TÜBİTAK
BİLGEM
YTE

DİJİTAL KABİLİYET
REHBERLERİ

SUNUCU YÖNETİMİ REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Eylül 2020

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Aralık 2019	İlk sürüm	TÜBİTAK BİLGEM YTE
Sürüm 1.1	Eylül 2020	Revizyon	TÜBİTAK BİLGEM YTE

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

YÖNETİCİ ÖZETİ

Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan, kurumsal dijital kabiliyetlerini bütüncül bir yapı üzerinden değerlendirmeyi sağlayan **Dijital Olgunluk Değerlendirme Modeli**'nin geliştirilmesi ve bu **Model** ile uyumlu **Rehberlerin** hazırlanması ile dijital kurumsal kapasitenin artırılmasına ihtiyaç bulunmaktadır. Bu ihtiyaç doğrultusunda TÜBİTAK-BİLGEM-YTE tarafından iç destekli olarak **Dijital Olgunluk 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 2834 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 İşletimi Rehberi**, **Kablosuz Ağların Yönetimi Rehberi**, **Aktif Dizin Yönetimi Rehberi**, **Sunucu Yönetimi Rehberi ve İstemci Yönetimi Rehberi** yayımlanmıştır. 2020 yılı içerisinde bunlara ek olarak **Uzaktan Çalışma Rehberi**, **VOIP Rehberi ve Alan Adı Sistem Yönetimi Rehberi** yayınlanmıştır.

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

Sunucu Yönetimi 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, Sunucu Yönetimi Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Sunucu Yönetimi 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.
ACL	[Access Control List] Erişim denetim listesi
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.

Terim / Kısaltma	Tanım
BT	Bilişim teknolojileri
CA	[Certification Authority] Güvenli iletişim için kullanılan sertifikaları ve ortak anahtarları yöneten ve sağlayan otoriteye verilen isimdir.
CPU	[Central Processing Unit] Merkezi İşlem Birimi. Bilgisayar programlarının komutlarını işleyen merkezi birim olan işlemci veya mikroişlemci için kullanılan terimdir.
d-Devlet	Dijital Devlet
DMZ	[DeMilitarized Zone] İnternet üzerinden erişilebilir sunucuların konumlandırıldığı, iç ağdan ayrıştırılmış bölge
DNS	[Domain Name System] TCP/IP ağlarda kullanılan isim çözümleme protokolüdür.
DOS	[Denial of Service] Erişim engelleme saldırısı
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
EV	[Extended Validation] Genişletilmiş Doğrulama
GnuPGP	[GNU Privacy Guard] PGP yerine kullanılabilen GPL lisanslı bir özgür yazılım alternatifidir.

Terim / Kısaltma	Tanım
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. (Örnek: Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
HSTS	[HTTP Strict Transport Security] Sunucuya yapılan her talep için veri aktarımında HTTPS kullanmaya zorlayarak saldırılara karşı sunucuyu koruyan bir protokoldür.
HTTPS	[HTTP over SSL veya HTTP Secure] HTTP'nin, SSL veya TLS kullanılarak güvenlik katmanı eklenmiş halidir.
ICMP	[Internet Control Message Protocol] Sorun giderme, kontrol ve hata mesajı servisleri sağlayan TCP / IP ağ katmanı protokolüdür.
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.

Terim / Kısaltma	Tanım
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
LDAP	[Lightweight Directory Access Protocol] Dizin hizmetindeki bilgilerin sorgulanmalarını ve güncellenmelerini sağlayan endüstri standardı bir protokoldür.
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.
PFS	[Perfect Forward Secrecy] İleri Yönlü Kusursuz Güvenlik veya İleri Yönlü Güvenlik olarak da adlandırılır. Şifrelenmiş verilerin anahtar bilgisinin istenmeyen kişilerce ele geçirilmesi durumunda dahi bu anahtar ile geçmişte şifrelenmiş verilerin çözümlemesinin yapılamadığı yönteme verilen addır.

