TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

UZAKTAN ÇALIŞMA REHBERİ

İŞLETİM VE BAKIM

Mayıs 2020

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Mayıs 2020	İlk sürüm	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 Değerlendirme 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 2764 soru belirlenmiştir.

Model'in 8 kurumda 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 Yönetimi Rehberi, Aktif Dizin Yönetimi Rehberi, Sunucu Yönetimi Rehberi** ve **İstemci Yönetimi Rehberi** yayımlanmıştır. 2020 yılının Mayıs ayında bunlara ek olarak **Uzaktan Çalışma Rehberi** yayımlanmıştır.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** **www.dijitalakademi.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. 38 bilişim profesyonel rolü ile bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 6 kurumda yaklaşık 550 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

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

1 GİRİŞ

Uzaktan Çalışma 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, Uzaktan Çalışma Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Uzaktan Çalışma Rehberi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
Akıllı Kart	Temaslı veya temassız olarak kart okuyucu cihazlardan okunabilen, içerisinde kendine özel işlemcisi olan, özel şifreleme tekniğiyle izinsiz kopyalanma ve içeriğini okumaya izin vermeyen plastik kartlardır.
Ayrıcalıklı Hesap	[Privileged Account] Standart hesaplardan farklı olarak güçlü haklar, ayrıcalıklar ve izinlerin verildiği hesaplardır.
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
Bilgi Güvenliği	Bilginin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunmasıdır.
Biyometrik	İnsanların kendine özgü benzersiz, fiziksel ve davranışsal izleridir.
BT	Bilişim Teknolojileri

Terim / Kısaltma	Tanım
d-Devlet	Dijital Devlet
DOS	[Denial of Service] Erişim engelleme saldırısı
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
HA	[High Availability] Yüksek erişilebilirlik olarak adlandırılır ve sunulan servisin herhangi bir nedenle kesintiye uğramaması, sürekliliğinin sağlanmasıdır.
Hizmet	Kullanıcını ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (ör. Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
IDS	[Intrusion Detection System] Saldırı tespit sistemi
IPS	[Intrusion Pevention System] Saldırı önleme sistemi
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanabilmesi yetisidir.
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.
LAN	[Local Area Network] Yerel alan ağı

Terim / Kısaltma	Tanım
LOG	Sistemde meydana gelen işlem ve olayların kaydedildiği dosyalara verilen addır.
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.
PIN	[Personal Identfication Number] İçerisinde alfanümerik veya sayısal karakterleri barındıran, bir sistemde erişim hakkına sahip olmak için kullanılan paroladır.
Problem	Bir veya birden fazla arızaya/kesintiye neden olan ve çözülmesi istenen sorundur.
Risk	Hedeflenen kazanç veya çıktıya, gelecekte olumlu veya olumsuz etkisi olabilecek belirsizliklerdir.
SSL	[Secure Sockets Layer] Sunucu ile istemci arasındaki iletişimi şifreleme yöntemidir.
STK	Sivil Toplum Kuruluşu
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme

Terim / Kısaltma	Tanım
Token	Elektronik olarak yetkisiz erişimlere karşı kısıtlanmış bir kaynağa erişmek için kullanılan aygıttır.
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
VPN	[Virtual Private Network] İletişimi, kimlik doğrulaması ve şifrelemeye tabi tutarak güvenli hale getiren tünelleme yöntemi
WAN	[Wide Area Network] Geniş alan ağı
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1.2 REFERANSLAR

Ref 1. NSA (2018), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri

Ref 2. IT Grundschutz 1.Yayım (2018): Bilgi Teknolojileri Güvenliği Enstitüsü (BSI), Almanya.

Ref 3. ISO (2013). ISO/IEC 27001 - Information security management.

Ref 4. ISO (2013). ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security controls

Ref 5. Mataracıoğlu, T., Kalıpcıoğlu, C., Arıkan, S., Işık, G., Demiral, Y.,(2020). Küresel Salgın Sonrasında Ulusal Bilişim Güvenliği, TÜBİTAK BİLGEM, Ankara.

2 DİJİTAL OLGUNLUK DEĞERLENDİRME MODELİ VE REHBERLİĞİ PROJESİ

Dijital Olgunluk Değerlendirme 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, On Birinci Kalkınma Planı'nda "Kamu Hizmetlerinde e-Devlet Uygulamaları" başlığı altında yer alan aşağıdaki politika ve tedbirler ile desteklenmektedir:

- "811.2. Kamu kurumlarının bilişim projeleri hazırlama ve yönetme kapasitelerinin artırılmasına yönelik eğitimler verilecek ve rehberler hazırlanacaktır."
- "814.2. Kamu kurumlarında bilgi güvenliği yönetim sistemi kurulması ve denetlenmesine yönelik usul ve esaslar belirlenecek, hazırlanacak rehberlerle bu konuda kamu kurumlarına yol gösterilecektir."
- "811.3. Kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilerek kamu kurumlarında yaygınlaştırılacaktır."

2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda doğrudan rehberlik mekanizmalarına yönelik tanımlanan aşağıdaki eylemlere de bu proje ile 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 **Rehberler** 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.

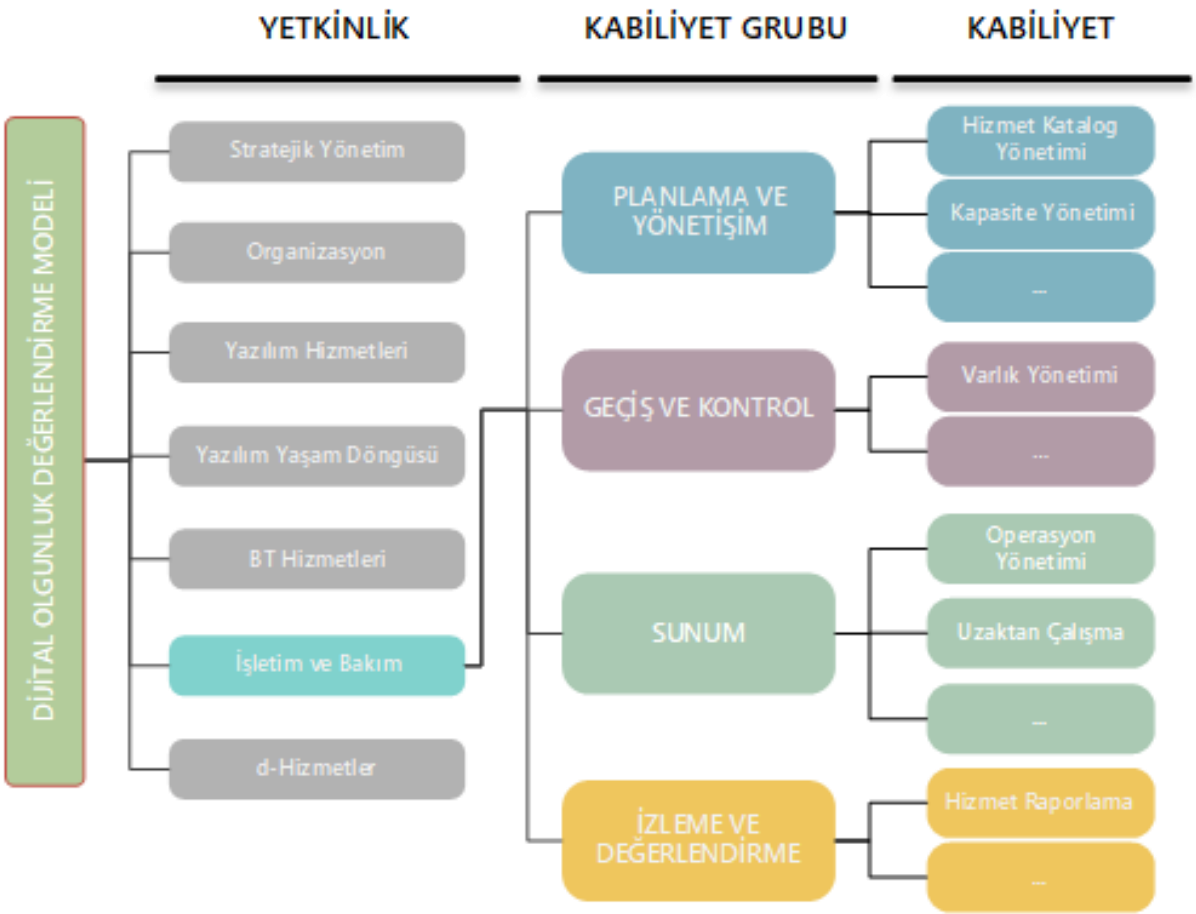
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır. 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 **Model'in** 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

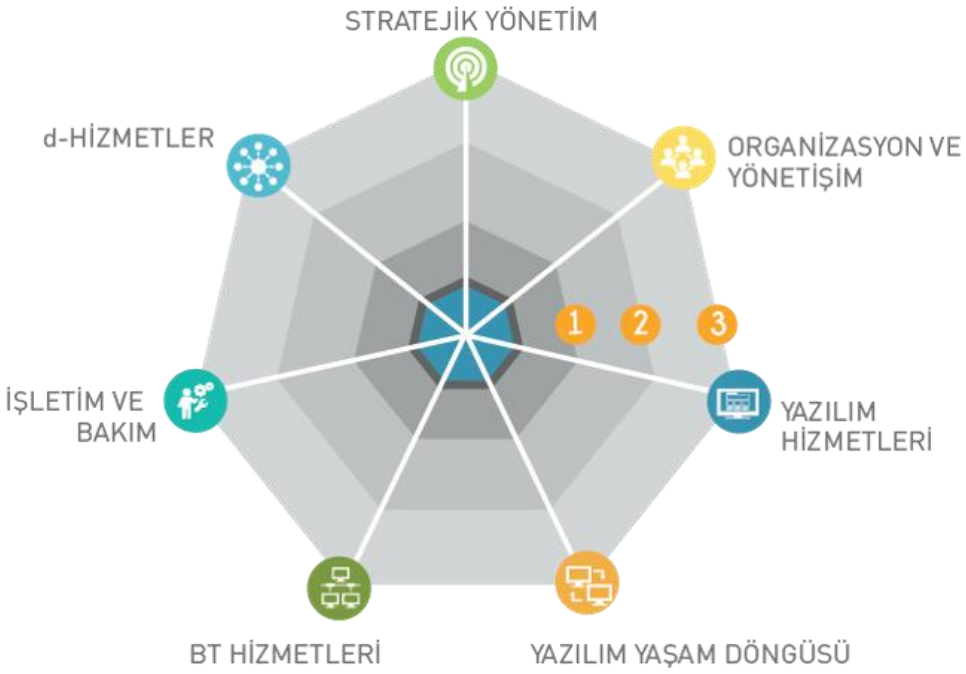
Dijital Olgunluk Değerlendirme Modeli 7 yetkinlik altında tanımlanmış 35 kabiliyet grubu ve bu kabiliyet grupları altında gruplandırılmış çeşitli kabiliyetlerden oluşmaktadır:

- **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 yönetimi, kurumsal mimari yönetimi, dijital dönüşüm yönetimi ve bütçe yönetimi kabiliyet gruplarını içermektedir.

2. Yetkinlik: ORGANİZASYON VE YÖNETİŞİM

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, dijital kapasite geliştirme ve dijital yönetişim 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, gereksinim mühendisliği, teknik çözüm, doğrulama ve geçerleme, konfigürasyon yönetimi ve kalite güvence kabiliyet gruplarını içermektedir.

5. Yetkinlik: BT HİZMETLERİ

Kurumun sahip olduğu teknolojiler ile mevcut donanım ve altyapıların yönetilmesini kapsar. Bu yetkinlik, ağ ve iletişim, veri merkezi, uygulamalar ve BT sistemleri 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, 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 hizmetlerinin 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;

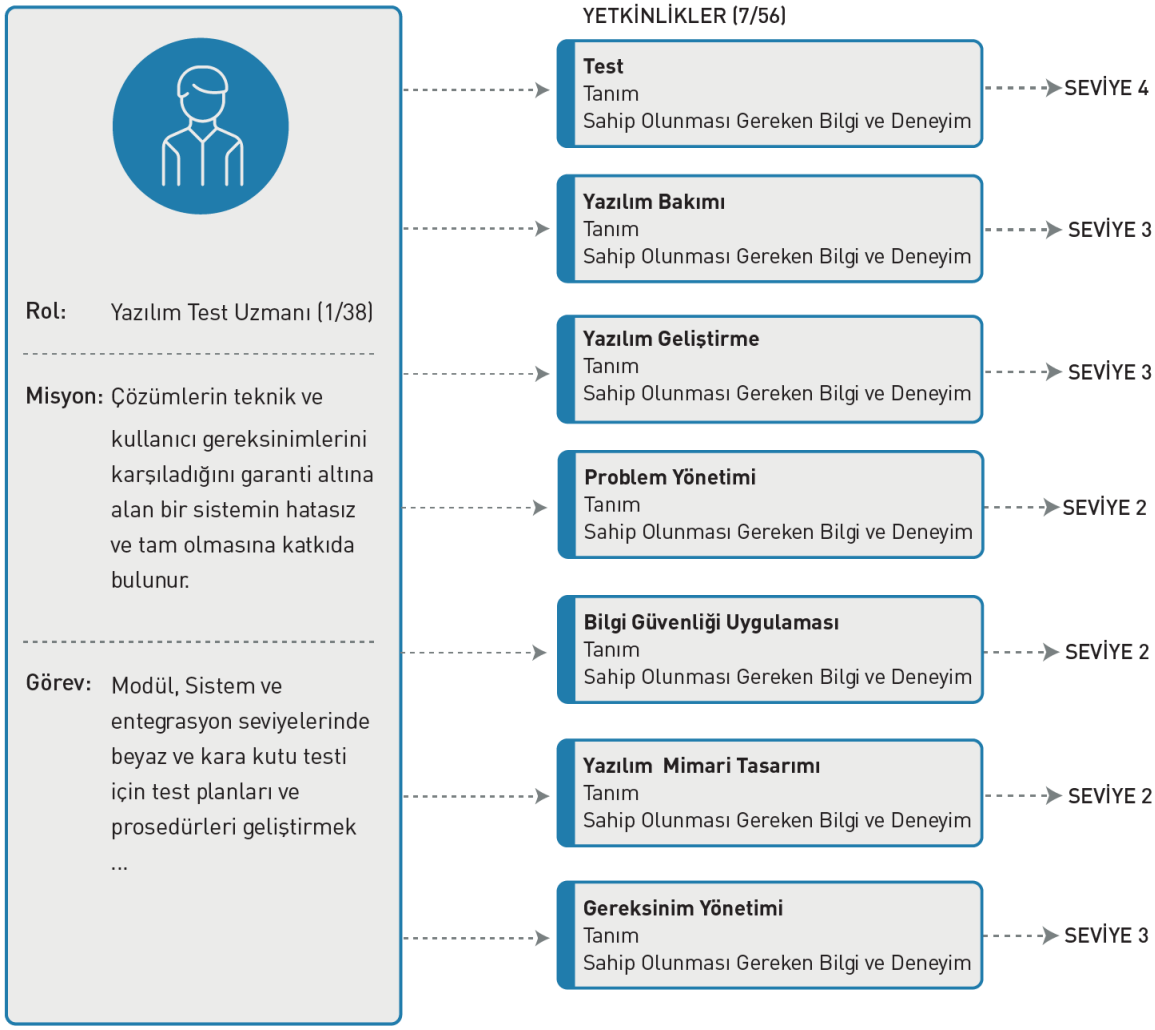
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının 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;

