yerleştirilebilecek her bir BT donanımının (bileşen) U cinsinden yüksekliğinin bilinmesi gereklidir. Kabin sistemlerinin sadece yetkili kişilerin erişimine izin verilen sistem odalarına veya genel olarak erişilebilir alanlara kurulup kurulmadığına bağlı olarak, koruma gereksinimlerini karşılayan kapıları, yan kapakları ve kilitleri bulunmalıdır. Kabinlerin altında bulunan ayaklar, kullanılacak kabloların kabin içerisine yerleştirilmesini kolaylaştırır. Ayrıca kabin ayakları, kabin ile oda zemini arasında mesafe oluşturduğundan, olası küçük boyutlu su baskınlarının kabin içerisinde yer alan BT donanımlarını etkilememesine yardımcı olur.

Bakım/onarım açısından kabin iç tasarımı son derece önemlidir. Örneğin, kabin içerisinde yer alan bir bileşenin, komşu bileşenler olumsuz bir şekilde etkilemeden hızlıca değiştirilmesi mümkün olmalıdır. Kabin içerisine bileşenlerin düzgün bir biçimde yerleştirilmelerinin yanı sıra uygun bir (patch) kablo yönetiminin de sağlanması gerekmektedir. Elektrik ve BT kablolarının kabin içi bileşenlere, gerekli korumalar ile yönlendirilmeleri sağlanmalıdır. Aşırı uzun kablo kullanımından kaçınılmalı, etiketlemelere dikkat edilmelidir. Pek çok kabin sistemi üreticisi, kabin içi kablolama yönlendirmelerini, kurumların özel isteklerine ve gereksinimlerine uygun olarak sunmaktadır. Kabinler arası kablolamanın da ayrıca planlanması gerekir.

Kabin içerisine monte edilecek bileşenlerin planlanması aşamasında, bileşenlerin fiziksel alanlarının (genellikle yükseklikleri) yanı sıra, işletim sırasında kabin içerisinde yer alan bileşenler tarafından üretilecek ısı miktarının da göz önünde bulundurulması gereklidir. Kabine monte edilen BT bileşenlerinin sıcaklık yüklerinin yüksek olması durumunda, kabin içerisinde ısı yayılımı (heat dissipation) problemleri ortaya çıkabilmektedir.

Benzer sorunlar çok sayıda pasif bileşen içeren ağ kabinlerine, fazla sayıda kablo takıldığında ortaya çıkabilir. Böyle bir durumda, kabin içerisindeki havanın akışı bozulabilir ve bileşenlerde arızalar meydana gelebilir. Kabin içerisine kurulacak bileşenler planlanırken, kabinde yer alacak kablo miktarı da dikkate alınmalıdır.

Birbirine yakın (bitişik veya arkalı/önlü) konumlandırılan kabinlerde, kabin içerisinde yer alan bileşenlerin oluşturduğu hava akışı da kontrol edilmelidir. Bileşenlerden çıkan sıcak havanın bitişik bir bileşenin soğuk hava tedarikini etkilemesini önlemek önemlidir. Bu nedenle özellikle kabin içerisinde kullanılmayan rafların kapalı tutulması sağlanmalıdır.

Kabin içerisine yerleştirilmiş bileşenlerin öngörülen sıcaklık aralıklarında çalıştırılmalarını sağlamak için kabinlerin uygun şekilde donatılmış ve yerleştirilmiş olması gerekir. Veri merkezi ve/veya sistem odasının yeterince soğuk olması, çoğu zaman kabinlerin pasif soğutması için yeterlidir. Bunu destekleyecek şekilde kabin içerisine fan sistemleri yerleştirilebilir. Oda sıcaklığının çok yüksek olması veya hızla yükselmesi durumunda, farklı tipte aktif soğutma sistemleri kullanılabilir. Oda soğutma sistemleri ve kabinin üstüne/yanına/altına monte edilen soğutma sistemleri aktif soğutma sistemleri olarak sıralanabilir.

Çok fazla miktarda ısı üreten BT bileşenleri için, bağımsız iklimlendirme sistemlerine sahip özel kabin sistemlerinin kullanılması düşünülmelidir. Genellikle dâhili sıvı soğutmalı bu tür kabinler, etraflı bir ihtiyaç ve risk analizi sonrası kullanılmalıdır. Kullanılması düşünülen her tür iklimlendirme sistemine ilişkin, ilgili maliyet analizi de dâhil olmak üzere tüm parametreler dikkate alınarak, planlama yapılmalıdır.