Terim / Kısaltma	Tanım
PGP	[Pretty Good Privacy] Gönderilen ya da alınan verinin gizliliğini ve doğrulamasını sağlamak için, veri şifrelemek, şifreli veriyi çözmek veya veriyi imzalamak için kullanılan bir uygulamadır.
PIN	[Personal Identfication Number] İçerisinde alfanümerik veya sayısal karakterleri barındıran, bir sistemde erişim hakkına sahip olmak için kullanılan paroladır.
PKI	[Public Key Infrastructure] Dijital sertifikaların oluşturulması, yönetilmesi, dağıtılması, kullanılması ve yeri geldiğinde iptal edilebilmesi için donanım, yazılım, kullanıcılar, kurallar ve gerekli prosedürlerden meydana gelen yapıdır.
Problem	Bir veya birden fazla arızaya/kesintiye neden olan ve çözülmesi istenen sorundur.
RAID	[Redundant Array of Independent Disks] bir disk arızası durumunda verileri korumak için aynı verileri birden fazla sabit diskte farklı yerlerde depolama yöntemidir.
Risk	Hedeflenen kazanç veya çıktıya, gelecekte olumlu veya olumsuz etkisi olabilecek belirsizliklerdir.
SAN	[Storage Area Network] Depolama alanı ağı. Büyük ağ kullanıcılarına hizmet vermek üzere veri sunucuları ile birlikte farklı tipte veri depolama cihazını birbirine bağlayan özel amaçlı, yüksek hızlı ağ.
SPOF	[Single Poing Of Failure] Herhangi bir sorundan dolayı çalışması durduğu zaman, dahil olduğu tüm sisteminin çalışmasını durduracak sistem bileşenidir.

Terim / Kısaltma	Tanım
SSH	[Secure Socket Shell] Güvenli Kabuk. Ağ hizmetlerinin güvenli olmayan bir ağ üzerinde güvenli şekilde çalıştırılması için kullanılan bir kriptografik ağ protokolüdür.
SSL	[Secure Sockets Layer] Sunucu ile istemci arasındaki iletişimi şifreleme yöntemidir.
STK	Sivil Toplum Kuruluşu
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme
TCP	[Transmission Control Protocol] Bilgisayar ağlarında kontrollü veri iletimini sağlayan protokoldür.
TLS	[Transport Layer Security] Bilgisayar ağı üzerinden güvenli haberleşmeyi sağlamak için tasarlanmış şifreleme protokolüdür.
TS	Türk Standartları
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDP	[User Datagram Protokol] Bilgisayar ağlarında veri iletimini sağlayan protokoldür.
UPS	[Uninterruptible Power Supply] Kesintisiz Güç Kaynağı. Elektrik, kesildiğinde ya da kabul edilen gerilim aralığının dışına çıktığında, BT sistemlerini besleyerek güvende kalmalarını sağlayan aygıt.

Terim / Kısaltma	Tanım
URL	[Uniform Resource Locator] İnternetteki bir sayfanın ve dosyanın adresidir.
VPN	[Virtual Private Network] İletişimi, kimlik doğrulaması ve şifrelemeye tabi tutarak güvenli hale getiren tünelleme yöntemi
WAN	[Wide Area Network] Geniş alan ağı
WLAN	[Wireless Local Area Network] Kablosuz yerel alan ağı
X.509	Kriptografide açık anahtar altyapısını uygulamak için kullanılan bir haberleşme standardıdır.
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü
Yük Dengeleyici	[Load Balancer] Gelen ağ trafiğini sunucu havuzundaki sunucular arasında paylaştırma işlemini yapan sistemdir.

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

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.