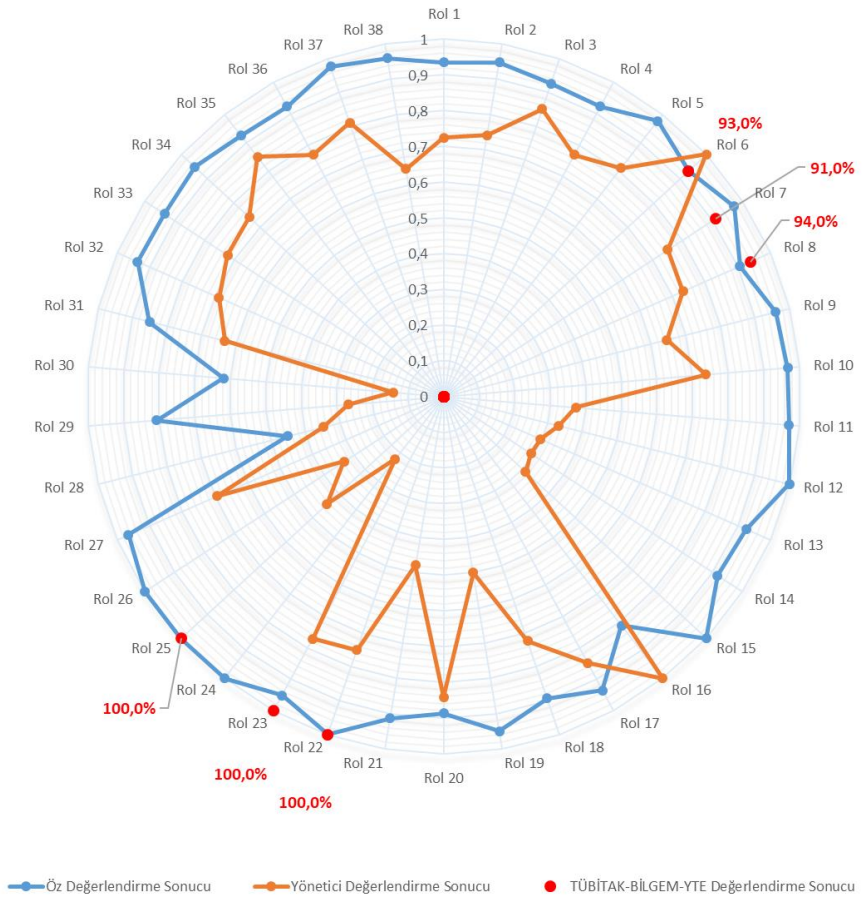
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

alanlarında Türkiye'deki organizasyon yapılarına özgü 38 bilişim profesyonel rolü tanımlanmıştır: Ayrıca, bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller; yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. Bunun için bir örnek aşağıdaki gibidir:



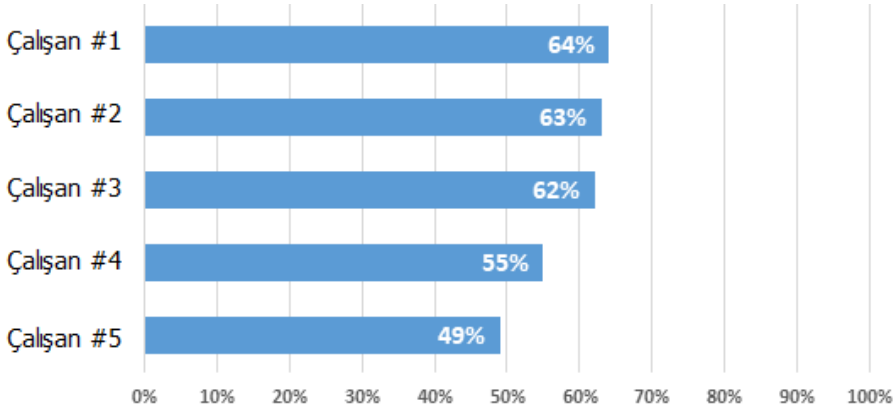
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

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 38 rol bazında uygunluğu raporlanmaktadır:



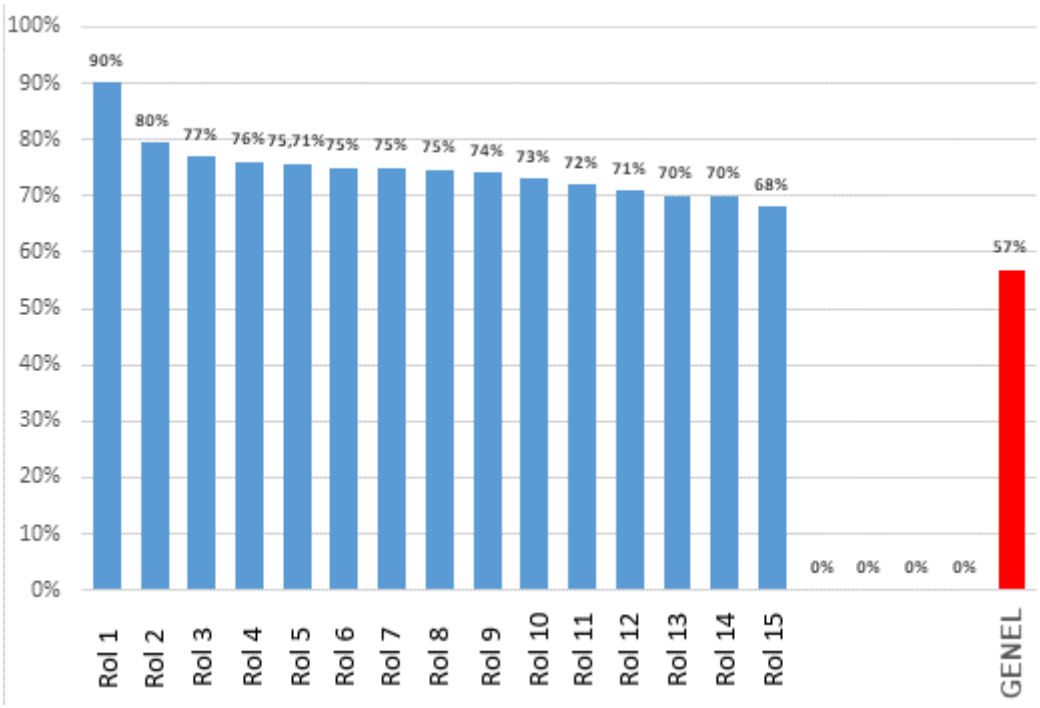
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

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 İŞLETİM VE BAKIM YETKİNLİĞİ

İşletim ve Bakım Yetkinliği altında toplanan rehberler ile kamu kurumlarına işletim ve bakım alanında yol göstermesi amacıyla 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 sunulması amaçlanmıştır. 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 seviyesi artıkça sürekli kullanılabilecek bir rehber olma özelliği taşımaktadır.

Rehberin hedef kitlesi öncelikli olarak kamu kurumlarında, işletim ve bakım proje ve faaliyetlerini yürütmekle sorumlu birimlerdir. Bu birimler kurumlarda genel olarak Bilgi İşlem Daire Başkanlığı olmaktadır. Bir diğer **Rehber** kullanıcısı olan özel sektör ve STK gibi d-Devlet ekosistemi paydaşları ile **Rehberler** üzerinden ortak bir dil oluşturulması ve bilgi alışverişi yapılması hedeflenmektedir.

"**İşletim ve Bakım**" altında geçen;

- "**İşletim**", her türlü uygulama, donanım, ağ, veritabanı, arşiv vb. BT ile ilgili varlığın sağlıklı bir şekilde işletilmesi ve BT hizmetlerini kullanan diğer iş alanlarına ve müşterilere sorunsuz sunum sağlamak amacıyla gerçekleştirilen operasyon ve destek çalışmalarını kapsamaktadır. Örn: Sunucu yönetimi, ağ yönetimi, veritabanı yönetimi, kimlik yönetimi, arıza yönetimi, uygulama destek.
- "**Bakım**" ise, BT varlıklarının devamlı olarak sağlıklı ve güvenli çalışmasını garanti etmek üzere düzenli / dönemsel olarak gerçekleştirilen çalışmalardır. Örn: Veri merkezi bakımı, sistem odası bakımı.

İşletim ve Bakım Yetkinliği altından hazırlanan rehberler kapsamında, BT hizmet yönetim standartları konusunda kamu kurumlarında ciddi bir açık olduğu, bu nedenle planlanan bu rehberin kamu kurumlarına önemli bir katkı sağlayacağı öngörülmüştür. BT yaşam döngüsü içerisinde işletim ve bakım proje ve faaliyet tiplerine odaklanılarak özel bir rehber üretilmesi ile ekosisteme büyük katkı sağlaması hedeflenmiştir

4.1 YÖNTEM

Bu rehber çalışmaları sırasında, uluslararası boyutta hazırlanmış ve bu alanda kabul görmüş çeşitli standartlar, çerçeveler ve makalelerden faydalanılmıştır.

Faydalanılan kaynaklar şunlardır:

- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) [Ref 1], Amerika Birleşik Devletleri.
- Bilgi Teknolojileri Güvenliği Enstitüsü (BSI) [Ref 2], Almanya.
- ISO 27001 [Ref 3]: Bilgi Güvenliği Yönetimi Sistemi gereksinimlerini tanımlayan uluslararası denetlenebilir standarttır.
- ISO 27002 [Ref 4]: Bilgi Güvenliği Yönetim Sistemine ait iyi uygulama örneklerini içeren dokümandır.
- Küresel Salgın Sonrasında Ulusal Bilişim Güvenliği.

Özellikle **Rehber'de** detaylandırılacak alt kabiliyetlerin belirlenmesi için IT-Grundschutz BSI, ISO 27001 ve ISO 27002 temel alınmıştır. Türkiye'nin yapısına uygun uluslararası model ve standartlar örnek alınarak ilgili temel başlıklar oluşturulmuş ve kabiliyetler üzerinden **Rehber'in** yapısı belirlenmiştir.

4.2 REHBER YAPISI

Rehber **Uzaktan Çalışma** kabiliyeti 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 bu kabiliyet kapsamında olgunluk seviyesini artırmaya yönelik sürekli kullanılabilecek bir rehber olma özelliği taşımaktadır.

Her konu, (açıklamalar, riskler ve gereksinimleri anlatan) temel bileşen ve buna ek olarak (gereksinimlerin nasıl karşılanacağına dair talimatlar içeren) uygulama rehberinden oluşur.

Bu rehber, 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. Rehber içerisindeki standartlaştırılmış güvenlik gereksinimleri, BT çalışanları tarafından kendi kurumsal koşullarına uyan koruma önlemlerine kolay bir şekilde dönüştürülebilir. Rehberde uygulanan analiz yöntemi, temel

bileşenlerde önerilen güvenlik gereksinimleri ile mevcut durumun karşılaştırılmasını mümkün kılmaktadır.

Rehberde 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 kurum ve kuruluşlar, en önemli gereksinimleri öncelikli karşılamak için 1. seviye gereksinimlere göre kendilerini sınırlandırabilirler. Ancak, yeterli korunma yalnız 2. seviye gereksinimlerin uygulanmasıyla sağlanacaktır. 3. seviye koruma gereksinimleri için örnek olarak, uygulamada kendini kanıtlamış ve kurumun daha fazla koruma 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 bir risk analizi yapılmalıdır. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin uygulanması ve bu yöndeki ihtiyaçların giderilmesi, kurumun veya kuruluşun hedefleri doğrultusunda yeterlidir.

Temel bileşen rehberlerine ek olarak oluşturulan uygulama rehberi, hedeflenen gereksinimlerin en iyi şekilde nasıl uygulanabileceğine dair ek bilgiler içerir. Bu rehberde yer alan 1. ve 2. seviye gereksinimlerin yerine getirilmesi, ISO 27001 süreçlerine de katkı sağlayacaktır.

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

TEMEL BİLEŞEN YAPISI

Temel bileşenler, ilgili konunun prosedürlerini ve açıklamalarını içermekte, risklere ve bileşenin korunmasını sağlamaya yönelik özel gereksinimlere kısa bir genel bakış sunmaktadır. 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.

Rehberler içerdikleri konular itibari ile birbirleri arasındaki ilişkinin kurulması için bir referanslama metodu kullanılmıştır. Bu amaçla her gereksinim maddesi numaralandırılmıştır. Örneğin, Sunum rehberlerinde yer alan **SNM.7.G1** kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

“Sunum” kabiliyet grubu için kullanılan kısaltma	**Kabiliyet Sıra Kodu**	**Gereksinim maddesi**
SNM	7	G1

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberinde ise yalnız “**G**” harfi yerine “**U**” harfi kullanılmıştır. Örneğin, SNM.7.G1 gereksinim maddesinin karşılığı SNM.7.U1 olarak geçmektedir.

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 rehberi “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 rehberinde yer alan gereksinimlere ait hazırlanan kontrol soruları **EK-A**’da verilmektedir.

4.3 KABİLİYET GRUPLARI

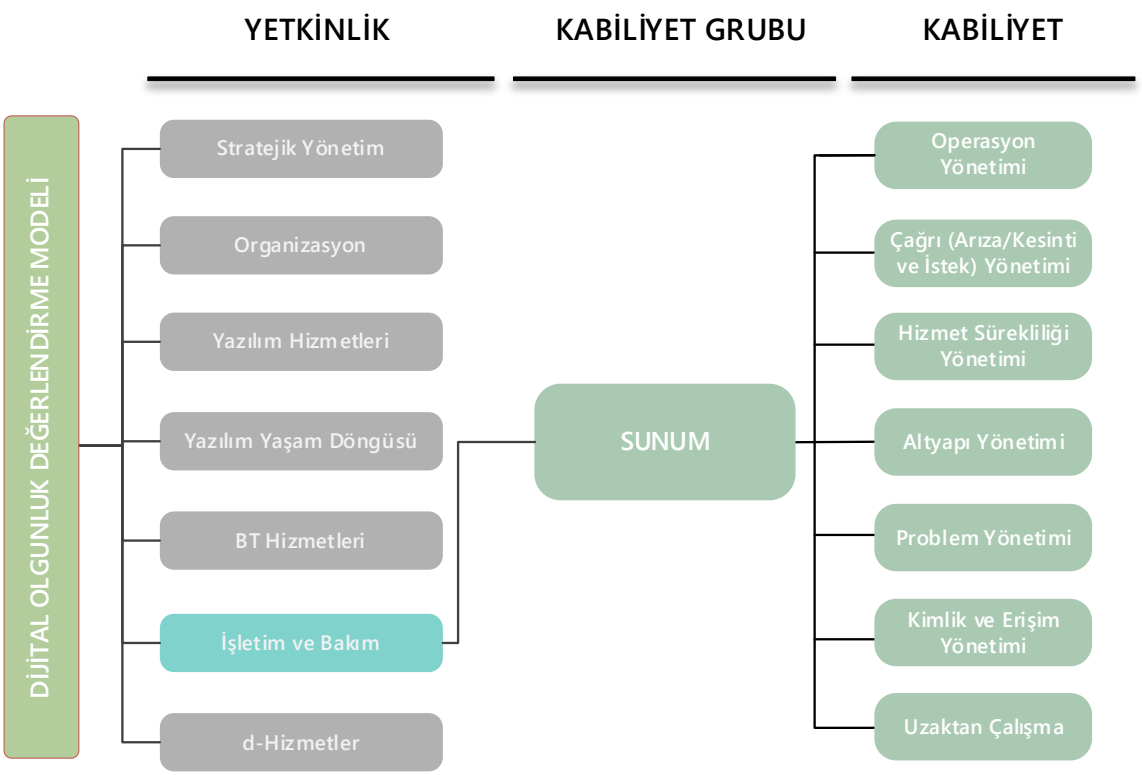
İşletim ve bakım yetkinliğinde ele alınan kabiliyet gruplarının açıklaması ve altlarındaki kabiliyetler şu şekildedir (Şekil 7).