Kurum içerisinde kullanılacak kabin sistemlerine ilişkin özelliklerin belirlenmesi ve bu özelliklere uygun tek tip kabinlerin seçilmesi önerilmektedir. Bu sistemlerin kullanımı ve yönetimi için gerekli yönergeler hazırlanmalı ve ilgili kişiler ile paylaşılmalıdır.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

BT kablolama ile ilgili detaylı konulara aşağıdaki referans ve kaynaklardan ulaşılabilir:

- [EN50173] EN 50173:2007
- [EN50174] EN 50174:2009
- [EN50310] EN 50310:2017-02
- [EN50346] EN 50346:2010-02
- [IEC60364] IEC60364
- [IEEE8023] IEEE8023
- [ISO11801] ISO/IEC 11801:2002-09
- [VDE100] DIN VDE 0100

EKLER

EK-A: KONTROL SORULARI

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U1	Bina güvenliği planlaması	• Bina için bir güvenlik kavramı/planı oluşturuldu mu? • Tüm girişler, korunan alanlara yetkisiz kişilerin erişemeyeceği şekilde kontrol ediliyor mu?
Genel Bina	VRM.1.U2	Elektrik yük dağılımının ayarlanması/yapılandırılması	• Elektrik tesisatının ve yük kapasitesinin güncel gereksinimlerini karşıladıkları, düzenli olarak gözden geçiriliyor mu? • Elektrik tesisatının farklı fazları üzerinde yükün dengeli olup olmadığı izleniyor mu? • Yüksek erişilebilirlik kapsamında BT, iki bağımsız enerji hattı üzerinden besleniyor mu?
Genel Bina	VRM.1.U3	Yangın güvenliği yönetmeliklerine uyulması	• Kurumun kendine ait yangın koruma prosedürleri var mı? • Prosedürlerin uygulanması düzenli olarak denetleniyor mu? • Yangın güvenliği görevlisi (acil durum sorumlusu) veya bu konuda eğitim alan çalışanlar var mı? • Acil çıkış ve kaçış yolları düzgün bir şekilde işaretlenip açık tutuluyor mu? • Binadaki yangın yüklerinin varlığı düzenli şekilde kontrol ediliyor mu? • Gereksiz yangın yükleri ortadan kaldırılıyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U4	Binalarda yangın algılama	• Yangın algılama ve yangın durumunda zamanında uyarı yapılmasına yönelik önlemler nelerdir? • Binada yeterli duman dedektörü var mı? • Duman dedektörlerinin ve yangın alarm sistemini oluşturan cihazların işlevselliği düzenli olarak kontrol ediliyor mu?
Genel Bina	VRM.1.U5	Taşınabilir yangın söndürücüler	• Yangın durumunda, taşınabilir yangın söndürücülere kolayca erişilebiliyor mu? • Taşınabilir yangın söndürücüler düzenli olarak kontrol ediliyor ve denetleniyor mu? • Çalışanlara taşınabilir yangın söndürücülerinin kullanımı konusunda eğitim/talimat veriliyor mu?
Genel Bina	VRM.1.U6	Kapalı pencereler ve kapılar	• Dışa bakan pencere ve kapıların kilitlenmesi gerektiğini gösteren talimatlar varmı? • Mesai sonrası ve herkes odadan ayrıldıktan sonra, dışa bakan pencere ve kapıların kilitli olup olmadığı ile ilgili bir kontrol yapılıyor mu? • Yangın korumalı kapıların kapalı tutulduğu kontrol ediliyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U7	Güvenlik ve Erişim Kontrolü	• Binanın koruma gerektiren alanlarında erişim kontrol sistemleri uygulanıyor mu? • Tutarlı bir şekilde uygulanan bir erişim kontrol prosedürü bulunuyor mu? • Erişim kontrol önlemleri düzenli olarak denetleniyor mu?
Genel Bina	VRM.1.U8	Binanın fiziksel güvenlik çerçevesi	• Bina kullanımı için iş süreçlerine uygun koruma gereksinimleri belirlendi mi? • Kurum faaliyetlerinden kaynaklanan temel koruma hedefleri tanımlandı mı?
			• Binanın kullanımındaki değişiklikler konsepte yansıtılıyor mu?
Genel Bina	VRM.1.U9	Uygulanabilir standartlara ve düzenlemelere uyum	• Binanın planlanması, inşası, yenilenmesi ve teknik ekipmanların kurulumunda dikkate alınan standartlar ve düzenlemeler nelerdir?
Genel Bina	VRM.1.U10	Kapıların kilitlenmesi	• Mesai sonrası ve herkes odadan ayrıldıktan sonra, kapıların kilitli olup olmadığı ile ilgili bir kontrol yapılıyor mu? • Çalışanlardan, ofis odalarından çıktıklarında bu alanları kilitlemeleri ve kurumsal bilgi içeren belgeleri güvenli hale getirmeleri isteniyor mu?
Genel Bina	VRM.1.U11	Anahtar/kilit yönetimi	• Anahtarlar kullanılmadığı zamanlarda, güvenli bir şekilde saklanıyor mu? • Verilen her anahtar belgelere kayıt olarak düşülüyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U12	Dağıtım panolarına erişimle ilgili düzenlemeler	• Binanın tüm dağıtım panolarına (elektrik, su, gaz, telefon, alarm sistemi vb.) erişimler düzenlenmiş midir? • Dağıtım panoları içerisinde etiketleme kullanılıyor mu?