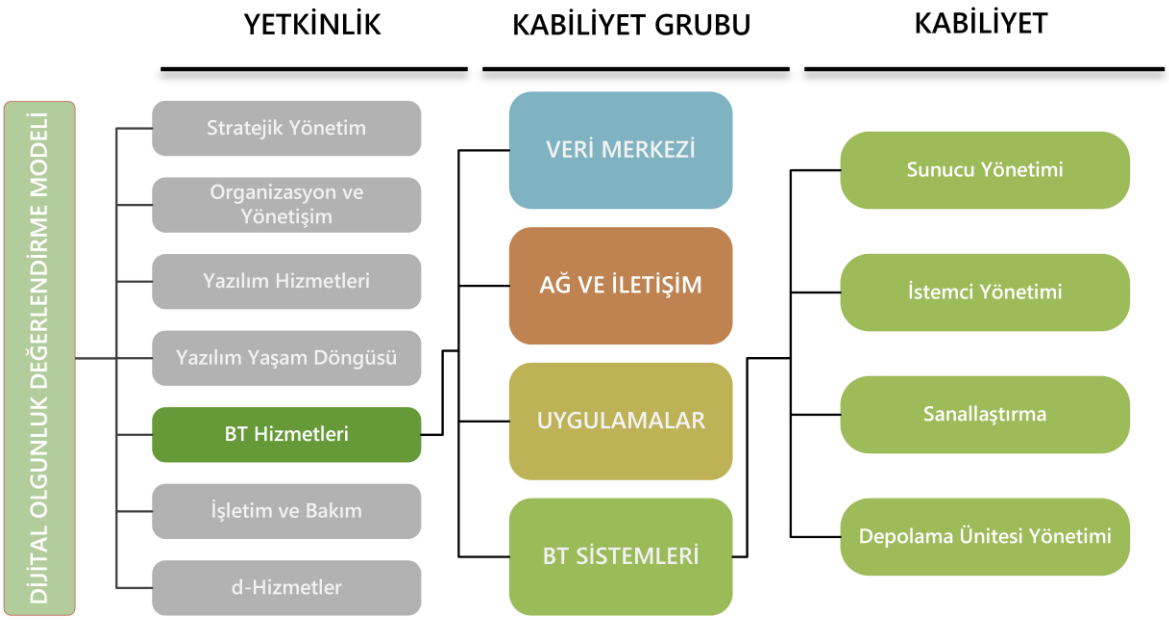
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır.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



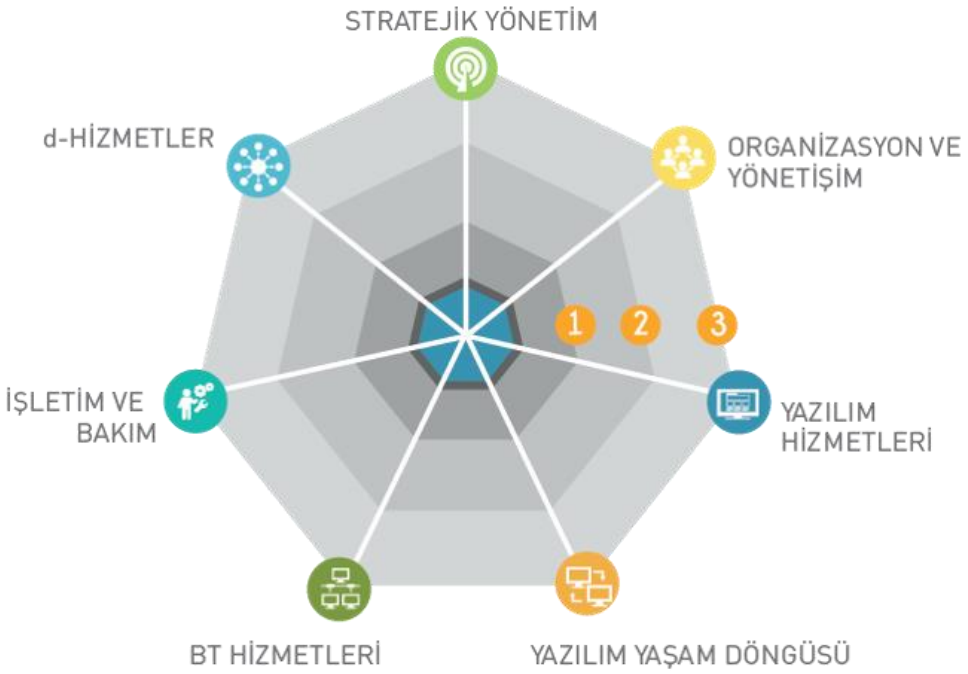
Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

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;