Şekil 7 İşletim ve Bakım Yetkinliği Kabiliyet Grupları

- **Planlama**; BT hizmetlerinin planlanmasının sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
    - Hizmet Katalog Yönetimi
    - Kapasite Yönetimi
    - Yeni / Değişen Hizmetlerin Tasarımı
    - İş İlişkileri Yönetimi
    - Hizmet Seviyesi Yönetimi
    - Hizmet Erişilebilirlik Yönetimi
    - Bütçeleme ve Muhasebe Yönetimi
- **Geçiş ve Kontrol**; Yeni planlanan / değişen BT hizmetlerinin devreye alınması ve kontrolünün sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
    - Varlık Yönetimi
    - Değişiklik Yönetimi
    - Konfigürasyon Yönetimi
    - Sürüm ve Yaygınlaştırma Yönetimi
- **Sunum**; BT hizmetlerinin yönetimi, sunulması ve desteğinin sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
    - Operasyon Yönetimi
    - Çağrı (Arıza / Kesinti Ve İstek) Yönetimi
    - Hizmet Sürekliliği Yönetimi
    - Altyapı Yönetimi
    - Problem Yönetimi
    - Kimlik ve Erişim Yönetimi
    - Uzaktan Çalışma
- **İzleme ve Değerlendirme**; BT Hizmet kalitesinin sürekli iyileştirilmesinin sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
    - Hizmet Raporlama
    - Hizmet İyileştirme

Rehber'de yer alan sorular EK-A'da yer almaktadır.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

SNM: SUNUM

SNM.7.G UZAKTAN ÇALIŞMA

TEMEL BİLEŞEN REHBERİ

SNM.7.G UZAKTAN ÇALIŞMA TEMEL BİLEŞEN

1 AÇIKLAMA

1.1 TANIM

Dizüstü bilgisayarlar, akıllı telefonlar veya video konferans yazılımları gibi giderek yaygınlaşan iletişim araçları sayesinde, çalışanlar neredeyse her yerde işlerini sürdürebilme imkânı bulmaktadır. Teknolojinin gelişmesiyle beraber, işler yalnızca ofis alanlarında değil, ofis dışındaki alanlarda da rahatlıkla yürütülebilmektedir. İster otel odasında veya ulaşım aracında olsun, ister müşterinin yanında; uzaktan çalışma modeli, mesai saatlerini, çalışma alanını ve görev dağılımına kadar iş hayatımızda yer alan birçok tanımı değiştirmektedir.

Teknik altyapıları, insan kaynakları, politika ve prosedürleri ile iş yapış şekilleri bakımından uzaktan çalışma modeline uyumluluk gösteren kurum ve kuruluşlar, bu modeli uygulamada daha güvenli ve başarılı bir yerde konumlanırlar. Ayrıca müşteriler, tedarikçiler ve iş ortakları gibi diğer paydaşların da uzaktan çalışma modeline gösterdikleri uyum, bu modelin güvenliğini ve başarısını etkiler. Paydaşların bu modeli uygularken yaşadıkları sorunlar veya iş yapış şeklinden kaynaklanan bir takım doğal kısıtlar, uzaktan çalışma modeline geçiş sürecini olumsuz etkileyebilir. Bazı sektörlerin yapısı gereği bu modeli uygulaması da mümkün olmayabilir.

Uzaktan çalışma modeli ile birlikte iletişim altyapısına olan ihtiyaç artmaktadır, buna paralel olarak karşı karşıya kalınan bilgi güvenliği riskleri de artış göstermektedir. Birçok kurum ve kuruluş uzaktan çalışma için istekli olsa bile, çok azı uygun bilgi güvenliği politikalarına ve altyapısına sahiptir. Kimlik avı dolandırıcılığı, DDOS atakları, hassas bilginin ifşasına neden olan saldırılar ya da farklı yöntemlerle mevcut sistem açıklarından faydalanan saldırganlar; işlerini uzaktan sürdüren çalışanları herhangi bir açık ağ üzerinden hedef alabilirler.

İşlerin uzaktan yürütülmesi esnasında tüm bu saldırı ve risklere karşı önlem alınabilmesi, ağların ve verilerin bilgi güvenliği gereksinimlerinin karşılanabilmesi için kuruma ait iş modeli, süreç ve politikaların bu modele uygun olarak hazır hale getirilmesi gerekmektedir.

1.2 HEDEF

Bu rehber, uzaktan çalışma modelinin ve içerdiği başlıkların güvenli bir şekilde uygulanmasına yönelik gerekli bilgileri paylaşmayı amaçlamaktadır. Kurum ve kuruluşların yerleşik çalışma alanları için oluşturdukları güvenlik kontrollerinin uzaktan çalışma ortamları için de aynı güvenlik seviyesinde oluşturulabilmesi hedeflenmektedir.

1.3 KAPSAM DIŞI

Bu bileşen rehberi, kurum ve kuruluşların **Uzaktan Çalışma** ile ilgili süreçlerinde kullanılabilir. Uyulması gereken kurallar ve karşılanması gereken temel gereksinimler, bu rehberde sunulmaktadır.

Rehberin odak noktası, uzaktan çalışma modelini kısmen veya tamamen kullanan veya kullanmayı planlayan kurum ve kuruluşların idari, teknik ve personel gereksinimlerini tanımlamaktır.

Uzaktan çalışma esnasında kullanılan BT sistemleri, veri taşıyıcılar, dosyalar, işletim sistemleri ve yazılımlara özgü olan gereksinimler, bu çalışmanın konusu içerisinde yer almamaktadır. Daha özgü alanlar ile ilgili gereksinimler hakkında detaylı bilgi almak için, **Dijital Olgunluk Değerlendirme Modeli**'nin diğer çalışmalarına başvurabilirsiniz.

2 RİSK KAYNAKLARI

Aşağıdaki riskler ve eksiklikler temel düzeyde dikkat edilmesi gereken gereksinim maddeleridir.

2.1 UZAKTAN ÇALIŞMA İLE İLGİLİ EKSİK VEYA YETERSİZ DÜZENLEMELER

Uzaktan çalışma modelinin usul ve esaslarını yeterli seviyede düzenlemeyen kurumlar, iş süreçlerinde yaşanabilecek aksamaların yanı sıra maddi zararlara ve imaj kayıplarına da uğrayabilirler.

Örneğin; bu modelin uygulanması esnasında, (dosyalar, diskler, BT sistemleri gibi) hangi bilgi varlıklarının kurum/kuruluş binası dışına çıkabileceği ve bu süreçte hangi koruyucu önlemlerin dikkate alınacağı düzenlenmez ise kurumun sahip olduğu hassas bilgiler, yetkisi olmayan üçüncü tarafların eline geçebilir ve kurum saygınlığını zedelemek veya siber saldırılar gerçekleştirmek için kullanılabilir.

2.2 DEĞİŞEN ORTAMLARDAN DOLAYI ZARAR GÖRÜLMESİ

Son kullanıcı cihazları ve veri taşıyıcıları farklı ortamlarda kullanıldığında birçok tehlikeye maruz kalır. Uzaktan çalışma ortamı, yerleşik iş ortamları kadar güvenli değildir bu sebeple cihazlar farklı ortamlarda; çok yüksek neme, sıcaklığa veya toza maruz kalabilir. Bu olumsuz ortam koşulları donanımda geri dönülemeyecek hasarlar verebilir. Ayrıca hareket halindeyken BT sistemlerinin taşımasından kaynaklı hasarlara da dikkat edilmesi gerekmektedir.

Fiziksel etkilere ek olarak, farklı güvenlik seviyelerine sahip çalışma ortamları da dikkate alınmalıdır. Akıllı telefonlar, tabletler, dizüstü bilgisayarlar ve benzeri taşınabilir cihazlar düşük güvenlik seviyesine sahip ağlarda, kurumun sahip olduğu diğer BT sistemleriyle iletişim kurduklarında, kötü amaçlı yazılımlar kurumun BT sistemlerine erişebilir ve korunması gereken bilgiler çalınabilir veya fidye yazılımlarıyla şifrelenebilir.

Cihazların kullanıldığı ortam koşulları güvenli bir şekilde yönetilemez ise bu durum; işlerin zamanında yerine getirilememesine, müşteri taleplerinin takip edilememesine veya BT sistemlerinin ciddi zararlar görmesine neden olabilir.

2.3 BT BİLGİ VARLIKLARININ MANİPÜLASYONU VE KULLANILAMAZ HALE GETİRİLMESİ

Uzaktan çalışma esnasında (BT sistemleri, BT ekipmanları, yazılımlar ve belgeler gibi) bilgi varlıklarının saldırganlar tarafından manipüle edilmesi veya kullanılmaz hale getirilmesi daha kolay olabilmektedir. Bu durum, uzaktan çalışma ortamına erişebilen yetkisiz kişi sayısının yerleşik ofis ortamına göre daha fazla olmasından

kaynaklanmaktadır. Bilgi varlıkları manipüle edilirse veya tamamen kullanılamaz hale getirilirse çalışmalar kesintiye uğrayabilir veya tamamen durabilir. Ayrıca kullanılamaz hale getirilen BT bileşenlerinin onarılması veya değiştirilmesi gerekebileceğinden bu durum, maddi zarara yol açabilir.

2.4 GEÇİCİ VE KISITLI ERİŞİLEBİLİRLİK NEDENİYLE GECİKMELER

Genellikle uzaktan çalışanların sabit çalışma saatleri yoktur ve hareket halindeyken çalışanlara ulaşmak daha zor olabilir. Bu durum, iş süreçleriyle ilgili bilgi akışının önemli ölçüde gecikmesine neden olabilir. İletilen e-postalara çalışanın erişiminde gecikmeler yaşanabileceği dikkate alındığında, iş süreçleriyle ilgili mesajlara yanıt verme süresi uzayabilir. İletişim sistem ve alt yapılarına kısıtlı erişimden kaynaklı bu durum, iş süreçleriyle ilgili farklı etki ve sonuçlara neden olabilir.

2.5 BİLGİ VARLIKLARININ GÜVENLİ OLMAYAN ŞEKİLDE TAŞINMASI

BT sistemleri, veri taşıyıcıları, dosyalar gibi bilgi varlıklarının kurum dışına çıkarılması; üzerinde bulunan bilgilerin kaybolmasına, çalınmasına, yetkisiz kişilerce okunmasına veya değiştirilmesine neden olabilir. Bu durum, kurum için prestij kaybına, maddi zararlara ve bilgi güvenliği risklerine yol açabilir. İş yeri dışına çıkarılan bilgi varlıklarının taşınmasında aşağıdaki hususlar dikkat alınmalıdır.

- Yedeksiz dosyaların veya veri taşıyıcılarının taşınması sırasında, varlıkların kaybolması veya çalınması geri döndürülemez kayıplara neden olabilir.
- Şifresiz veri taşıyıcılarının yetkisiz kişilerin eline geçmesi yüksek seviyeli bilgi güvenliği ihlallerine yol açabilir.
- Güvenlik önlemleri yeterli düzeyde değilse, bilgi varlıklarında bulunan veriler fark edilmeden kopyalanabilir veya değiştirilebilir.

2.6 BİLGİ VARLIKLARININ UYGUN OLMAYAN ŞEKİLDE İMHA EDİLMESİ

Hassas bilgi varlıklarının imhası için yerleşik iş ortamları kadar güvenli imha yöntemleri uzaktan çalışma esnasında sunulamayabilir. CD, DVD gibi veri ortamlarının ve dokümanların uygun şekilde imhasının mümkün olmadığı durumlarda genellikle çöp kutuları kullanılır. Otel odası, seyahat için kullanılan toplu taşıma araçları, dinlenme tesisleri, kafe, restoran gibi halka açık alanlarda çalışırken çöp kutusuna atılan bilgi varlıkları bilgi güvenliği ihlali için büyük bir risktir. Saldırganlar, bu bilgileri şantaj amaçlı kullanabilir veya bilgi casusluğu girişiminde bulunabilirler. Bilgi casusluğu sonucunda örneğin, yeni geliştirilen bir ürün hakkında önemli bilgiler rakip firmalara satılabilir.

2.7 HASSAS BİLGİLERDE GÜVENLİK İHLALİNİN YAŞANMASI

Saldırganlar, özellikle profesyonelce hareket ediyorlarsa, sabit sürücülerde, çıkarılabilir depolama ortamlarında, belgelerde veya taşınabilir iş istasyonlarında bulunan hassas bilgilere daha kolay erişebilirler. Ayrıca iletişim kanallarını dinleyebilirler. Bu şekilde bilgiye yetkisiz kişiler tarafından erişilir veya bilgi ifşa edilirse, bu durum ciddi sonuçlara neden olabilir. Her şeyden önce, korunması gereken hassas bilgilerin gizliliklerinin kaybedilmesi; kurumun bağlı olduğu yasaları ihlal etmesine, rekabet gücünü kaybetmesine ve dolayısıyla kurum için maddi zararlara yol açabilir.

2.8 BİLGİ VARLIĞININ KAYBOLMASI VEYA ÇALINMASI

Uzaktan çalışma ortamı, yerleşik iş ortamları kadar güvenli değildir. Dolayısıyla, iş yerlerinin dışına çıkarılan BT cihazları, veri taşıyıcıları, belgeler vb. bilgi varlıkları yolculukta, konaklama esnasında, evde daha kolay kaybolabilir veya çalınabilir. Taşınabilir cihazların kaybolması veya çalınmasından dolayı maddi hasara ek olarak, e-postalar, toplantılardan alınan notlar, adresler, belgeler vb. hassas verilerin yetkisiz kişiler tarafından ele geçirilmesi söz konusu olabilir. Böyle bir durum, itibar ve rekabet gücü kaybına, ayrıca kurumun siber saldırılar için açık hedef haline gelmesine neden olabilir.