Genel Bina	VRM.1.U13	Yıldırımdan korunma cihazları	• Standartlara uygun yıldırımdan korunma sistemi var mı? • Yoğun BT donanımının bulunduğu binaların, cihazları en az koruma sınıfı II'ye uygun mu? • Yıldırımdan korunma sistemi düzenli olarak kontrol ediliyor mu?
Genel Bina	VRM.1.U14	Altyapı tesisat hatlarının yerleşim planları	• Tüm tesisat hatlarının yerleşim planları mevcut mu? • Bu planların oluşturulması ve yönetiminden kimlerin sorumlu olduğu belirlendi mi? • Bu planlara kimlerin erişilebileceği belirlendi mi?
Genel Bina	VRM.1.U15	Korunma gerektiren bina bölümlerine ilişkin konum/tabela bilgilendirilmelerinden kaçınma	• Korunması gereken alanlara ilişkin konum/tabela bilgilendirilmelerinden kaçınılıyor mu? • Bu alanların dışarıdan kolaylıkla görünmemesi için gerekli önlemler alındı mı?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U16	Dumandan Koruma	• Bina içerisinde dumandan koruma için gerekli önlemler alınıyor mu? • Duman koruma bileşenlerinin düzgün çalıştıkları düzenli olarak test ediliyor mu? Yapısal duman koruması, kurulum ve yenileme çalışmalarından hemen sonra kontrol ediliyor mu?
Genel Bina	VRM.1.U17	Yangın güvenlik kontrolleri	• Yangın önleme kontrolleri düzenli olarak gerçekleştiriliyor mu? • Tespit edilen eksikliklerin giderilmesi planlanıp, uygulanıyor mu?
Genel Bina	VRM.1.U18	Acil durum sorumlusunun zamanında bilgilendirilmesi	• Yangın güvenlik görevlilerine; tesisat güzergâhları, kat koridorları, kaçış ve kurtarma güzergâhları üzerinde gerçekleştirilecek çalışmalara ilişkin detaylı bilgi çalışma öncesi aktarılıyor mu? • Yangın güvenlik görevlilerinin bu çalışmalara dahil edilmesi ile ilgili bir talimat var mı?
Genel Bina	VRM.1.U19	Acil durum planı ve yangın tatbikatları	• Yazılı bir acil durum planı var mı? • Düzenli aralıklarla yangın tatbikatları gerçekleştiriliyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U20	Bağımsız elektrik hatları üzerinden beslenme	• Yüksek erişilebilirlik kapsamında, bina içerisinde bulunan kritik BT bileşenleri iki farklı güç kaynağı üzerinden besleniyor mu? • Kritik BT bileşenlerinin güç kaynağı bağlantılarının doğru çalışıp çalışmadığı, düzenli aralıklar ile kontrol ediliyor mu?
Genel Bina	VRM.1.U21	Güvenli Kapılar ve Pencereler	• Kritik alanların kapıları ve pencereleri, hırsızlığa, yangına ve dumana karşı güvenli hale getirildi mi? • Güvenli kapılar ve pencereler, işlevsellikleri bakımından kontrol ediliyor mu?
Genel Bina	VRM.1.U22	Güvenlik bölgelerinin oluşturulması	• Bina ve yerleşke için bir güvenlik bölgesi modeli geliştirilip, dokümante edildi mi?
Genel Bina	VRM.1.U23	Otomatik drenaj	• Su sızıntısı veya tehlikesi barındıran tüm alanlar, otomatik drenaj (tahliye sistemleri) ile güvenli hale getirildi mi? • Aktif /pasif su drenaj sistemlerinin çalışması düzenli olarak kontrol ediliyor mu?
Genel Bina	VRM.1.U24	Uygun yer seçimi	• Binayı tehdit edebilecek çevresel tehlikelere karşı genel bir plan/yaklaşım oluşturuldu mu? • Bu tehlikelere karşı ne tür önlemler uygulanıyor?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U25	Güvenlik görevlileri ve bina güvenlik hizmeti	• Güvenlik hizmetinin görevleri net ve yazılı bir şekilde tanımlandı mı? • Ziyaretçi veya çalışanlara, binaya girişlerde ne tür geçiş kontrolleri uygulanıyor? • Çalışanlar veya güvenlik görevlileri ziyaretçilere eşlik ediyor mu?
Genel Bina	VRM.1.U26	Hırsızlığa Karşı Koruma	• Bina içerisinde hırsızlığa ve saldırıya karşı hangi önlemler uygulanıyor? • Hırsızlığa karşı korunma için oluşturulan planlama, uygulama ve operasyon adımları, yetkili bir kişi tarafından düzenli olarak değerlendiriliyor mu? • Çalışanlar, hırsızlığa karşı korunma düzenlemeleri hakkında bilgilendiriliyor mu?