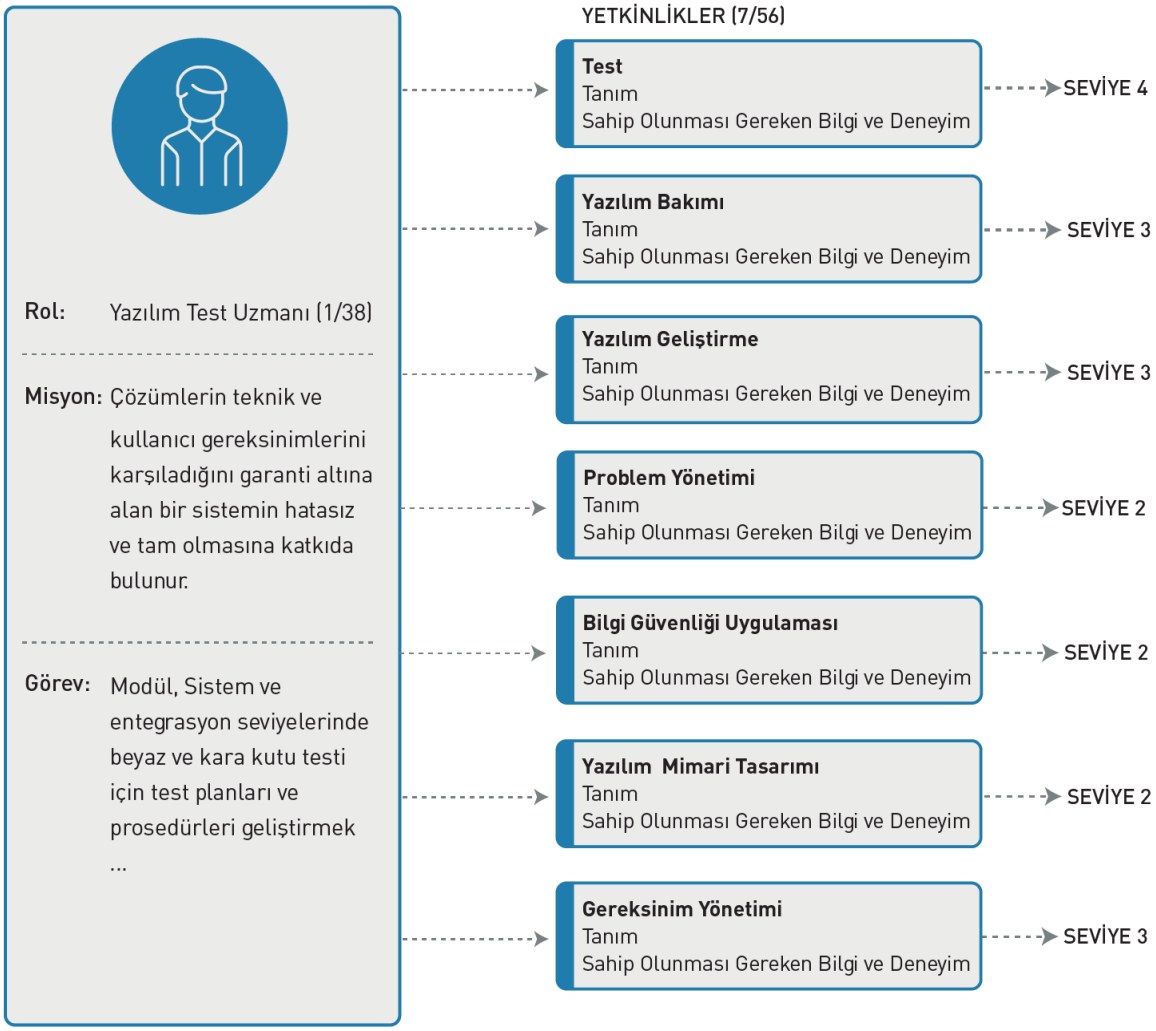
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının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