2.9 UZAKTAN ÇALIŞMA ESNASINDA ARTAN GÜVENLİK OLAYLARI

Oltalama e-Postaları

Kurum ve ofis dışı alanlarda çalışanlar, oltalama e-postalarında bulunan linkler aracılığıyla yönlendirilen sahte sayfalara daha çok maruz kalırlar. Bu yol ile saldırganlar, çalışanları istedikleri sayfaya yönlendirmekte ve girilen e-posta bilgileri saldırganların eline geçmektedir.

Zararlı Alan Adları

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin araştırmasına göre Koronavirüs salgını ile ilgili 4000 tane alan adının alındığı ve bunların 320'sinin zararlı web siteleri olduğu görülmüştür. Ulusal Siber Olaylara Müdahale Merkezi (USOM) zararlı alan adları listesinde ise 100'den fazla alan adının Koronavirüs ile ilgili sözcükler içerdiği görülmüştür. Bu alan adlarının özellikle Türkiye'de yaşayan kişileri ve kurumları hedef alması önemli bir noktadır. Aynı şekilde yabancı dillerde de dolandırıcılık amacıyla alan adlarının alındığı görülmektedir.

Emotet

Emotet türü kötü amaçlı yazılımların ve siber suçlar uzaktan çalışma ortamlarında ki vaka sayılarının arttığı görülmüştür. Genelde uzaktan yönetim aracı ve truva atı tipinde olan bu zararlıların yanında bazı fidye yazılımlarının da bu şekilde dağıtıldığı araştırmacılar

tarafından doğrulanmıştır. Bu girişimlerden biri de Emotet zararlısını yeniden yaymayı amaçlayan oltalama saldırılarıdır.

Android Casus Yazılımları

Benzer şekilde Koronavirüs salgını döneminde hastalıklarla ilgili istatistiksel bilgiler sağlayan zararlı bir uygulamanın Google Play Store harici kaynaklardan dağıtıldığı görülmüştür. John Hopkins Üniversitesi tarafından hazırlanan Koronavirüs haritasındaki bilgileri kullanıcılara yansıtan uygulama, arka planda SpyMax adlı uzaktan yönetim aracını (RAT) barındırmaktadır. Yapılan detaylı araştırmada benzer şekilde Koronavirüs temalı ve benzer yapıda Android uzaktan yönetim araçları barındıran birden çok uygulama olduğu belirlenmiştir.

Video Konferans Uygulamaları

Uzaktan çalışma modelinde internet üzerinde görüşme ihtiyacının artmasıyla beraber video konferans uygulama kullanımı yaygınlaşmıştır. Bu tür iletişim uygulamalarına yoğun talebi gören saldırganlar, uygulamaları yeniden paketleyerek kötü amaçlı yazılımlarını yaymak için kullanmaktadırlar. Genellikle reklam geliri elde etmek amacıyla yapılan bu saldırılar kullanıcıların gizliliğini tehlikeye atmaktadır.

Diğer Olaylar

Pulse Secure VPN yazılımında bulunan zafiyet kullanılarak birden çok firmaya Revil (Sodinokibi) fidye yazılımının bulaştırılmış olduğu tahmin edilmektedir. Aynı şekilde Palo Alto ve Fortinet VPN yazılımlarında da güncel zafiyetler olduğu görülmektedir. Bu nedenle kullanılan VPN yazılımlarının güncellemelerinin yapılması ve ek güvenlik önlemlerinin alınması gerekmektedir.

2.10 BİLGİ GÜVENLİĞİ FARKINDALIK EKSİKLİĞİ

Kurum ve kuruluşlar genellikle taşınabilir BT sistemleri ve veri taşıyıcılarının güvenliğini sağlayabilmek için yerleşik iş ortamlarında uygulanacak kurumsal düzenlemelere ve teknik güvenlik önlemlerine sahip olabilir. Ancak, gelişen teknoloji ile saldırganlar uzaktan çalışma sürecinde risk seviyesi artmış çalışanların zafiyetlerinden yararlanarak sistemlere sızabilmektedir.

Kurum bünyesinde oluşturulan düzenlemelerin uzaktan çalışma esnasında yeterli seviyede uygulanmaması ve teknolojinin dikkatsiz kullanımı, güvenlik açıklıklarının meydana gelmesine neden olur. Bu zafiyetlere aşağıdaki örnekler verilebilir:

- BT sistemleri ve veri taşıyıcıları gibi bilgi varlıklarının toplu taşıma ile yapılan seyahatlerde gözetimsiz bırakılması,

- Herhangi bir yerde hediye olarak kabul edilen USB bellek kartının kurum bilgisayarına bağlanması ile kötü amaçlı yazılımın bilgisayara bulaşması sonucu hassas bilgilerin çalınmasına, işlenmesine, şifrelenmesine veya kullanılamaz hale gelmesine sebebiyet verilmesi,
- Çalışanların, toplu taşıma araçlarında veya toplantılarda iş süreçleri açısından kritik bilgileri sesli bir şekilde anlatması veya ekranlarına kontrolsüz bir şekilde açması,
- Bilgi güvenliği farkındalığı eksik olan çalışanların, zararlı yazılım bulunduran web sayfalarını ziyaret etmesiyle kurum yerel ağına zararlı yazılımlar bulaştırması.

3 GEREKSİNİMLER

Bu rehberin özel gereksinimleri aşağıda listelenmiştir. Öncelikli olarak, BT Operasyon Ekibi bu gereksinimlerin karşılanmasından sorumludur. Buna ek olarak, Bilgi Güvenliği Birimi tüm stratejik karar süreçlerinde yer almalıdır. Bilgi Güvenliği Birimi taleplerin kurum güvenlik politikasına uygun olarak gerçekleşmesini sağlamak ve bunu doğrulamakla sorumludur.

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

Tablo 2. Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	Bilgi Güvenliği Uzmanı (BGYS)
Diğer Sorumlular	BT Yöneticisi, Üst Yönetici, Çalışan

3.1 1.SEVİYE GEREKSİNİMLER

Uzaktan çalışma modeli için aşağıda listelenen gereksinimler öncelikli olarak ele alınmalıdır.

SNM.7.G1 Uzaktan çalışma ortam seçimi ve kullanımı

Kurum ve kuruluşlar, çalışanlarına uzaktan çalışma ortamlarının nasıl seçilmesi ve uygun şekilde nasıl düzenlenmesi gerektiğiyle ilgili önerilerde bulunmalıdır. Uzaktan çalışma ortamının sahip olması ve olmaması gereken özellikler mutlaka tanımlanmalıdır. Düzenlemeler yapılırken aşağıda verilen hususlara asgari düzeyde dikkat edilmelidir:

- Kurumun sahip olduğu hassas verinin hangi ortamlarda işlenebileceği,
- Çalışanların yetkisiz erişimlere karşı nasıl bir koruma sağlayacağı,
- Sürdürülebilir bir iletişim alt yapısının ve kesintisiz enerji kaynağının olup olmadığı,
- Hangi ortamlarda uzaktan çalışmanın tamamen yasaklanması gerektiği.

SNM.7.G2 Uzaktan çalışma usul ve esasları

Uzaktan çalışmada kurum dışına çıkarılan taşınabilir BT sistemleriyle ilgili düzenlemelerin de mutlaka yapılması gerekmektedir. Bu kapsamda, hangi bilgi varlıklarının kimler tarafından kurum dışına çıkarılabileceği, kurum dışına çıkarılan bu bilgi varlıklarıyla ilgili temel güvenlik gereksinimlerinin ne olacağı belirlenmelidir. Kurum dışına çıkarılan bilgi varlıklarının kim tarafından ne zaman çıkarıldığı kayıt altına alınmalıdır

Çalışanlar dışarıya çıkarılan bilgi varlıklarının ve üzerinde depolanan bilgilerin önemi konusunda mutlaka bilgilendirilmelidir. Ayrıca çalışanın, cihaza özel riskler ve tehditler olabileceğinden dışarıya çıkarılan bilgi varlıklarının sahip olduğu özgün riskler ve bunlara karşı alınması gereken önlemler konusunda da bilgilendirilmesi gerekmektedir. Tüm kullanıcılar uymaları gereken kurallardan, almaları gereken önlemlerden ve gerçekleştirmeleri gereken düzenlemelerden haberdar olmalı ve bu kapsamda çalışanlara düzenli aralıklarla eğitimler verilmelidir.

SNM.7.G3 Güvenlik ve erişim kontrolü

Ofis dışında çalışan personel, uzaktan çalışma alanında oluşabilecek hırsızlık veya erişim koruması ile ilgili önlemler hakkında bilgilendirilmelidir. Çalışma alanı boşaltıldıktan sonra çalışma alanın kapıları kilitlenmeli böylece yetkisiz kişilerin oda içerisinde yer alan belgelere ve BT bileşenlerine fiziksel erişimi önlenmelidir. Çalışanın bu uygulamaya uyumluluğu belirli aralıklarla kontrol edilmelidir.

Çalışmaya kısa süreliğine ara verilip BT sisteminin bulunduğu ortamdan uzaklaşılacaksa BT sisteminin ara yüzüne erişim ancak başarılı bir kimlik doğrulaması sonrası mümkün olacak şekilde ekranın kilitlenmesi sağlanmalıdır.

SNM.7.G4 Ortak çalışma alanlarında harici BT sistem ve alt yapılarının kullanımı

Kurum ve kuruluşlar, ortak kullanım alanlarında bulunan ve üçüncü taraflarca yönetilen harici BT sistem ve altyapılarının kullanımıyla ilgili düzenlemeleri yapmalıdır. Bu tür sistem ve alt yapıların güvenlik koruma seviyesi, kurumun sahip olduğu güvenlik seviyesinden farklı olabileceğinden, kullanıcılar bu sistem ve altyapıların kullanımı ile ilgili düzenlemelere uymalı ve sadece gerekli düzeyde bu hizmetlerden faydalanmalıdır.

Çalışma sonlandırıldığında, çalışma sırasında ortaya çıkan tüm veriler üçüncü taraflara ait bilgi işleme ortamından geri döndürülmez bir şekilde silinmelidir. Kullanıcı adı ve parolanın otomatik olarak tamamlanmasını sağlayan tarayıcı işlevleri kullanılmamalıdır.

3.2 2.SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, uzaktan çalışma ortamını daha güvenli bir seviyeye getirmeyi hedefleyen kurum ve kuruluşlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerinde bulunabilir.

SNM.7.G5 Bilgi varlığının kaybolması veya çalınması

Ofis dışında çalışanlar, BT cihazları veya veri taşıyıcılarını kaybettiği durumlarda ivedilikle kurumlarını bilgilendirmelidirler. Kurumun ilgili prosedüründe bu süreç açık ve net bir şekilde düzenlenmeli ve irtibat noktası belirlenmelidir.

SNM.7.G6 Hassas bilgilerin imha edilmesi

Uzaktan çalışma esnasında kullanılan hassas veriler güvenli bir şekilde silinmeli, imha edilmeli veya anonim hale getirilmelidir. Ömrünü bitiren veya arızalanmış veri taşıma ortamları ve belgeler atılmadan önce, hassas bilgiler içerip içermedikleri kontrol edilmelidir. Mümkünse, hassas bilgiler içeren veya içerdiği düşünülen materyallerin imhası kurum içerisinde gerçekleştirilmelidir.

SNM.7.G7 Uzaktan çalışmayla ilgili yasal düzenlemeler

Uzaktan çalışmaya ilişkin iş hukukunda ve iş güvenliğinde yer alan hükümler gözetilerek kurumun ilgili prosedürleri güncellenmelidir. Ayrıca, çalışanla yapılan veya diğer bağlayıcı sözleşmelerde yer alan ve ileride fikir ayrılığına neden olabilecek tüm hususlar açık bir şekilde düzenlenmelidir.

SNM.7.G8 Uzaktan çalışma ortamı için güvenlik politikası

Uzaktan çalışma modelini uygulayan kurum ve kuruluşlar, modelin ilgili tüm güvenlik gereksinimlerini kapsayan bir politika hazırlamalı ve bu modelde çalışan personele gereksinimleri uygulama zorunluluğu getirmelidirler. Bu politika, kurumun güvenlik gereksinimleri ile ilgili tüm uzman birimler ile koordineli hazırlanmalı ve düzenli olarak güncellenmelidir. Kurum çalışanları mevcut güvenlik politikalarına ek olarak uzaktan çalışmayla ilgili güvenlik politikasından haberdar edilmeli ve bu kapsamda çalışanlara eğitimler verilmelidir.

SNM.7.G9 Taşınabilir bilgi varlıklarının şifrelenmesi

Hassas bilgilere, yetkisiz üçüncü taraflar tarafından erişiminin engellenmesi veya görsel hırsızlığın önlenmesi için prosedür, talimat ve kılavuzlar oluşturulmalıdır. Hassas bilgiler içeren BT sistemleri veya veri taşıyıcıları mümkünse tamamen şifrelenmelidir. Şifreleme anahtarları şifrelenmiş aygıttan ayrı bir ortamda tutulmalıdır.

3.3 3.SEVİYE GEREKSİNİMLER

Aşağıda verilen gereksinimler, standart korumaya ilave olarak daha yüksek korumaya ihtiyaç duyulması halinde dikkat edilmesi gereken konulardır. Parantez içindeki harfler, önlem özelinde hangi temel değerler için öncelikli koruma sağlandığını ifade etmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

SNM.7.G10 Hırsızlık önleme ürünlerinin kullanımı (GBE)

Kurum ve kuruluşların yüksek seviye koruma ihtiyacı mevcutsa, hırsızlık önleme ürünlerini ve güvenli bağlantı yöntemlerini kullanmalıdır. Özellikle bu ürünler ve yöntemler, halka açık alanlarda çalışma yapıldığında veya erişim kontrolü sağlama olanağı bulunmayan

ortamlarda kullanılmalıdır. BT sistemlerinde depolanan bilgilerin değeri genellikle BT sisteminin donanım maliyetlerinden daha yüksektir. Bilgi varlıklarının hırsızlığa karşı korunması için kriterler kurumun süreçlerine uyarlanmalı ve yazılı hale getirilmelidir.

SNM.7.G11 Güvenli olmayan ortamların kullanımı (GE)

Uzaktan çalışma ortam koşullarını ve şartlarını içeren bir düzenleme tanımlanmalıdır. Bu şartlar en azından aşağıdaki maddeleri içermelidir:

- Yetkisiz kişiler tarafından çalışma ortamına erişim,
- Kapalı, kilitlenebilir veya korunan odalar,
- Kesintisiz ve güvenli iletişim,
- Yeterli ve yedekli güç kaynağı.

SNM.7.G12 Bulut bilişim ortam güvenliği (GBE)

Kurum ve kuruluşlar uzaktan çalışma modelleri için hazırladıkları politikalarda bulut bilişim gereksinimleri tanımlamalı ve bu gereksinimlere uygun güvenlik yöntemlerini ayrıntılı bir şekilde belirlemelidir.