Genel Bina	VRM.1.U27	İklimlendirme (Klima) Sistemleri	• İklimlendirme sistemleri binanın kullanım amacına göre tasarlandı mı? • Klimanın bakımı, temizliği ve özellikle hava filtrelerinin belirli aralıklar ile değişimleri kontrol ediliyor mu? • İklimlendirme sistemleri herkesin erişimine açık mıdır?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U28	Bina temizliği için prosedürler	• Temizlik firma çalışanlarının, sözleşmede belirtilen şekilde kendilerine verilen kimlik ve kimlik kartlarını kullanıp kullanmadıkları kontrol ediliyor mu? • Temizlik personeli görevini yaparken, BT donanımına nasıl davranacağı konusunda talimatlar oluşturuldu mu, uygulanıyor mu? • Temizlik personeli, özellikle hassas alanlarda çalışırken kontrol ediliyor mu?
Genel Bina	VRM.1.U29	Uygun bina seçimi	• Bina seçiminde, binanın kullanıma uygunluğu değerlendiriliyor mu? • Binanın mevcut tehlikeleri belirleniyor mu? • Bu tehlikelere karşı önlemler yazılı belge haline getiriliyor mu?
Genel Bina	VRM.1.U30	Bina tahliyesi	• Yakın zamanda taşınma gerçekleştirildi mi? • Taşınma öncesi, taşınacak ekipmanlara ilişkin bir envanter oluşturuldu mu? • Taşınma sonrası, eksik envanter çalışması yapıldı mı?
Genel Bina	VRM.1.U31	Korunması gereken alanların düzenlenmesi	• Bina içerisinde korunması gereken alanlar, güvenli hale getiriliyor mu? • Güvenli hale getirilemeyen ve riskli alanlar, güvenlik süreçlerinde kayıt altına alınıyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Genel Bina	VRM.1.U32	İkaz ve Alarm Sistemi	• Bina için herhangi bir alarm sistemi kuruldu mu? • Alarm sistemi düzenli olarak kontrol ediliyor mu? • Alarm mesajlarına verilecek tepkiler belirlenip, roller ve sorumluluklar tanımlandı mı?
Veri Merkezi	VRM.2.U1	İhtiyaçların Tanımlanması	• Veri merkezinin teknik ve kurumsal gereksinimleri, kurum bünyesinde tanımlanıyor mı? • Bu gereksinimlerin belirlenmesi sırasında veri merkezi erişilebilirlik seviyeleri, olası çevresel tehlikeler, iç ve dış unsurlar dikkate alındı mı?
Veri Merkezi	VRM.2.U2	Yangın bölgelerinin oluşturulması	• Veri merkezini oluşturan alanlar, uygun bir şekilde yangın bölgelerine ayrılıyor mu? • Yangın duvarları ve yangın bölmeleri; binanın ve envanterin korunması için koruma hedeflerini yerine getiriyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U3	Kesintisiz güç kaynağı (UPS) kullanımı	• Veri merkezinde UPS kullanılıyor mu? • Akülerin gerekli sıcaklık aralığında tutulması sağlanıyor mu? • UPS'nin bakım aralıklarına uyuluyor mu? • Akülerin gerçek kapasitesi ve UPS'lerin yedekleme süresi düzenli olarak test ediliyor mu? • BT altyapı ve bileşenlerinde değişiklik yapıldığında besleme süresinin yeterli olup olmadığı tekrar kontrol ediliyor mu?
Veri Merkezi	VRM.2.U4	Acil durumlarda elektrik iletiminin acil kapatılması	• Acil durumlarda elektrik iletiminin kapatılması için bir mekanizma bulunuyor mu? • Acil durum kapatma anahtarının (hangi BT odalarında bulunması gerektiği değerlendirildi mi? • Acil durum anahtarının, UPS ve jeneratörde dahil tüm güç kaynaklarını da kapattığı test edildi mi?
Veri Merkezi	VRM.2.U5	Hava sıcaklığı ve nemi ile uyumluluk	• Veri merkezinin ısı-yük değerleri düzenli olarak kontrol ediliyor mu? • BT için izin verilen sıcaklık ve nem değerlerinin maksimum ve minimum değerlere uyulması sağlanıyor mu? • BT bileşenlerinin soğutulması yeteri derecede sağlanıyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U6	Erişim kontrolleri	• Veri merkezinde yetkisiz erişime karşı bir erişim kontrol mekanizması kurulmuş mu? • Bütün ziyaretçiler erişim kontrol sisteminden geçiyor mu? • Ziyaretçiler ilgili alanlara, refakatçı eşliğinde mi ulaşıyor? • Anti-passback fonksiyonu (giriş yapmadan çıkış yapamama/çıkış yapmadan giriş yapamama kontrolü) kullanıyor mu?
Veri Merkezi	VRM.2.U7	Kilitleme ve koruma	• Yüksek koruma gerektiren veri merkezinin kapıları ve pencereleri, hırsızlığa, yangına ve dumana karşı güvenli hale getirildi mi? • Güvenli kapılar ve pencereler, işlevselliği bakımından kontrol ediliyor mu?