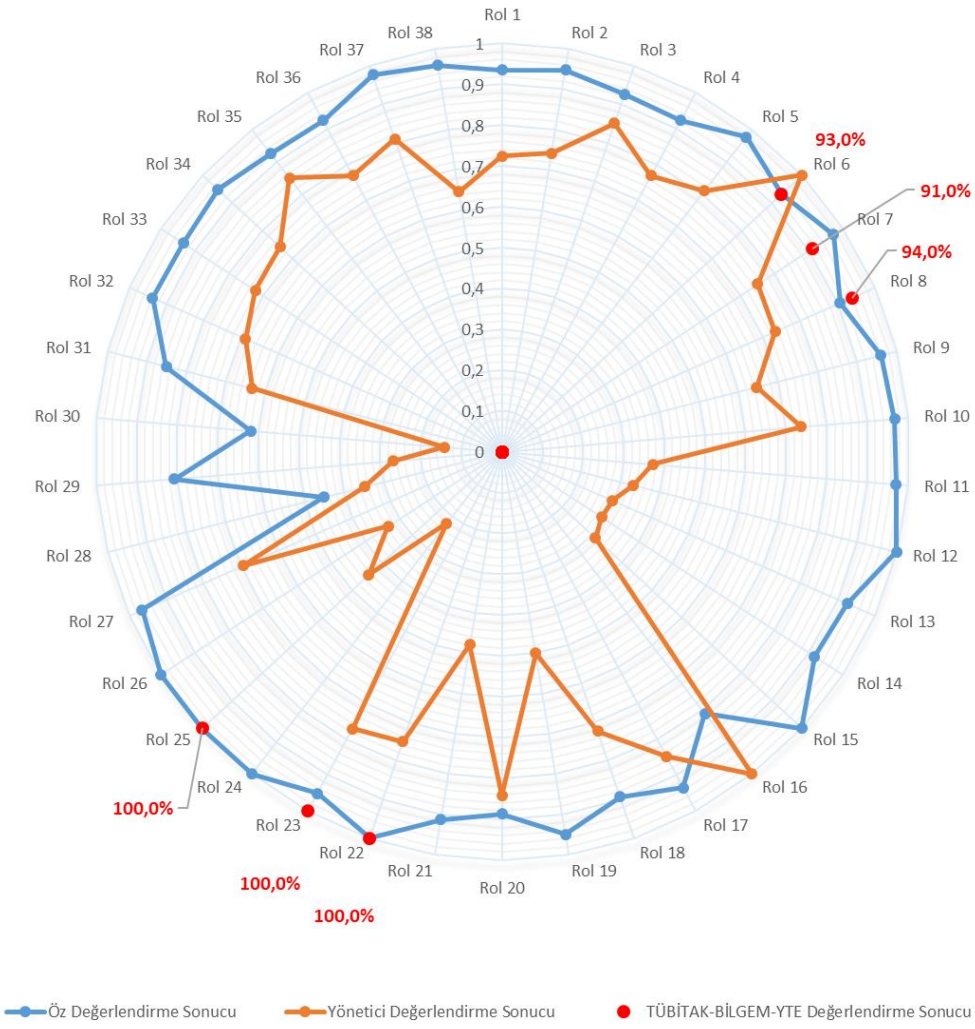
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

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:



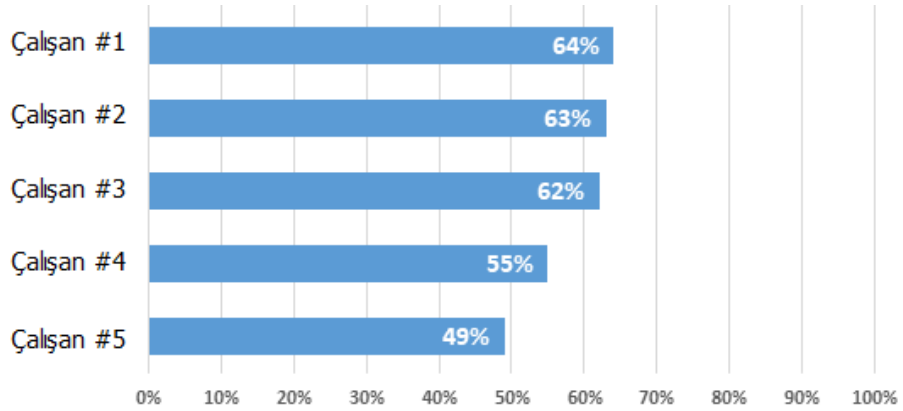
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

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:



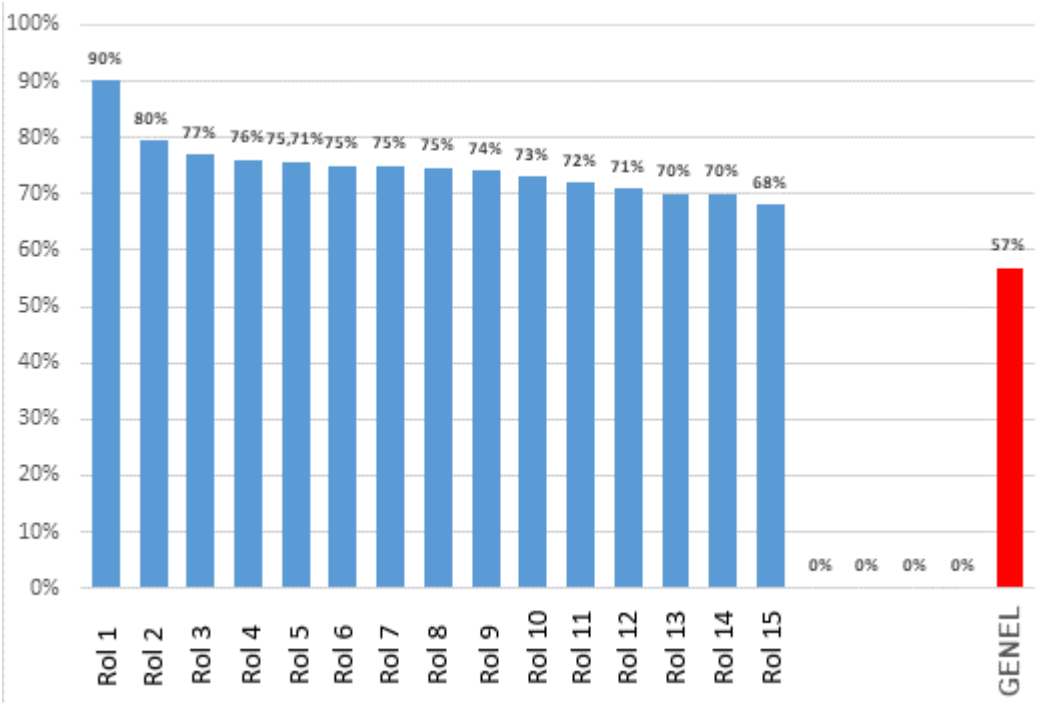
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

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 BT HİZMETLERİ YETKİNLİĞİ

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

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

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

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

Yüksek gereksinimler, ele alınması gereken 3. seviye güvenlik eksikliklerini gösterir. Yüksek gereksinim hedefleri, bir taraftan sistemlerin en iyi şekilde korunması sağlar diğer tarafta uygulamada ve bakımda önemli ölçüde maliyetleri artıracaktır. Bundan dolayı yüksek koruma gereksinimleri hedefleniyorsa, maliyet ve etkililik yönleri dikkate alınarak bireysel bir risk analizi yapılmalıdır. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin

uygulanması ve bu yöndeki ihtiyaçların giderilmesi, kurumun veya organizasyonun hedefleri doğrultusunda yeterlidir.

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

4.1 YÖNTEM

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

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

Her kabiliyet, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) 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. Ayrıca BT bileşenleri, aynı fihrist/dizin yapısında düzenlenmiştir. Temel bileşen yapısı aşağıdaki gibi oluşturulmuştur:

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
    - **1.1 Tanım**: Bileşenin kısa tanımıdır.

- **1.2 Hedef**: Bu bileşenin uygulanmasıyla ne tür güvenlik kazanımlarının sağlanacağı hedefler verilmektedir.
- **1.3 Kapsam Dışı**: Bileşende ele alınmayan kapsamın yanı sıra hangi bileşenin konusu olduğu gibi bilgiler yer alır.

- **Bölüm 2 – Risk Kaynakları**
  - Temel bileşene ait özet riskler anlatılmaktadır. Bunlar, sistemlerin kullanımında önlem alınmadığı takdirde ortaya çıkabilecek güvenlik sorunlarının bir resmini çizer. Olası risklerin açıklanması, kullanıcının konu hakkındaki bilinç düzeyini artırır.
- **Bölüm 3 – Gereksinimler**
  - **3.1 1. Seviye Gereksinimler:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir .
  - **3.2 2. Seviye Gereksinimler:** İhtiyaçlar doğrultusunda bu standart gereksinimlerin yerine getirilmesi tavsiye edilir.
  - **3.3 3. Seviye Gereksinimler:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 4 – Detaylı Bilgi için Kaynaklar**
  - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