SNM: SUNUM

SNM.7.U UZAKTAN ÇALIŞMA

UYGULAMA REHBERİ

SNM.7.U UZAKTAN ÇALIŞMA UYGULAMA

1 AÇIKLAMA

1.1 TANIM

Dizüstü bilgisayarlar, akıllı telefonlar veya video konferans yazılımları gibi giderek yaygınlaşan iletişim araçları sayesinde, çalışanlar neredeyse her yerde işlerini sürdürebilme imkânı bulmaktadır. Teknolojinin gelişmesiyle beraber, işler yalnızca ofis alanlarında değil, ofis dışındaki alanlarda da rahatlıkla yürütülebilmektedir. İster otel odasında veya ulaşım aracında, isterse müşterinin yanında; uzaktan çalışma modeli, mesai saatlerini, çalışma ortamlarını ve görev dağılımına kadar iş hayatımızda yer alan birçok tanımı değiştirmektedir.

Uzaktan çalışma modeli, sadece kurum kararıyla değil aynı zamanda hükümetlerin aldığı kararlardan veya yürürlüğe koyduğu düzenlemelerden ötürü de oluşabilir. Salgın hastalıkların yaşanması, çalışanların uzaktan çalışmaya duydukları istek, trafikte harcanan zamanın azalması, bina giderlerinde tasarruf vb. nedenler uzaktan çalışmayı giderek daha cazip hale getirmekte, bu modelin zamanla daha da yaygınlaşması düşünülmektedir.

2016 yılında 6715 sayılı kanun ile uzaktan çalışmaya ilişkin hükümler 4857 Sayılı İş Kanunu'nun 14. maddesine eklenmiştir. Kanunda "Uzaktan çalışma", "İşçinin işveren tarafından oluşturulan iş organizasyonu kapsamında iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan bir iş ilişkisidir" şeklinde ülkemizde ilk defa resmi olarak tanımı yapılmıştır.

Teknik altyapıları, insan kaynakları, politika ve prosedürleri ile iş yapış şekilleri bakımından uzaktan çalışma modeline uyumluluk gösteren kurum ve kuruluşlar, bu modeli uygulamada daha güvenli ve başarılı bir yerde konumlanırlar. Ayrıca müşteriler, tedarikçiler ve iş ortakları gibi diğer paydaşların da uzaktan çalışma modeline gösterdikleri uyum, bu modelin güvenliğini ve başarısını etkiler. Paydaşların bu modeli uygularken yaşadıkları sorunlar veya iş yapış şeklinden kaynaklanan bir takım doğal kısıtlar, uzaktan çalışma modeline geçiş sürecini olumsuz etkileyebilir. Bazı sektörlerin yapısı gereği bu modeli uygulaması da mümkün olmayabilir.

Uzaktan çalışma modeli ile birlikte iletişim altyapısına olan ihtiyaç artmaktadır, buna paralel olarak karşı karşıya kalınan bilgi güvenliği riskleri de artış göstermektedir. Birçok kurum ve kuruluş uzaktan çalışma için istekli olsa bile, çok azı uygun bilgi güvenlik politikalarına ve altyapısına sahiptir. Kimlik avı dolandırıcılığı, DDOS atakları, hassas

bilginin ifşasına neden saldırılar ya da farklı yöntemlerle mevcut sistem açıklarından faydalanan saldırganlar; işlerini uzaktan sürdüren çalışanları herhangi bir açık ağ üzerinden hedef alabilirler.

Diğer yandan, mevcutta uzaktan çalışma altyapılarına sahip ve bu modeli halihazırda uygulayan kurum ve kuruluşlarda bile uzaktan çalışma aktivitelerindeki ani artış; özellikle telekomünikasyon altyapısının gelişmemiş olduğu bölgelerde, sistem, ağ ve veri güvenliği yönünden bazı olumsuz etkilerin oluşmasına neden olabilir.

İşlerin uzaktan yürütülmesi esnasında tüm bu saldırı ve risklere karşı önlem alınabilmesi, ağların ve verilerin bilgi güvenliği gereksinimlerinin karşılanabilmesi için kuruma ait iş modeli, süreç ve politikaların bu modele uygun olarak hazır hale getirilmesi gerekmektedir.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

İş yerlerindeki verimli çalışmanın, uzaktan çalışma modelinin uygulanması esnasında aynı şekilde sürdürülebilmesi için, uzaktan çalışma ortamının uygun şekilde oluşturulması gerekmektedir. Uzaktan çalışma ortamı oluşturulurken bazı gereksinimler ortaya çıkacaktır. Bu gereksinimlerin karşılanabilmesi için kurum ve kuruluşların öncelikli olarak bu gereksinimleri tanımlamaları gerekir (SNM.7.U1 Uzaktan çalışma ortamının seçimi ve kullanımı). Örneğin, evden çalışma (home office) için oluşturulan ortamların uygunluğu ve güvenliği, kurumsal düzenlemelere ve çalışanın kişisel önlemlerine dayanmaktadır. Bu düzenlemelerle ilgili detaylar, “SNM.7.U2 Uzaktan çalışma usul ve esasları” ve “SNM.7.U8 Uzaktan çalışma ortamı için güvenlik politikası” başlıklarında ele alınmıştır.

Uygulama

İş ve ofis alanlarının dışındaki tüm çalışmalarda, hangi bilgilerin kurum/kuruluş dışında kullanılabileceğine dair politika, prosedür ve talimatların oluşturulması gerekmektedir (SNM.7.U2 Uzaktan çalışma usul ve esasları). Bununla birlikte, çalışanların kurumsal bilgilere dışarıdan erişim koşulları da açık bir şekilde yazılı olarak düzenlenmelidir.

İşletim

Uzaktan çalışma modelinde çalışanların kullandığı BT sistemlerin (ör. bilgisayar, telefon, tablet vs.) yanı sıra, bu çalışma modeli esnasında oluşturulan ve paylaşılan verilerin de dikkatli bir şekilde ele alınması gerekir. Bu kapsamda, işveren tarafından belirlenen çalışma ortamına ilişkin düzenlemelere uyulmalı ve çalışma materyalleri güvenli şekilde kullanılmalıdır (SNM.7.U3 Güvenlik ve erişim kontrolü ile SNM.7.U4 Ortak çalışma alanlarında harici BT sistem ve alt yapılarının kullanımı).

Kurum veya kuruluşların yüksek seviye koruma ihtiyacı mevcutsa, hırsızlık önleme sistemi (SNM.7.U10 Hırsızlığa karşı koruma ürünlerinin kullanımı) veya güvenli iletişim bağlantıları (SNM.7.U11 Güvenli olmayan ortamların kullanımı) gibi önlemler de uygulanmalıdır.

Kullanım Dışı Bırakma

Uzaktan çalışma modelinde kullanılan verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslara, normal çalışma modelindekinden daha çok dikkat edilmesi önerilmektedir (SNM.7.U6 Hassas bilgilerin imha edilmesi).

2 UYGULAMALAR

Aşağıda yer alan maddeler, uzaktan çalışma modeline özel uygulama maddeleridir. Uzaktan çalışma modelini uygulayan kurum, kuruluşlar ve çalışanlar için dikkat edilmesi gereken hususlar, alınması gereken önlemler ve en iyi uygulama örnekleri aşağıda belirtilmiştir.

2.1 1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınmalıdır.

SNM.7.U1 Uzaktan çalışma ortamının seçimi ve kullanımı

BT donanımlarının boyutlarının fiziksel olarak küçülmesi ve iletişim teknolojilerinde gelişmeler sayesinde, günümüzde işler neredeyse her yerde yürütülebilir hale gelmiştir. Bu bağlamda, zamandan ve mekândan bağımsız olarak çalışma olanağı sunan uzaktan çalışma modeli kurum ve kuruluşların gündemine girmiştir. Bu model sayesinde çalışanlar, ister bir otel odasında veya evde, isterse müşterinin yanında olsun; istediği vakit veya gerektiği durumda ofis ortamında yapabileceği bütün işleri uzaktan yürütebilmektedir.

Bu çalışma ve iş birliği modelinde, çalışma ortamı gereksinimleri genelde net değildir. Ayrıca ofis çalışma modelinden farklı gereksinimler de gündeme gelebilmektedir. Etkili ve güvenli uzaktan çalışma ortamının, çalışanlar tarafından oluşturulması beklenmektedir. Ancak, bu ortam çalışanlar tarafından sınırlı ölçüde oluşturulabilir veya mevcut durumu ile beklenilen etkinlik ve güvenlik seviyesini sağlayamayabilir. Bu nedenle kurum ve kuruluşlar, kullanıcının uzaktan çalışma ortamının uygunluğunu kontrol etmeli ve değerlendirmelidir. Değerlendirme süreci yazılı prosedürlerle desteklenmelidir.

Uzaktan çalışma modelinin uygulanabilir olmadığı durumlar aşağıda listeleniştir:

- Kurum ve kuruluşun sahip olduğu hassas verilerin iş alanları dışında işlenmesinin ciddi riskler ortaya çıkardığı durumlarda,

- Çalışmaların yetkisizi üçüncü taraflarca rahatlıkla görülebilmesi ve dolayısıyla bunun görsel hırsızlığa neden olabileceği durumlarda (ör. Bilgisayar ekranının seyahat halinde yan veya arka koltuktan görülebilmesi),
- Enerji/güç kaynağı ve/veya ağ bağlantısının yetersiz veya hiç olmadığı durumlarda,
- BT aygıtlarının çalıştırılmasının yasak olduğu veya uygun olmadığı durumlarda (ör. Uçakta veya askeri alanlarda).

Uzaktan çalışma modeli uygulanırken dikkat edilmesi gereken durumlar aşağıda listelenmiştir:

- Birçok BT ekipmanı yüksekten düşme nedeniyle zarar görebildiğinden veya kullanılamaz hale gelebildiğinden, kullanılan cihazlar dayanıklı bir zemin üzerine sabitlenmelidir.
- Sessiz ve uygun bir çalışma ortamı oluşturulmalıdır.
- Çalışma ortamı yeterince aydınlık olmalı sadece monitör ışığı ile uzun süre çalışılmamalıdır.
- Görsel hırsızlığı engelleme amacıyla ekranlar, üçüncü taraflarca görülemeyecek şekilde konumlandırılmalıdır. Görsel hırsızların bilgisayar ekranlarına yandan bakarak bilgi çalmasını önleyen gizlilik filtreleri veya ekran folyoları tercih edilebilir.
- Çalışma ortamında kullanılan iklimlendirme sistemleri, BT sistem ve ekipmanlarını olumsuz etkilemeyecek şekilde ayarlanmalıdır. Örneğin ortam çok nemli, çok soğuk veya çok sıcak olmamalıdır. Çalışanlar, uzaktan çalışma esnasında ortam iklimlendirme koşullarını tam anlamıyla sağlayamayabilir veya bundan bilinçli olarak kaçınabilir. Bu sebeple, çalışanlara tahsis edilecek BT sistemleri ve çevre ekipmanlar için kullanım talimatları ve kılavuzları oluşturularak çalışanlar bu konuda bilgilendirilmelidir.
- BT varlıklarıyla ilgili çalınma ve kaybolma riskinin yüksek olduğu durumlarda hırsızlık önleme ürünleri kullanılmalıdır (SNM.7.U10 Hırsızlığa karşı koruma ürünlerinin kullanımı). Çalışma ortamının bu ürünleri kullanmak için elverişli olduğuna dikkat edilmelidir. (ör. taşınabilir bilgisayarın masa gibi sabit bir nesneye kilitlenmesini sağlayan düzenekler gibi.)
- Çalışma ortamında bulunan kapı ve pencereler, kişi odadan ayrıldığında kapatılmalı ve kilitlenmelidir. Bu durum özellikle otel veya toplantı odaları için dikkat edilmesi gereken bir husustur.
- Uzaktan çalışmanın yürütüldüğü (otel odası veya müşteri ofisi gibi) yabancı ortamlarda yangın veya başka bir acil durum meydana gelmesi durumunda nasıl davranılması ve nelere dikkat edilmesi (kaçış yolları, alarm zili vs.) gerektiği ile ilgili bilgi notları ve uyarılar dikkate alınmalı, gerekirse yetkili personelden bu konuda bilgi talep edilmelidir.

SNM.7.U2 Uzaktan çalışma usul ve esasları

Uzaktan çalışma modelinde, (dosyalar, diskler, veri taşıyıcıları, bilgisayarlar gibi) hangi bilgi varlıklarının iş yerleri dışına çıkarılabileceğine ve hangi verilerin iş yeri dışında işlenebileceğine dair düzenlemelerin açık bir şekilde oluşturulması ve bunlara göre koruyucu önlemlerin belirlenmesi gerekmektedir.

Dışarı çıkarılan bilgi varlıkları, kurum binasındakilerine göre daha fazla riske maruz kalır. Bu nedenle, uzaktan çalışma esnasında aşağıda belirtilen önlem ve düzenlemelere dikkat edilmelidir:

- Uzaktan çalışanlar, hangi bilgiler veya veriler üzerinde uzaktan çalışma yapabileceği konusunda bilgilendirilmelidir. Veriler sınıflandırılarak, kısıtlamalar kullanıcılar için şeffaf hale getirilmelidir.
- Kuruma ait hassas bilgiler gerekli güvenlik önlemleri alınmış olan kuruma ait BT sistemlerinde işlenmelidir.
- Hassas bilgiler içeren taşınabilir cihazlar ve veri taşıyıcıları gibi BT sistemleri mümkünse tamamen şifrelenmelidir. İlgili BT sistemleri ek uygulamalar gerekmeden şifrelenmiş olarak kullanılabiliyorsa, bu özelliğin her daim açık halde tutulması önerilir.
- Uzaktan çalışma esnasında kullanılan BT sistemlerinde gizlilik seviyesi düşük veriler bulunsa dahi şifreleme özelliğinin her zaman açık olması önerilir.
- Yüksek düzeyde koruma gerektiren kuruma ait (teklifler, tasarım verileri, hizmete özel bilgiler gibi) hassas veriler taşınabilir BT cihazlarında her zaman şifrelenmiş şekilde saklanmalıdır.
- Uzaktan çalışan personelin, kurumun hangi yerel verilerine uzaktan erişip erişemeyeceği açık bir şekilde belirlenmelidir. Ayrıca, uzaktan erişim esnasında kullanılan iletişim altyapısı gerekli güvenlik önlemleri alınarak korunmalıdır.
- Uzaktan çalışma esnasında kullanılan BT sistemlerinin, (sosyal medya erişimi, bilgisayar oyunu oynamak, özel işlerin yapılması, e-ticaret gibi) şahsi amaçlar için kullanılıp kullanılamayacağı açık bir şekilde belirlenmelidir. Şahsi amaçlı kullanıma izin verilmesinin saldırı yüzeyini artıracağı göz önünde bulundurulmalıdır.
- Kullanıcıların uzaktan çalışma esnasında kullandıkları BT sistemleri ve donanımları, çalınmaya veya kaybolmaya karşı güvenli hale getirilmelidir. Ayrıca, cihazların uzun ömürlü olmasını sağlayacak kullanım kılavuzları ve bakım talimatları oluşturulmalıdır. Bu talimat ve kılavuzlarda, BT ekipmanları çok yüksek veya çok düşük sıcaklıklara duyarlı oldukları için ekipmanların uygun şartlarda kullanılmasına; manyetik alan ve sıvı teması gibi tehditlere karşı cihazların korunması gerektiğine dair maddeler yer alabilir. Olumsuz koşullar BT ekipmanlarına maddi zarar verebileceği gibi kopyası veya

yedeği bulunmayan kurumsal verilerin geri dönülmez bir şekilde bozulmasına da neden olabilir.