Veri Merkezi	VRM.2.U8	Yangın alarm sisteminin kullanımı	• Bilişim sektörüne özel olarak tasarlanmış bir yangın alarm sistemi var mı? • Yangın alarm sisteminin işlevselliği düzenli olarak kontrol ediliyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U9	Yangın söndürme veya yangın önleme sistemi kullanımı	• Veri merkezinde bir yangın önleme/söndürme sistemi yer alıyor mu? • Yangın durumunda uygun taşınabilir yangın söndürücülere kolayca erişilebilir mi? • Taşınabilir yangın söndürücüler düzenli olarak kontrol ediliyor ve denetleniyor mu? • Çalışanlara taşınabilir yangın söndürücülerin kullanımı konusunda eğitim/talimat verildi mi?
Veri Merkezi	VRM.2.U10	Altyapı kontrol ve bakım çalışmaları	• Veri merkezi altyapı ekipmanları düzenli olarak gözden geçiriliyor mu? • Bakım talimatları uygulanıyor mu? • Bakım programı, özel gereksinimleri karşılayacak şekilde uyarlanıyor mu? • Olağandışı aşınma ve yıpranma var ise, nedenleri araştırılıyor mu?
Veri Merkezi	VRM.2.U11	Altyapının ortam izlemesi	• Kritik BT ekipmanı ve destek sistemleri için arızalar uzaktan izlenebiliyor mu (bir sistem var mı)?
Veri Merkezi	VRM.2.U12	Veri merkezi için çevre koruma tasarımı ve uygulanması	• Veri merkezi ve çevresini içeren bir koruma konsepti oluşturuldu mu? • Gerekli çevre koruma önlemleri alındı mı?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U13	Alarm sistemlerinin planlanması ve kurulumu	• Kritik alanlar ve olası riskler için herhangi bir alarm sistemi kuruldu mu? • Alarm sistemi düzenli olarak kontrol ediliyor mu? • Alarm mesajlarına verilecek tepkiler belirlenip, roller ve sorumluluklar tanımlandı mı?
Veri Merkezi	VRM.2.U14	Jeneratör kullanımı	• Veri merkezini besleyen ayrı jeneratör bulunuyor mu? • Jeneratörün üzerindeki yük ve depo doluluk oranları gibi unsurlar düzenli olarak kontrol ediliyor mu? • Jeneratörün bakım aralıklarına uyuluyor mu? • Bakım sırasında yük ve fonksiyonel testler yapılıyor mu? • Her 2 yılda, en az bir kere gerçek koşullar altında jeneratör test çalışmaları yapılmakta mıdır?
Veri Merkezi	VRM.2.U15	Aşırı gerilimden korunma cihazları	• Veri merkezinin aşırı gerilimden korunma konsepti oluşturuldu mu? • Yıldırım ve aşırı gerilim koruma cihazları, periyodik olarak ve belli olaylardan sonra kontrol ediliyor ve gerekirse değiştiriliyor mu? • Uçtan uca bir topraklama/potansiyel dengeleme uygulandı mı? • Yeni donanım eklendiğinde, topraklamaya dikkat ediliyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U16	Veri merkezi iklimlendirme	• Veri merkezinde uygun iklim koşullarının sağlanması için iklimlendirme sistemleri kullanılıyor mu? • BT için izin verilen sıcaklık ve nem değerlerinin maksimum ve minimum derecelerine uyuluyor mu, örn. yeterli ve ekonomik soğutma? • Kullanılan klimaların bakımları düzenli olarak yapılıyor mu?
Veri Merkezi	VRM.2.U17	Erken yangın algılama	• Yangınların mümkün olduğunca erken tespiti sağlanabiliyor mu? • Veri merkezinde bir yangın algılama sistemi bulunuyor mu?
Veri Merkezi	VRM.2.U18	Su sızıntısına karşı koruma	• Veri merkezini su sızıntısına karşı korumak için gerekli önlemler alınıyor mu? • BT alanlarında su boruları bulunuyor mu ve varsa kaldırılması ile ilgili bir çalışma yapıldı mı? • Su borularındaki sızıntının önceden tespiti için düzenlemeler yapıldı mı? • Kritik noktalardaki su boruları, düzenli aralıklar ile görsel kontrole tabi tutuluyor mu? • Yüksek erişilebilirlik kapsamında, su sızıntı lokalize edilebiliyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U19	Teknik altyapı fonksiyonel testler	• Temel altyapı bileşenleri için gerçek fonksiyonel testler gerçekleştiriliyor mu? • Fonksiyon testleri düzenli aralıklarla mı gerçekleştiriliyor?
Veri Merkezi	VRM.2.U20	Altyapı ve inşaat planlarının düzenli güncellemeleri	• Veri merkezine ilişkin tüm altyapı ve bina planları güncel mi? • Bu planların güncelliğini sağlamak için nasıl bir yöntemden yararlanılıyor?
Veri Merkezi	VRM.2.U21	Felaket Kurtarma Merkezi	• Felaket durumunda, kritik iş süreçlerinin ve BT hizmetlerinin çalışabilmesini sağlayacak bir FKM mevcut mu?
Veri Merkezi	VRM.2.U22	Veri merkezi operasyonu sırasında inşaat projeleri	• BT odalarında özelikle taşınma durumlarındaki toz koruma önlemleri nelerdir? • Bu alanlardaki inşaat çalışmaları, BT personeli tarafından izleniyor mu?