BT Hizmetleri rehberleri içerdikleri konular itibari ile birbirleri arasındaki ilişkinin kurulması için bir referanslama metodu kullanılmıştır. Bu amaçla her gereksinim maddesi numaralandırılmıştır. Örneğin, BT Hizmetleri rehberlerinde yer alan BTS.1.G1 kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

"BT Sistemleri" kabiliyet grubu için kullanılan kısaltma	**"Sunucu Yönetimi" kabiliyeti için atanan numara**	**1. Gereksinim maddesi**
BTS	1	G1

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberlerinde ise yalnız "G" harfi yerine "U" harfi kullanılmıştır. Örneğin, BTS.1.G1 gereksinim maddesinin karşılığı BTS.1.U1 olarak geçmektedir.

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

UYGULAMA REHBER YAPISI

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

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
    - **1.1 Tanım:** Bileşenin detaylı tanımıdır.
    - **1.2 Yaşam Döngüsü:** Uygulama rehberleri “Planlama ve Tasarım”, “Tedarik”, “Uygulama”, “Operasyon”, “Elden Çıkarma” ve “Acil Durum Hazırlık” gibi aşamalardan oluşan yaşam döngüsüne yönelik önlemlerin genel resmini içerir.
- **Bölüm 2 – Uygulamalar:**
    - **2.1 1.Seviye Uygulamalar:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir.
    - **2.2 2.Seviye Uygulamalar:** İhtiyaçlar doğrultusunda bu standart gereksinimleri yerine getirilmesi tavsiye edilir.
    - **2.3 3.Seviye Uygulamalar:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 3 – Detaylı Bilgi için Kaynaklar**
    - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

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

4.3 KABİLİYET GRUPLARI

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

Şekil 7. BT Hizmetleri Yetkinliği Kabiliyet Grupları

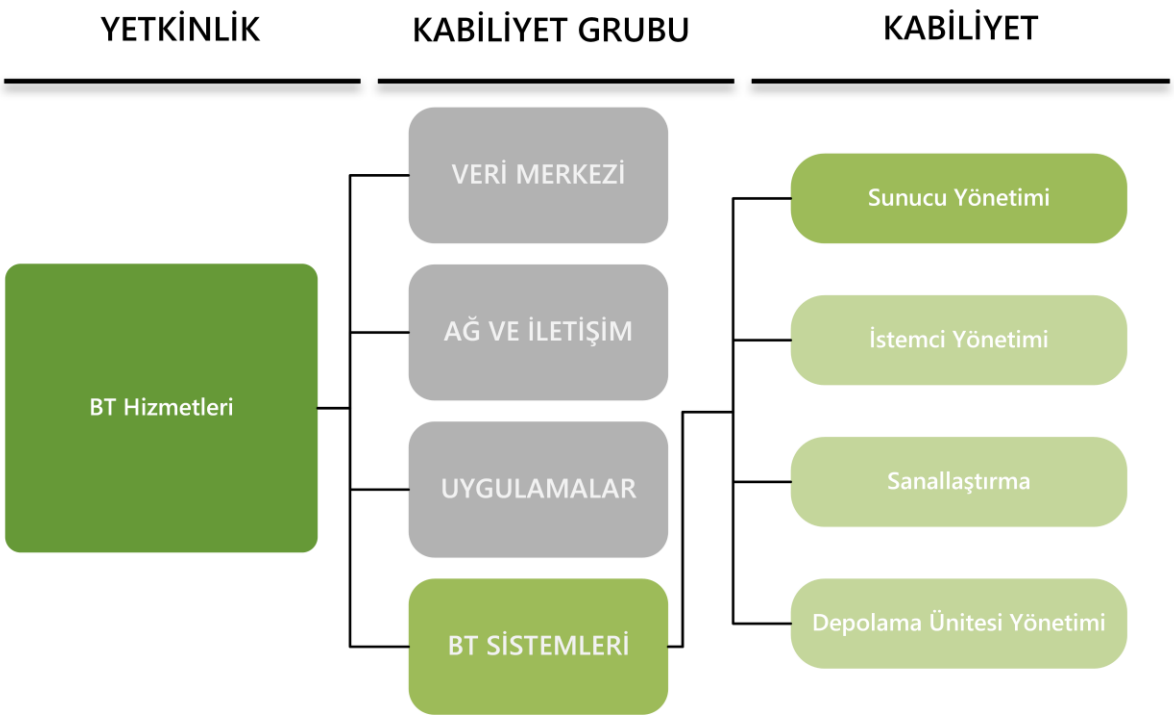
- **Veri Merkezi;** Veri merkezi kapsamında, kritik BT bileşenlerini içeren kurumun yapısal-teknik koşullarının yanında, altyapı güvenliği ile ilgili yönlerini de irdeler. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Genel Bina
    - Veri merkezi içerisinde bulunan binalar için, genel bina önlemleri en az bir kere uygulanmalıdır.
  - Veri Merkezi ve/veya Sistem Odası
    - Veri merkezi ve/veya sistem odası modülü, kurumun kritik odaları için uygulanmalıdır.
    - Kurum/organizasyon erişilebilirlik hedeflerine veya organizasyon boyutuna göre bu tür alanlar, rehber içeriğinde kritiklik düzeyine göre özelleştirilerek verilmiştir.
  - Elektrik Kablolama
    - Veri merkezini ve kritik bileşenleri besleyen güç kaynaklarının hedeflenen erişilebilirlik prensipleri doğrultusunda en az bir kere uygulanması gereklidir.
  - BT Kablolama
    - Kural olarak bu modül veri merkezinin içerisinde yer alan bina veya yerleşke için en az bir kere uygulanmalıdır. Ayrıca veri merkezi için de kullanılabilir.
- **Ağ ve İletişim;** Ağ ve iletişim hizmetlerinin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Ağ
    - Ağ Mimarisi ve Tasarımı ile Ağ İşletimi konularındaki kabiliyetleri içermektedir.