- Uzak kullanıcıların kişisel cihazları ile kurum ağına bağlanması gerektiği durumlarda, şifrelenmiş güvenli bağlantı oluşturulmadan önce, bağlantı için kullanılacak cihazda anlık güvenlik denetimleri yapabilen Sanal Özel Ağ (VPN) uygulamaları tercih edilmelidir. Bu VPN uygulamaları, kullanıcının kimlik doğrulamasını ve yetkilendirmesini yaptığı gibi kullanılan cihazın (güncel virüsten koruma yazılımının yüklü olup olmadığı, işletim sisteminin güncel olup olmadığı gibi) asgari güvenlik gereksinimlerini sağlayıp sağlamadığını da kontrol edebilmelidir.
- Uzaktan çalışanların sayısı arttıkça, kurumların (SSL VPN gibi) güvenli bağlantı trafiklerinde ciddi artışlar yaşanabilir. Bundan dolayı güvenli bağlantı lisans sayıları ve iletişim hattının bu talebi karşılayabilecek azami kapasitesi gözden geçirilmelidir.
- Uzaktan erişim ile kurum yerel ağına bağlanacak kullanıcılara, sadece görevini icra edebilecek asgari düzeyde erişim yetkisi tanımlanmalıdır. Özellikle hassas verilerin saklandığı veri tabanları ve yedekleme sistemi gibi veri kaynaklarına uzaktan erişim yapacak kullanıcıların minimum yetki prensibine aykırı erişim yetkileri mutlaka sınırlandırılmalıdır. Ayrıca bu gibi ayrıcalıklı hesaplar için log ve bildirim üreten denetim mekanizmaları aktif hale getirilerek diğer sistem yöneticileri ve/veya bilgi güvenliği birimleri yapılan işlemlerden haberdar edilmelidir.
- Uzaktan çalışmada kullanılan taşınabilir BT sistemlerinin ve veri taşıyıcılarının yönetimi, bakımı ve devredilmesi hakkında düzenlemeler oluşturulmalıdır.
- Cihazı kullanan personelin değişmesi durumunda, cihaz üzerinden bulunan (MAC adresi ile yetkilendirme gibi) tüm donanımsal yetkilendirmeler ve cihaz üzerinde saklanan parolalar güvenli şekilde kaldırılmalıdır.
- Uzaktan çalışma modelinde BT sistemleri ve veri ortamları her zaman güvenli olarak muhafaza edilmelidir. İş seyahatlerinde özellikle, toplu ulaşımla yapılan seyahatlerde bu cihazlar araçlarda, dinlenme tesislerinde, lobi gibi kamuya açık alanlarda denetimsiz bir şekilde bırakılmamalı ve unutulmaması için özellikle dikkat edilmelidir.
- Taşınabilir bilgisayarlar, tabletler veya akıllı telefonlar gibi BT sistemleri ve bunlarda kullanılan uygulamalar, biyometrik güvenlik denetimleri, PIN veya parolalarla güvence altına alınmalıdır.
- Güvenli uzak bağlantı için kullanılacak parolalar kurum politika, prosedür ve uygulamalarına uygun olacak şekilde belirlenmelidir. Parolaların en az 12 haneli, büyük harf, küçük harf, rakam ve özel karakter içerecek şekilde oluşturulması önerilmektedir. Bu parolalar güvenli bir şekilde saklanmalıdır.

- Kaba kuvvet (brute force) ile parola tahmin saldırılarına karşı korunmak için CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) adı verilen ve robot/insan ayrımını yapan doğrulama sisteminin kullanılması etkin bir tedbir olarak öne çıkmaktadır.
- Kurum dışında hangi BT cihazının ne zaman ve kim tarafından kullanıldığı kayıt altına alınmalıdır.
- Kurum ve kuruluşlar, risk yaklaşımına uzaktan çalışma modelini de dahil etmelidir. Salgın hastalıklar ve benzeri durumlar için iş sürekliliği planları tekrar gözden geçilmeli ve bu durumlar için de mutlaka uyarlanmalıdır.
- Uzaktan çalışma modelinde kullanılan verinin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yazılı olarak düzenlenmelidir (SNM.7.U6 Hassas bilgilerin imha edilmesi).

Ek olarak, kurum ve kuruluş dışında kullanılan taşınabilir BT sistemlerinin güvenli kullanımı hakkında kullanıcılar için kısa ve net talimatlar, kılavuzlar ve mümkünse görsel medyalar hazırlanmalıdır.

Taşınabilir BT sistemleri ofis dışı alanlarda gözetimsiz bırakılmamalıdır. Bu cihazların araçta bırakılması gerektiği durumlarda, dışarıdan görülemeyecek şekilde saklanmasına dikkat edilmelidir. Dışarıdan görünebilen (taşınabiliri bilgisayarlar, tabletler ve akıllı telefonlar gibi) BT ekipmanları, potansiyel hırsızların dikkatini çekebileceğinden üzeri örtülmüş ve kilitlenmiş bir şekilde bagajda saklanmalıdır.

Otel odaları gibi yabancı ortamlarda, taşınabilir BT sistemleri korunmasız halde bırakılmamalı, tüm parola koruma mekanizmalarının etkin olduğundan emin olunmalıdır. Mümkünse, BT ekipmanı, çalınmaya ve yetkisiz erişime karşı dolaba veya oda kasasına kilitlenmelidir.

Taşınabilir BT cihazlarının kurum dışına çıkarılması

Veri taşıyıcılarının ve BT ekipmanlarının kurum dışına çıkarılmalarıyla ilgili prosedürler açık ve net bir dille düzenlenmelidir. Prosedürler oluşturulurken dikkat edilmesi gereken hususlar aşağı belirtilmiştir:

- Hangi BT ekipmanları ve veri taşıyıcılarının kurum/kuruluş dışına çıkarılabileceği,
- BT ekipmanlarını ve veri taşıyıcılarını kurum dışına kimlerin çıkartabileceği,
- BT ekipmanlarının dışarı çıkartılması sürecinde (virüsten koruma yazılımının yüklü olup olmadığı, ekipmanın tamamen veya hassas verilerin kısmen şifrelenip şifrelenmediği gibi) hangi temel güvenlik kontrollerinin yapılıp yapılmayacağı gibi hususlar net bir şekilde belirlenmelidir.

Kurum dışına çıkarılan taşınabilir BT sistemleri ve ekipmanlarına uygulanacak güvenlik önlemlerinin türü ve kapsamı; cihazlarda bulunan verilerin hassasiyetine ve (disk şifreleme gibi) cihazın sağladığı güvenlik özelliklerine bağlıdır.

BT ekipmanlarının dışarıya çıkarılma sürecinde, yukarıda bahsedilen güvenlik kontrollerine, usul ve esaslara uyulup uyulmadığı rastgele örnekleme ile denetlenmelidir. Rastgele örnekleme yöntemiyle yapılan bu denetim, dışarı çıkarılan BT ekipmanlarının kontrolünün BT süreçleriyle doğrudan ilgisi olmayan güvenlik görevlileri tarafından yapıldığı kurum ve kuruluşlarda ayrıca önem taşımaktadır.

Kullanıcı farkındalığının artırılması

Çalışanlar, ofis dışına çıkardıkları BT ekipmanları üzerinde depolanan bilgilerin hassasiyeti ve önemi konusunda bilgilendirilmelidir. Üzerinde veri barındıran (taşınabilir bilgisayarlar, farklı işletim sistemine sahip tabletler, akıllı cihazlar veya kuruma has özel cihazlar gibi) çok çeşitli BT ekipmanları olabilmektedir. Bu sebeple çalışanlara kullandıkları BT ekipmanlarına özel güvenlik riskleri ve bunlara karşı alınabilecek önlemler hakkında bilgi verilmelidir.

Uzaktan çalışma esnasında çalışanların üçüncü taraf kişilerce duyulma veya çalışmalarının görülme ihtimali varsa, çalışanlar kurum için hassas bilgileri konuşarak veya yazarak paylaşmamaları konusunda bilgilendirilmelidir. Ayrıca, uzaktan çalışma farklı paydaşlarla yürütülecekse birlikte çalışma yapılacak kişilerin kimliği hassas bilgiler paylaşılmadan önce mutlaka sorgulanmalıdır.

SNM.7.U3 Güvenlik ve erişim kontrolü

Uzaktan çalışmanın yürütüldüğü odanın dışa bakan pencereleri ve (balkon, teras gibi) dışa açılan kapıları oda kullanılmadığı zamanlarda kapalı tutulmalıdır. Binanın zemin katı ve en üst katlarda bulunan açık pencereler ve kapılar, çalışma saatleri içerisinde dahi hırsızlar için ideal giriş noktaları olarak kullanılabilir.

Çalışma alanından ayrılırken kapılar kilitlenmeli böylece yetkisiz kişilerin oda içerisinde yer alan belgelere ve BT bileşenlerine erişimi önlenmelidir. Özellikle halka açık alanlarda bulunan veya giriş çıkış kontrolü sağlanamayan (paylaşmalı çalışma alanları gibi) ortamlarda kullanılan odaların kilitlenmesi önemlidir.

Oda veya çalışma alanlarında acil çıkış kapıları bulunabilir. Acil çıkış kapılarının, sadece içeride bulunan kişiler tarafından açılması mümkün olmalıdır. Oda ile dış ortam arasında doğrudan bağlantı kuran bu tür kapıların, dışarıdan içeriye yetkisiz erişimleri önleyecek şekilde düzenlenmeleri gerekir.

Toplantı, eğitim salonu ve etkinlik alanlarında yer alan (belge ve BT bileşenlerini gibi) bilgi varlıklarını korumak zor olabilir. Bu nedenle toplantılar ve etkinlikler sonrasında söz konusu alanları kontrol edilmelidir.

Açıkta belgeler ve veri taşıyıcılar gibi korumaya ihtiyaç duyulan herhangi bir bilgi varlığı yoksa ve odadaki BT bileşenlerine yetkisiz erişim mümkün değilse, kapıların kilitlenmesine gerek olmayabilir.

Uzaktan çalışma esnasında kullanılan ortamda bulunan BT sistemlerine yetkisiz erişim kullanıcı kimlik doğrulaması ile engellenebiliyorsa kapıların kilitlenmesine gerek olmayabilir. Ancak, saldırganın erişim bilgilerini ele geçirmesi durumunda bu koruma etkisiz hale gelebilir.

BT sistemleri kapalı olarak tutulduğu durumlarda ise, bilgisayarın önyükleme işlemi esnasında bir parola girilmesi zorunlu tutuluyor veya BT sistemi akıllı kart veya dongle gibi ek güvenlik mekanizmaları kullanılarak başlatılabiliyorsa kapıları kilitlemeye gerek olmayabilir.

Düzenli çalışma alanı

Gün içinde gerçekleşen iş görüşmeleri ve bilgisayar başında yapılan işlemler sonucunda kağıtlara alınan notlar çalışma masasında kontrolsüz olarak bırakılabilmekte, hatırlatıcı olması için bazı bilgiler yapışkan notlar ile etrafa yapıştırılabilmektedir. Hassas bilgilerin kontrolsüz bir şekilde çalışma ortamında bırakılmadığından emin olmak için çalışma ortamının temiz ve düzenli tutulması önerilmektedir. Karışık ve dağınık bir çalışma masasında hangi önemli bilgilerin bulunduğundan tam olarak emin olunamaz. Bu sebeple çalışanlar uzaktan çalışma sürecinde de çalışma ortamlarını düzenli tutmaları konusunda bilgilendirilmelidir. İhtiyaç duyulmayan malzeme ve ekipmanlar çalışma alanlarından uzaklaştırılmalıdır.

Çalışanlar, kurumsal bilgi varlıklarına yetkisiz kişilerin erişmesine imkân vermemeli, bilgi varlıklarının erişilebilirliği, gizliliği ve bütünlüğünü olumsuz etkileyebilecek tutum ve davranışlardan kaçınmalıdır. Uzaktan çalışan personel, çalışma süresince ve sonrasında hassas bilgilere yetkisiz kişiler tarafından serbestçe erişilmediğinden emin olmalıdır.

Çalışma saatleri boyunca kısa bir süre için odadan ayrılırken:

- Mümkünse oda kilitlenmeli,
- BT sistemlerine erişim, ancak başarılı bir kimlik doğrulaması ve yetkilendirmesinden sonra mümkün olacak şekilde ayarlanmalıdır.

Çalışanlar (uzun süreli toplantılar, iş gezileri, tatil ve benzeri nedenlerden dolayı) uzun bir süre boyunca çalıştıkları ortamdan uzaklaşmayı planlıyorsa hassas verileri barındıran BT

bileşenlerini ve belgeleri açık kalmayacak şekilde kilitli bir şekilde muhafaza etmelidir. Bunun için çalışanların uzaktan çalıştığı alanlarda, her türlü bilgi varlığını saklayabileceği kilitli bir dolaba ihtiyacı vardır.

Parolalar asla görünür tutulmamalı, monitör, masa veya kilitsiz çekmece gibi tahmin edilmesi kolay yerlerde hassas bilgi içeren notlar bulundurmamalıdır.

SNM.7.U4 Ortak çalışma alanlarında harici BT sistem ve alt yapılarının kullanımı

Uzaktan çalışma esnasında, kurumun elektronik bilgi ve belgelerine genellikle harici sistemler kullanılarak erişilir. Bunun için üçüncü tarafa ait BT ve iletişim alt yapılarını kullanmak çoğu zaman daha kolay ve daha cazip hizmet edinme seçeneği olarak karşımıza çıkar. Örnek vermek gerekirse:

- İnternet altyapısı sağlayan restoran veya bir kafeden,
- Ziyaret edilen farklı bir kurum/kuruluşa ait çalışma ofisinden,
- Otelde, bir vasıtayla seyahat ederken veya havaalanlarında bulunan bekleme salonlarında bulunan kablosuz ağları kullanarak bağlantı sağlamak gibi.

Bu alanlardaki BT sistemlerinin ve iletişim alt yapısının üçüncü taraf kişilerce yönetildiğinin farkında olunması ve buna karşı ek güvenlik önlemlerinin alınması gerekmektedir. Bundan dolayı, harici BT ortamının güvenlik seviyesinin bilinmediği durumlarda, ortam güvenlik seviyesinin en düşük seviyede olduğu kabul edilerek hareket edilmelidir. Ayrıca tüm çalışanlar, genel kullanıma açık harici BT sistemlerinin ve alt yapılarının daha yüksek güvenlik riskleri taşıdığı konusunda bilgi sahibi olmalıdırlar. Bulunulan ortam güvenlik seviyesinin mükemmel ve profesyonelce olduğu izlenimi verse bile, bu durum yanıltıcı olabilir.