Veri Merkezi	VRM.2.U23	Güvenli veri merkezi kabloları	• Veri merkezi içerisinde yer alan kablolar; kişiler, araçlar ve makineler tarafından verilebilecek hasara karşı yeterince korunuyor mu? • Cihaz bağlantı kablolarının uygun biçimde bağlanmasına dikkat ediliyor mu? • Veri merkezinin, yangın riski yüksek alanlarında kablo taşıma güzergahlarının bulunmamasına dikkat ediliyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Veri Merkezi	VRM.2.U24	Video gözetim sistemlerinin kullanımı	• Veri merkezinde video gözetim sistemleri kullanılıyor mu? • Video gözetimi bina güvenlik konseptine entegre mi? • Video gözetim sisteminin düzgün çalıştığı, düzenli olarak kontrol ediliyor mu?
Veri Merkezi	VRM.2.U25	Kesintisiz güç kaynaklarının (UPS) yedekli tasarımı	• Yüksek erişilebilirlik kapsamında, UPS sistemleri yedekli tasarlandı mı? • Yedekli yapı, düzenli olarak kontrol ediliyor mu?
Veri Merkezi	VRM.2.U26	Yedekli jeneratör	• Yüksek erişilebilirlik kapsamında, jeneratörler yedekli tasarlandı mı? • Yedekli yapı düzenli olarak kontrol ediliyor mu?
Veri Merkezi	VRM.2.U27	Felaket kurtarma ve yangın tatbikatları	• Yazılı bir acil eylem planı oluşturuldu mu? • Acil durum tatbikatları (yangın önleme vb.) uygulandı mı?
Elektrik Kablolama	VRM.3.U1	Uygun kablo tiplerinin seçimi	• Kablo seçilirken, teknik gereksinimlerin yanında ortam koşulları da inceleniyor mu? • Kablo kılıfı ile ilgili olarak gerekli kriterler (örn. sıcaklık aralığı, fonksiyonel bütünlük, su basıncı direnci vb.) dikkate alınıyor mu? • Geçerli standartlar ve yönetmelikler (örn. yangından korunma, işletim güvenliği için) dikkate alınıyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Elektrik Kablolama	VRM.3.U2	Kablo yönetimi	• Kablo taşıma kanalları, olası genişletme veya asgari mesafeler bakımından yeterince boyutlandırılmış mı? • Veri ve elektrik kabloları birbirlerinden ayrı olarak iletiliyor mu?
Elektrik Kablolama	VRM.3.U3	Profesyonel kurulum	• Elektrik kablolaması, geçerli standartlara ve üreticinin özelliklerine uygun bir şekilde kuruldu mu?
Elektrik Kablolama	VRM.3.U4	Elektrik kablolamanın iş kabulü	• Mevcut ve geleceğe yönelik ihtiyaçlar göz önünde bulundurularak, elektrik kablolama gereksinimleri oluşturulmuş mu?
Elektrik Kablolama	VRM.3.U5	Elektrik kablolama muayene ve kabulü	• Elektrik kablolaması, kurulum sonrası BT güvenliğini de kapsayacak bir onay sürecinden geçiyor mu? • İş kabul belgeleri; giderilen eksiklikler, kalan işler, garanti bitiş tarihleri hakkında bilgileri içeriyor mu? • Katılımcılar ve sorumlu kişiler tarafından imzalanan kablolama kabul protokolü mevcut mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Elektrik Kablolama	VRM.3.U6	Aşırı gerilimden korunma	• Kurum veya organizasyonda, aşırı gerilimden korunma konsepti oluşturuldu mu? • Yıldırım ve aşırı gerilim koruma • cihazları, periyodik olarak ve belli olaylardan sonra kontrol ediliyor ve gerekirse değiştiriliyor mu? • Uçtan uca bir topraklama/potansiyel dengeleme uygulandı mı? • Yeni donanım eklendiğinde, topraklamaya dikkat ediliyor mu?
Elektrik Kablolama	VRM.3.U7	Gereksiz kabloların çıkarılması ve devre dışı bırakılması	• Yangın yüklerini önlemek için gerekli olmayan kablolar çıkartılıyor mu? • Kablolar kaldırıldıktan sonra, yangın duvarları doğru şekilde kapatılıyor mu? • Kablolamadaki değişiklikler kayıt altına alınıyor mu?
Elektrik Kablolama	VRM.3.U8	Kablo taşıma sistemlerinin yangından korunması	• Yangından korunma gereksinimleri ve yönetmelikleri, elektrik kablolama kurulumları sırasında yerine getiriliyor mu?
Elektrik Kablolama	VRM.3.U9	Elektrik kablolamanın dokümantasyonu ve etiketlenmesi	• Elektrik kabloları doğru biçimde etiketleniyor mu? • Elektrik kablolamanın etiketleme ve dokümantasyonu ile ilgili düzenlemeler mevcut mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Elektrik Kablolama	VRM.3.U10	Elektrik tesisatlarının ve bağlantılarının kontrolü	• Elektrik panoları ve prizleri, kablolama açısından düzenli olarak kontrol ediliyor mu? • Kabloların kontrolü sırasında tespit edilen eksiklikler, nedeni belirtilerek (kayıt altına alınarak) düzeltiliyor mu?
Elektrik Kablolama	VRM.3.U11	Elektrikli cihazların ve elektrik altyapısının yangın çıkarma riski	• İşyerinde kullanılan elektrikli cihazlar için düzenlemeler var mı? • Yüksek kalite grup prizi seçimine dikkat ediliyor mu? • Elektrik dağıtımı (özellikle bağlantı noktaları, terminal noktaları ve devre kesiciler) düzenli olarak kontrol ediliyor mu? • BT cihaz fanları düzenli olarak toz tortularına karşı kontrol ediliyor mu ve temizleniyor mu? • Elektrikli cihazlar ve elektrik dağıtımı, test sonuçları ile birlikte belgeleniyor mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Elektrik Kablolama	VRM.3.U12	İkincil güç kaynağı	• Veri merkezi ikincil bir güç kaynağı ile destekleniyor mu? • Jeneratör kaynakları düzenli olarak kontrol ediliyor mu? • Bakım sırasında yük ve fonksiyonel testler uygulanıyor mu? • Gerçek ortam koşulları altında ve iki yılda en az bir kere, jeneratör test çalışmaları icra ediliyor mu? • UPS aküleri gerekli sıcaklık aralığında tutuluyor mu? • UPS'in bakım aralıklarına uyuluyor mu? • Akünün gerçek kapasitesi ve dolayısıyla UPS'in yedekleme süresi düzenli olarak test ediliyor mu? • Yeni cihazlar sistemlere eklendiğinde, UPS besleme sürelerinin yeterliliği kontrol ediliyor mu?
Elektrik Kablolama	VRM.3.U13	A-B (“Dual bus”) yedekli sistem	• Kritik BT bileşenleri tamamen iki farklı kanaldan besleniyor mu?
Elektrik Kablolama	VRM.3.U14	Elektrik kablolamanın malzeme güvenliği	• Kurulu kabloların serbestçe erişilebildiği yerlerin sayısı minimuma (hasar, sabotaja vb.) indirildi mi? • Panolar kilitli olarak tutuluyor mu, panolara erişim yönetmelikleri mevcut mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
Elektrik Kablolama	VRM.3.U15	Kabin sistemlerinin kullanımı	• Kabin sistemleri, içinde barındığı BT bileşenlerinin güvenliğini sağlayacak özelliklere sahip midir? • Kabin sistemleri, içinde kurulu olan BT bileşenlerinin soğutulması için uygun mu? • Kullanılan kabin sistemlerinin seçimi için uygulanan genel bir prosedür var mı?
BT Kablolama	VRM.4.U1	Uygun kablo tiplerinin seçimi	• Kablo seçilirken, teknik gereksinimlerin yanında çevresel koşulları da inceleniyor mu? • Kablo kılıfı ile ilgili olarak gerekli kriterler (örn. sıcaklık aralığı, fonksiyonel bütünlük, su basıncı direnci vb.) dikkate alınıyor mu? • Geçerli standartlar ve yönetmelikler (örn. yangından korunma, işletim güvenliği için) dikkate alınıyor mu?
BT Kablolama	VRM.4.U2	Kablo yönetimi	• Kablo taşıma kanalları, olası genişletme veya asgari mesafeler bakımından yeterince boyutlandırılmış mı? • Veri ve elektik kabloları ayrı yollardan iletiliyor mu?
BT Kablolama	VRM.4.U3	Profesyonel kurulum	• Elektrik kablolaması, geçerli standartlara ve üreticinin özelliklerine uygun bir şekilde kuruldu mu?
BT Kablolama	VRM.4.U4	BT kablolama ihtiyaç analizi	• Mevcut ve geleceğe yönelik ihtiyaçlar göz önünde bulundurularak, BT kablolama gereksinimleri oluşturulmuş mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
BT Kablolama	VRM.4.U5	BT kablolama muayene (kabul)	• BT kablolama, kurulum sonrası BT güvenliğini de kapsayacak bir onay sürecinden geçiyor mu? • İş kabul belgeleri; giderilen eksiklikler, kalan işler, garanti bitiş tarihleri hakkında bilgileri içeriyor mu? • Katılımcılar ve sorumlu kişiler tarafından imzalanan BT kablolama kabul protokolü mevcut mu?
BT Kablolama	VMR.4.U6	Ağ dokümanlarının gözden geçirilmesi ve güncellenmesi	• BT kabloma dokümantasyonu, ağda yapılan değişiklikler sonrası güncelleniyor mu? • Mevcut durum bu dokümanlardan izlenebiliyor mu?
BT Kablolama	VRM.4.U7	Kablo taşıma sistemlerinin yangından korunması	• Yangın yükü oluşturan gereksiz kablolar sökülüp atılıyor mu? • Demontaj sonrası, yangın bariyerlerinin düzgün kapatıldığı kontrol ediliyor mu? • Demontaj kararı ilgili birimlerin incelemesinden sonra mı alınıyor? • İşletim belgelerin de bu tür değişikliler kayıt altına alınıyor mu?
BT Kablolama	VRM.4.U8	BT kablolamanın dokümantasyonu ve etiketleme	• BT kabloları doğru bir biçimde etiketleniyor mu? • BT kablolamanın etiketleme ve dokümantasyonu ile ilgili düzenlemeler mevcut mu?