Bu nedenle çalışanlar, yönetimi üçüncü taraflara ait BT sistem ve iletişim alt yapılarını kullanmadan önce aşağıdaki önerileri dikkate almalıdır:

- Kurumun, uzaktan çalışma modeli için oluşturulan erişim politikalarında, üçüncü taraflarca yönetilen BT sistemlerinin ve iletişim alt yapılarının hangi şartlarda, hangi düzeyde ve hangi bilgi varlıklarına erişim için kullanılabileceği mutlaka belirlenmelidir.
- Kullanılan harici BT sisteminde alınan güvenlik önlemleri hakkında bilgi sahibi olunmalıdır. Ancak, bu çoğu zaman mümkün olmayabilir.
- Kullanıcılar, üçüncü taraf BT sistemlerinin kullanımı ile ilgili yönergelere ve talimatlara dikkat etmelidir. Sağlanan tüm hizmetlerin kullanımı yerine, bilinçli ve sadece yeteri kadar bu hizmetlerden faydalanılmalıdır.
- Çalışma sonlandırıldığında, çalışma sırasında oluşan tüm veriler üçüncü taraf elektronik ortamından kalıcı bir şekilde silinmelidir. Fakat çoğu işletim sistemi birçok

yerde geçici veri oluşturduğundan bu silme işlemi verilerin genellikle tam anlamıyla silindiğini garanti etmeyebilir. Ayrıca, üçüncü taraf BT sistemlerinin erişim haklarının, bu geçici verilerin silinmesine izin vermemesi de söz konusu olabilir. Böyle bir durumda hassas bilgilerin üçüncü taraf elektronik ortamında kalması söz konusu olacağından kullanımdan önce bu durum kontrol edilmelidir.

- Hiçbir koşulda, kullanıcı adlarının ve parolaların otomatik olarak tamamlanması için tarayıcının bu bilgileri saklamasına izin verilmemelidir. Bu şekilde sonraki kullanıcıların bu kullanıcı adı altında oturum açmasının önüne geçilecektir.

2.2 2. SEVİYE UYGULAMALAR

Uzaktan çalışma modelini daha güvenli bir seviyeye getirmeyi hedefleyen kurum ve kuruluşlar 1.seviye gereksinimler ilave olarak aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

SNM.7.U5 Bilgi varlığının kaybolması veya çalınması

Kuruma ait (BT ekipmanları ve belgeler gibi) bilgi varlıklarından herhangi birisi kaybolur veya çalınırsa, çalışanların bu durumu raporlayabileceği irtibat noktası ve iletişim kanalı önceden belirlenmiş olmalıdır. Dizüstü bilgisayarlar, akıllı telefonlar, tabletler, PDA'lar USB bellekler ve benzeri BT ekipmanlarında hassas veriler bulunabilmektedir. Eğer bu tür hassas verilerin barındırıldığı bir bilgi varlığı kaybolur veya çalınırsa acilen aşağıdaki önlemler alınmalıdır:

- Kaybolan veya çalınan sistemin parola ve erişim yetkileri gibi tüm bilgileri acilen değiştirilmelidir.
- Gizli olarak sınıflandırılan bilgiler çalınır veya kaybolursa bu durumdan etkilenebilecek tüm birim ve bölümler gerekli işlemleri yapmaları için bilgilendirilmelidir.

Taşınabilir cihazlar kaybolduktan veya çalındıktan hemen sonra gerekli önlemler alınabilir olmalıdır. Bu cihazlar uzaktan engellenebilir, silinebilir ve yeri tespit edilebilir şekilde yapılandırılmalıdır.

Kaybolan BT sistemleri bulunursa, olası tahriplere karşı mutlaka ön incelemesi yapılmalıdır. Bu cihazların vidalarının açılıp açılmadığı, fiziksel bir değişikliğe maruz kalıp kalmadığı veya ağırlığında ilk satın alındığı duruma göre herhangi bir değişiklik olup olmadığı kontrol edilmelidir. Eğer en ufak bir şüphe bile oluşursa cihazlar imha prosedürüne uygun olarak kullanım dışı bırakılmalıdır.

SNM.7.U6 Hassas bilgilerin imha edilmesi

Kurum ve kuruluşların yerleşik çalışma modeline uygun olarak hazırlamış oldukları imha prosedürleri, uzaktan çalışma modeli için tam uygulanabilir olmayabilir. Bu nedenle,

hassas bilgiler içeren bilgi varlıklarının, uzaktan çalışma sürecinde kullanım dışına ayırma ve imha edilmesiyle ilgili yöntem ve politikalar belirlenmeli, bunlar için özel talimat ve kılavuzlar hazırlanmalıdır. Ayrıca bu konuda çalışanlar bilgilendirilmelidir.

Uzaktan çalışma süresince, (yazıcıdan alınan çıktılar, DVD'ler, USB bellekler, SD hafıza kartları, harici diskler veya hafızasında bilgi tutan özel toner kartuşları gibi) bilgi varlıkları daha fazla kullanılmayacakları durumda üzerlerine kaydedilmiş olan veriler hiçbir şekilde geri döndürülemeyecek şekilde imha edilmelidir. Üzerinde hassas bilgi saklanmış ancak kullanımı başka bir amaç için devam edecek olan BT ekipmanlarını tekrar kullanıma hazırlamak için üzerindeki veriler geri döndürülemeyecek şekilde silinmelidir. Çalışmayan veya artık kullanımına ihtiyaç duyulmayan (CD, DVD, belgeler gibi) bilgi varlıkları ise fiziksel olarak imha edilmelidir.

Hassas bilgiler içeren bilgi varlıklarının imha edilmesi toplu olarak yapılacak ise varlıkların toplanma ve imha edilme süresi boyunca yetkisiz erişime karşı korunmasına dikkat edilmelidir. Buna ek olarak, bilgi varlıklarının imha edilmesi (anlaşmalı bir firma gibi) dış kaynak kullanılarak yapılacaksa, bu süreç esnasında hangi yöntemlerin uygulandığına ve verinin kimler tarafından imha edildiğine dikkat edilmelidir. Ayrıca, bu sürecin güvenli bir şekilde tamamlandığı denetlenmelidir.

Seyahat esnasında bilgi varlıklarının imha edilmesi

Seyahat halindeyken dahi bazı bilgi varlıklarının çeşitli nedenlerden dolayı imha edilmesi gerekebilir. Kullanılmayan veri ortamlarını ve belgeleri imha etmeden önce, korunmaya değer bilgiler içerip içermedikleri kontrol edilmelidir. Eğer korunmaya değer bilgiler mevcutsa, bilgi varlığı muhafaza edilmelidir. Veri ortamı arızalanmış olsa bile, BT uzmanları bu ortamlardan değerli bilgileri kurtarabilir.

SNM.7.U7 Uzaktan çalışmayla ilgili yasal düzenlemeler

Kurum ve kuruluşlar, uzaktan çalışma esasları ile ilgili çeşitli iş kanunlarını ve iş güvenliği yönetmeliklerini gözetmek ve bunlara uymakla yükümlüdür. Uzaktan çalışmanın uygulanması esnasında iş veren ile çalışan arasında tartışma oluşturabilecek konular, kurum/kuruluş sözleşmelerinde, çalışan ile işveren arasında yapılan özel iş sözleşmelerinde veya ek sözleşmeler yoluyla açıklığa kavuşturulmalıdır. Aşağıda belirtilen hususlar yapılacak bu sözleşmelerde dikkate alınmalıdır.

- Uzaktan çalışmaya gönüllü katılım,
- Uzaktan çalışmanın başlangıcı ve bitişi,
- Çalışma saatleri, erişilebilirlik durumu ve fazla mesai süreleri,
- Uzaktan çalışma esnasında çalışanın bulunabileceği coğrafi sınırlar,

- Performans ölçümünde kullanılacak yöntemler,
- Çalışanın kurum ve müşteriler arasındaki seyahat masrafları,
- Elektrik, haberleşme, ısıtma, su, yemek ve kira masrafları,
- Hırsızlık, BT ekipmanlarına zarar gelmesi, iş kazası ve meslek hastalığı durumundaki yükümlülükler.

SNM.7.U8 Uzaktan çalışma ortamı için güvenlik politikası

Uzaktan çalışma esnasında kullanılan BT sistemleri ve iletişim alt yapısının güvenli kullanımına dair bir güvenlik politikası oluşturulmalı ve bu politikada aşağıdaki hususlar dikkate alınmalıdır.

Çalışma saatlerinin düzenlemesi: Kurum içinde ve dışında çalışılacak saat aralıkları düzenlenmeli, çalışanın erişilebilir olacağı zaman aralıkları da belirlenmelidir.

Yanıt süreleri: Uzaktan çalışanların iş süreçleriyle ilgili güncel bilgilere hangi aralıklarla erişmesi gerektiği (örneğin e-postalarını ne sıklıkla okuduğu) ve bunlara ne kadar sürede cevap vermeleri gerektiği belirlenmelidir.

Temsil yetkisi: Uzaktan çalışanların yürüttükleri mevcut işleri takip eden ve bu işlerin raporlanmasında sorumlu bir yönetici atanmalıdır. Böylece işler aksaklık yaşanmadan kısa süre içinde devralınabilir ve sürdürülebilir olacaktır. Uzaktan çalışanlar işlerle ilgili yaptıkları çalışmaları ve sonuçlarını açık bir şekilde raporlamalıdır. Uzaktan çalışanlar ve yöneticilerin düzenli aralıklarla toplantı yapması önerilir. Ayrıca, beklenmedik bir personel değişikliği durumunda yöneticinin BT sistemleri ve uygulamalardaki verilere nasıl erişebileceği veya mevcut belgelerin taşınabilir iş istasyonunda nasıl görüntülenebileceği de düzenlenmelidir. Bu süreç mutlaka test edilmeli ve uzak çalışan ve yöneticisi tarafından değerlendirilmelidir.

Hassas bilgilerin yönetimi: Uzaktan çalışma esnasında, bilgiler hem (kâğıt belgeler gibi) fiziksel ortamlarda hem de (veri taşıyıcılar ve iş istasyonları gibi) elektronik ortamlarda işlenebilir. Bilgi hangi biçimde bulunursa bulunsun mutlaka yetkisiz erişimlere ve diğer güvenlik risklerine karşı korunmalıdır. Önemli bilgiler tüm yaşam döngüsü boyunca yeterli güvenlik önlemleri alınarak korunmalıdır.

Raporlama: Uzaktan çalışanlar, bilgi güvenliği ihlaliyle ilgili meydana gelebilecek herhangi bir olayı önceden belirlenmiş bir kişi veya bölüme anında bildirmekle yükümlü kılınmalıdır.

Çalışma ekipmanı: Uzaktan çalışma esnasında hangi BT ekipmanların ve uygulamaların çalışanlar tarafından kullanılabileceği ve hangilerinin kullanılmaması gerektiği belirlenmelidir. Ayrıca, kullanımına ihtiyaç olmayacaksa uzaktan çalışma esnasında DVD veya USB bellek gibi veri taşıyıcıların kullanımı yasaklanabilir.

Bilgi varlıklarının taşınması: Uzaktan çalışma esnasında, (belgeler ve veri taşıyıcıları gibi) bilgi varlıklarının güvenli bir şekilde taşınması ile ilgili gerekli düzenlenmeler yapılmalıdır. Elektronik ortamdaki hassas veriler mutlaka şifrelenmiş olarak taşınmalıdır.

Veri yedekleme: Çalışanlar, yerel olarak depolanan verilerin yedeklerini almakla yükümlü tutulmalıdır. Buna ek olarak, daha yüksek erişilebilirliğin (HA) sağlanabilmesi için çalışanlar kullandıkları cihazlarda tutulan kurumsal verileri ve yedekleri belirli aralıklarla kurum sunucularına yüklemelidir.

Veri tabanlarının senkronizasyonu: Uzaktan çalışma esnasında kullanıcı cihazlarında yerel olarak kullanılan veri tabanları belirli aralıklarla ve uygun şekilde kurum veri tabanları ile senkronize edilmelidir. Senkronizasyon, çakışma ve dolayısıyla veri kaybı olmayacak şekilde dikkatlice yapılmalıdır. Bu iş için geliştirilmiş otomasyon yazılımlarının kullanılması tavsiye edilir.

Veri koruma: Uzaktan çalışanlar ilgili veri koruma yönetmeliklerine uymakla yükümlüdür. Uzaktan çalışma esnasında kişisel verilerin kullanımını gerektirecek durumlarda alınması gereken önlemler uyulması gereken konular hakkında çalışanlar bilgilendirilmelidir.

Veri iletimi: Hangi verilerin hangi şekilde iletilmesi gerektiği belirlenmelidir. Ayrıca, hangi verilerin elektronik ortamda iletilmemesi gerektiği veya sadece şifrelenmiş olarak iletilmesi gerektiği de açık bir şekilde tanımlanmalıdır. Kurumsal belgelerin kurum dışında nasıl taşınacağı ve bu verilerin nasıl korunacağı ile ilgili düzenlenmeler yapılmalıdır.

İmha etme: Güvenlik politikasında, çalışanların kullanılmayan veri ortamları ve belgeler gibi bilgi varlıklarını uzaktan çalışma esnasında nasıl imha etmesi gerektiğine dair düzenlemeler yapılmalıdır.

Farkındalık oluşturma: Uzaktan çalışma yapacak bütün çalışanlar, taşınabilir BT cihazlarının doğru kullanımı hakkında düzenli olarak bilgilendirilmelidir. Bu kapsamda çalışanlara, uyması gerekli güvenlik önlemleri ile ilgili eğitimler verilmelidir. Kurallar açık ve anlaşılır bir şekilde belgelenmeli ve bunlar uzaktan çalışma yürütecek bütün çalışanlarla paylaşılmalıdır.

Seyahatlerde kurumsal bilgilerin korunması: Çalışanlar, iş veya özel seyahatlerinde kurumsal hassas bilgileri kullanırken ayrıca dikkatli olmalı ve alınması gereken önlemlere mutlaka uymalıdır.

SNM.7.U9 Taşınabilir bilgi varlıklarının şifrelenmesi

Hassas bilgilerin yetkisi olmayan üçüncü taraflar tarafından ele geçirilmesini veya görüntülenmesini önlemek için, bilgiler kurum/kuruluş yönergelerine uygun olarak güvence altına alınmalıdır.