Uygulama	Gereksinim Kodu	Gereksinim Adı	Kontrol Soruları
BT Kablolama	VRM.4.U9	Mevcut bağlantıların kontrolü	• Pano ve kablo çıkışları (priz vb.) düzenli olarak kontrol ediliyor mu? • Kontroller sırasında tespit edilen eksiklikler nedeni belirtilerek, düzeltiliyor mu?
BT Kablolama	VRM.4.U10	Ağ yedekliliği	• Yüksek erişilebilirlik kapsamında, farklı hatlar üzerinden yedekli kablo taşıma sistemleri (birincil, ikincil, üçüncül vs.) kullanılıyor mu? • Yedekli kablolamanın işlevselliği düzenli olarak kontrol ediliyor mu?
BT Kablolama	VMR.4.G11	BT kablolamanın fiziksel güvenliği	• Kurulu kabloların serbestçe erişilebildiği yerlerin sayısı minimuma (hasar, sabotaja vb.) indirildi mi? • Panolara erişim yönetmelikleri mevcut mu?
BT Kablolama	VRM.4.U12	Korumalı (shielded) kablo kullanımı ile elektromanyetik alandan korunma	• Elektromanyetik alanların, kablo üzerinden iletilen sinyalleri bozması korumalı kablolar ile engelleniyor mu?
BT Kablolama	VRM.4.U13	Kabin sistemlerinin kullanımı	• Kabinlerin ve kabin ekipmanının seçimi ile ilgili genel bir düzenleme (tek tip kabin seçimi gibi) var mı?

TÜBİTAK BİLGEM
Yazılım Teknolojileri Araştırma Enstitüsü

Çukurambar Mah. Malcolm X Cad. No: 22 06100 Çankaya - ANKARA
T 0312 284 92 22 **F** 0312 286 52 22
E epid.yte@tubitak.gov.tr

www.yte.bilgem.tubitak.gov.tr
www.dijitaldonusum.gov.tr