Veri taşıyıcıları ve taşınabilir BT cihazlarında bulunan hassas bilgileri yetkisiz erişime karşı korumak için, bu bilgiler kurum prosedürlerine ve düzenlemelerine uygun bir şekilde şifrelenmelidir. Özellikle yeniden yazılabilir BT ortamlarında bilgiler mutlaka şifrelenerek tutulmalıdır. Veri taşıyıcılarında bulunan bilgiler kısmen şifrelenebileceği gibi kullanım ve denetim kolaylığı olması açısından diskin tamamının şifrelenmesi önerilir. Verilerin şifrelenmesi (Microsoft BitLocker, Apple FileVault benzeri) yazılımlarla veya bu iş için özel olarak geliştirilmiş donanımlarla yapılabilir. Verilerin şifresini çözebilmek için çipli kart veya USB token formunda harici bir aygıt şeklinde olması tavsiye edilen şifreleme anahtarına sahip olunması gerekmektedir. Verilerin şifrelenmesiyle ilgili olarak aşağıda belirtilen gereksinimler dikkate alınmalıdır:

- Şifreleme esnasında meydana gelebilecek (enerji kesintisi, şifreleme işleminin yarıda kesilmesi gibi) arızaların sebep olabileceği veri kayıplarına karşı önlem alınmalıdır.
- Kullanılan şifreleme algoritması kurum bilgi güvenliği gereksinimlerine uygun olmalıdır.
- Şifreleme yöntemi kurumda kullanılan BT sistemlerinin işlevleriyle uyumlu olmalıdır.
- Güvenlik anahtarları güvenli bir şekilde ve şifrelenmiş cihazlardan ayrı bir konumda tutulmalıdır.
- Taşınabilir BT sistemleri şifreleme anahtarları gibi kritik güvenlik parametreleri güvenli bir şekilde yönetilmelidir. Örneğin; kullanımı bitmiş güvenlik anahtarlarının okunabilir formatta şifrelenmemiş olarak saklanmamalı, mümkünse imha edilmelidir.

2.3 3. SEVİYE UYGULAMALAR

Aşağıda verilen uygulamalar, standart korumaya ilave olarak daha yüksek koruma seviyesine ihtiyaç duyulması halinde dikkat edilmesi gereken konulardır. Parantez içindeki harfler, önlem özelinde hangi temel değerler için öncelikli koruma sağlandığını ifade etmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

SNM.7.U10 Hırsızlığa karşı korunma ürünlerinin kullanımı

Hırsızlık önleme ürünleri, kurum için kritiklik seviyesi yüksek olan varlıkların tutulduğu veya başka önlemlerin uygulanamadığı yerlerde kullanılmalıdır. Örneğin hareket halinde kullanılan taşınabilir bilgisayarların için bu önlemi kullanmak önerilir. Hırsızlığa karşı koruma ürünlerinin kullanımı, halka açık alanların çalışma alanı olarak kullanıldığı ve insan hareketliliğinin yüksek olduğu yerlerde ayrıca önem kazanmaktadır. Bu ürünlerin kullanımıyla, sadece korunacak olan donanımın ürün maliyeti değil; aynı zamanda içinde barındırdığı bilgilerin değerinin de dikkate alındığı bilinmelidir. Hatta çoğu zaman korunan bilginin maliyeti donanım maliyetinden daha yüksektir.

Hırsızlığa karşı koruma ürünleri

Hırsızlık önlemek için kullanılabilecek çok çeşitli ürünler bulunabilmektedir. Bu ürünler genel anlamda mekanik ve elektronik olmak üzere ikiye ayrılır.

Mekanik koruma ürünlerine örnek olarak; kablo kilitleri (Şekil 9), güvenlik kilitli muhafazalar (Şekil 10) ve güvenlik kilitli çubuklar (Şekil 11) verilebilir. Bu ürünler ile BT cihazlarının çalınması önlenebildiği gibi çıkarılabilir parçaların yerinden oynatılması engellenerek ayarların sıfırlanması veya değiştirilmesi de engellenebilir.

Şekil 9. Kilitli Kablo

Şekil 10. Kilitli Çubuk

Şekil 11. Kilitli Muhafaza

Mekanik güvenlik ürünlerinin, ilgili ihtiyaçlara göre uyarlanmış bir kilitleme sistemine sahip olması önemlidir. Ürüne bağlı olarak farklı kilitleme özellikleri mevcut olabilir:

- **Aynı anahtarlı kilitle**r: Bu tür ürünlerde anahtarlar, kurumun veya bölümün kullandığı tüm ürünlerin üzerindeki kilitleri açabilir. Bunun avantajı kilit yönetim için daha az efor harcanması olacaktır. Dezavantajı ise çok sayıda aynı anahtarın dolaşımda olmasından kaynaklı olarak herhangi bir olay meydana gelmesi durumunda olayın gerçekleşmesine sebep olan kişinin ve ihmalin tespit edilemiyor olmasıdır.
- **Farklı anahtarlı kilitler**: Her cihaz kilidinin farklı anahtarı vardır. Bu durumda anahtar yönetimi için harcanan efor yüksek olacaktır; ancak dolaşımda daha az anahtar kopyası bulunacaktır.
- **Master anahtar sistemi:** Belli bir plan dahilinde hangi anahtarların hangi kilitleri açabileceğinin belirlendiği ve uygulandığı sistemdir. Bu şekilde tüm anahtarlar ve giriş hakları koruma altına alınır. Sistemin oluşturulması ve işletilmesi için harcanan toplam çabanın düşük olmasına karşın oluşturma maliyeti diğer kilit sistemlerine oranla daha yüksektir.

SNM.7.U11 Güvenli olmayan ortamların kullanımı (GE)

Artan koruma gereksinimleri doğrultusunda, risk kaynaklarını ve güvenlik açıklarını en aza indirmek için, çalışma ortamına özel bazı kriterler tanımlanmalıdır. Kriterler, güvenliğin sağlanması hususunda yeterli olabilmeleri için, asgari olarak aşağıda belirtilen konuları kapsamalıdır.

Yetkisiz kişiler tarafından çalışma ortamına erişim:

Ekranlar, üçüncü kişilerce görülemeyecek şekilde konumlandırılmalıdır. Görsel hırsızların bilgisayar ekranlarına yandan bakarak bilgi çalmasını önleyen gizlilik filtreleri veya ekran folyoları kullanılabilir

Kapalı, kilitlenebilir veya korunan odalar:

Bilgilerin korunması ihtiyacına bağlı olarak, bilgiler kapalı, kilitlenebilir veya korunan odalarda tutulmalıdır. Koruma gereksinimi arttığında aralarından seçim yapabileceğiniz birkaç seçenek varsa, daima mümkün olan en yüksek korumaya sahip olan seçilmelidir.

Kesintisiz ve güvenli iletişim:

Uzaktan çalışma modelinin olmazsa olmaz gereksinimlerinden bir tanesi iletişim alt yapısına sahip olmaktır. Gelişen teknoloji sayesinde geçmişte çok büyük teçhizatlar kullanılarak yapılan işler (ör. canlı yayın araçları) günümüzde daha küçük donanımlar kullanılarak daha hızlı, kaliteli ve güvenli yapılabilmektedir. İletişim teknolojileri de günden güne gelişmekte iletişim için kullanılan bağlantılar her geçen gün daha hızlı hale gelmektedir. Bu durum uzaktan çalışmayı mümkün kılmaktadır. Bu sebeple, uzaktan çalışma modelini uygulayan kurum ve kuruluşlar çalışanlarına kesintisiz ve güvenli iletişim alt yapısını sağlamak durumundadır. Uzaktan çalışanlar, gerektiğinde evlerinde sahip oldukları sabit iletişim alt yapısına ek olarak yedek mobil iletişim teknoloji ve alt yapılarına sahip olmaları için desteklenmelidir.

Uzaktan çalışma için iletişim seçenekleri her zaman koruma gereksinimlerine göre belirlenmelidir. Bu nedenle, Sanal Özel Ağ (VPN) veya Mobil Cihaz Yönetimi (MDM) yoluyla güvenlik çözümleri, artan koruma gereksinimleri olan ofis dışı çalışmalara uygun şekilde uyarlanmalıdır.

Yeterli ve yedekli güç kaynağı:

Taşınabilir cihazların çalışma boyunca şarj sürelerinin yeteceğinden emin olunmalıdır. Eğer bu süre yeterli olmayacaksa, mutlaka yedek bir güç kaynağı sağlanmalıdır. Özellikle seyahatlerde yedek piller, yedek bilgisayar bataryaları veya kurumun uygun gördüğü taşınabilir güç üniteleri kullanılmalıdır.

SNM.7.U12 Bulut bilişim ortam güvenliği (GBE)

Uzaktan çalışma yönteminin yaygınlaşması ile birlikte bulut bilişim ortamlarının kullanımı artmıştır. Bundan dolayı bulut bilişim ortamlarının güvenliği, operasyonel açıdan etkinliği iş sürekliliğinin sağlanması aşamasında oldukça kritik bir öneme sahip olmuştur.

NIST (National Institute of Standards & Technology)'e göre bulut sisteminin aşağıdaki özelliklere sahip olması beklenmektedir (P. & Grance, 2011):

- İsteğe Bağlı Self Servis (On-demand Self-service)
- Geniş Ağ Erişimi (Broad Network Access)
- Kaynak Havuzu Oluşturma (Resource Pooling)
- Hızlı Elastikiyet (Rapid Elasticity)
- Ölçülen Hizmet (Measured Service):

Bulut bilişim sayesinde kaynakları yönetilebilen esnek ortamlar oluşturabilir. Bulut sistemler, teknoloji dünyasında aktif olarak kullanılmaktadır. Tercih edilecek bulut hizmeti modelinin belirlenmesi için esneklik, ölçeklenebilirlik, birlikte çalışabilirlik ve hizmetin kontrolü faktörleri dikkate alınır. Bulut bilişim ortamlarında tutulan verilerin ve kaynakların güvenli şekilde muhafaza edilebilmesi için kapsamlı bir kimlik doğrulama ve yetkilendirme mekanizması gerekmektedir. Etkili kimlik doğrulama ve yetkilendirme mekanizmasında yaşanabilecek eksiklikler, siber saldırılar, veri sızıntısı gibi çeşitli problemler neden olabilir. Bir bulut sisteminde, verilerin depolanması ve işlenmesi kurumlar tarafından veya üçüncü taraf hizmet sağlayıcıları yardımıyla yapılabilir. Servis sağlayıcı, bulutta depolanan verilerin ve uygulamaların korunmasının yanı sıra bulut altyapısının güvenli olmasını da sağlamalıdır. Güvenlik sorunları ile karşılaşmamak için ağ yapıları en güncel güvenlik standartları ile yapılandırılmalıdır.

Her sistemde olduğu gibi, bulut sistemlerde de doğası gereği kurum/kuruluşları ve kullanıcılarını etkileyebilecek çeşitli güvenlik sorunları bulunabilmektedir. Bu sorunlar öncelikle, veri erişimi, veri bütünlüğü, veri mahremiyeti ve veri gizliliği gibi temel güvenlik gereksinimleriyle ilgilidir. Kurum ve kuruluşlar uzaktan çalışma modelleri için hazırladıkları politikalarda bulut bilişim gereksinimleri tanımlamalı ve bu gereksinimlere uygun güvenlik yöntemlerini ayrıntılı bir şekilde belirlemelidir.

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
SNM.7.U1	Uzaktan çalışma ortamının seçimi ve kullanımı	Uzaktan çalışma esnasında çalışanların kullandığı alanların uygun olup olmadığı değerlendiriliyor mi?
SNM.7.U2	Uzaktan çalışma usul ve esasları	Hangi bilgi varlıklarının iş yerleri dışına çıkarılabileceği ve hangi verilerin iş yeri dışında işlenebileceğine dair düzenlemeler oluşturuluyor mu?
SNM.7.U2	Uzaktan çalışma usul ve esasları	Kullanıcıların uzaktan çalışma esnasında kullandıkları BT sistemleri ve donanımları, çalınmaya veya kaybolmaya karşı güvenli hale getiriliyor mu?
SNM.7.U2	Uzaktan çalışma usul ve esasları	Taşınabilir BT sistemleri ve verileri, şifrelenerek korunuyor mu?
SNM.7.U2	Uzaktan çalışma usul ve esasları	Uzaktan çalışmada kullanılan herhangi bir kimlik doğrulama yöntemi mevcut mu?
SNM.7.U3	Güvenlik ve erişim kontrolü	Ofis dışı çalışma alanlarında herhangi bir erişim kontrolü uygulanıyor mu?
SNM.7.U4	Ortak çalışma alanlarında harici BT sistem ve alt yapılarının kullanımı	Tüm çalışanlar, üçüncü taraflarca yönetilen harici BT sistem ve alt yapılarının kullanımının daha yüksek güvenlik riskleri taşıdığı konusunda bilgilendiriliyor mu?
SNM.7.U4	Ortak çalışma alanlarında harici BT sistem ve alt yapılarının kullanımı	Üçüncü taraflarca yönetilen harici BT sistemleri kullanıldıktan sonra oluşan tüm veriler bu sistemlerden kalıcı bir şekilde siliniyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
SNM.7.U4	Ortak çalışma alanlarında harici BT sistem ve alt yapılarının kullanımı	Üçüncü taraflarca yönetilen harici BT sistemlerinde tarayıcıların kullanıcı adı ve parolaları otomatik kaydetmesi engelleniyor mu?
SNM.7.U5	Bilgi varlığının kaybolması veya çalınması	Kuruma ait bilgi varlıklarından herhangi birisinin kaybolması/çalınması durumunda, çalışanların bu durumu raporlayabileceği irtibat noktası ve iletişim kanalı belirlendi mi?
SNM.7.U6	Hassas bilgilerin imha edilmesi	Hassas bilgi içeren varlıklar uzaktan çalışma sürecinde uygun şekilde imha ediliyor mu?
SNM.7.U6	Hassas bilgilerin imha edilmesi	Hassas bilgiler içeren bilgi varlıklarının, uzaktan çalışma sürecinde kullanım dışına ayırma ve imha edilmesiyle ilgili yöntem ve politikalar belirlendi mi?
SNM.7.U6	Hassas bilgilerin imha edilmesi	Hassas bilgilerin güvenli bir şekilde imha edildiği denetleniyor mu?
SNM.7.U7	Uzaktan çalışmayla ilgili yasal düzenlemeler	Uzaktan çalışma esasları ile ilgili çeşitli iş kanunları ve iş güvenliği yönetmelikleri gözetiliyor mu?
SNM.7.U8	Uzaktan çalışma ortamı için güvenlik politikası	Uzaktan çalışma yapacak bütün çalışanlar, taşınabilir BT cihazlarının doğru kullanımı hakkında düzenli olarak bilgilendiriliyor mu?
SNM.7.U9	Taşınabilir bilgi varlıklarının şifrelenmesi	Hassas bilgilerin yetkisiz kişilerce ele geçirilmesini önleyen yöntemler uygulanıyor mu?
SNM.7.U10	Hırsızlığa karşı koruma ürünlerinin kullanımı	Kurum için kritiklik seviyesi yüksek olan varlıkların tutulduğu yerlerde hırsızlığa karşı koruma ürünleri kullanılıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
SNM.7.U11	Güvenli olmayan ortamların kullanımı	Artan koruma gereksinimleri doğrultusunda, risk kaynaklarını ve güvenlik açıklarına karşı, çalışma ortamına özel prosedürler tanımlanıyor mu?
SNM.7.U12	Bulut bilişim ortam güvenliği ve operasyonel açıdan etkinliği	Bulut bilişimde barındırılan uygulamaların güvenliği hangi yöntemler ile sağlanıyor?

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.dijitalakademi.gov.tr