- Kablosuz Ağlar
  - Kablosuz Ağların Kullanımı ve İşletimi konularındaki kabiliyetleri içermektedir.
- Ağ Bileşenleri
  - Yönlendirici ve Ağ Anahtarlama Cihazı, Güvenlik Duvarı, VPN ve IDS/IPS konularındaki kabiliyetleri içermektedir.
- Telekomünikasyon
  - PBX, VOIP, Fax ve Video Konferans konularındaki kabiliyetleri içermektedir.

- **Uygulamalar;** BT hizmetlerinde kullanılan çeşitli uygulamaların planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler:
  - Kullanıcı
    - Bu kabiliyet, tüm kurum veya organizasyonda kullanılan ofis uygulamalarını, web tarayıcılarını ve/veya mobil uygulamalarını içerir.
  - Dizin
    - Kurum veya organizasyonda kullanılan dizin hizmetine (Active Directory, OpenLDAP vs.) özel kabiliyetleri kapsar.
  - Ağ Tabanlı Uygulamalar
    - BT sistemlerinde kullanılan web hizmetleri (ör. İntranet veya internet), web sunucusu, dosya paylaşımı, DNS hizmetleri gibi kabiliyetleri kapsar.
  - İş Uygulamaları
    - Kurum veya organizasyon genelinde, kurumsal kaynakların yönetimi için iş birimleri tarafından kullanılan uygulamalara özel kabiliyetleri içerir.
  - Veri tabanı
    - Belli bir amaca yönelik düzenli, büyük miktarda veriyi depolayabilen, bu verilerin hızlı bir şekilde yönetilip değiştirilebilmesine ve raporlanmasına imkan sağlayan ilişkisel veya ilişkisel olmayan veri tabanı uygulamalarına dair kabiliyetleri içerir.
  - İletişim Uygulamaları
    - Organizasyon genelinde, çalışanların iletişim amaçlı kullandıkları uygulamalara dair kabiliyetleri kapsar.

- **BT Sistemleri;** BT hizmetlerinde kullanılan sistemlerin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler; sunucu, istemci sanallaştırma ve depolama ünitesi yönetimlerini kapsar.
    - Sunucu Yönetimi
        - Bu kabiliyet, tüm kurum veya organizasyonda kullanılan sunucuların yaşam döngüsü boyunca güvenli bir şekilde yönetimi için kabiliyetleri kapsar.
    - İstemci Yönetimi
        - Kurumda kullanılan istemcilerin yaşam döngüsü boyunca güvenli yönetimi ve kullanımı için kabiliyetleri kapsar.
    - Sanallaştırma
        - BT sistemlerinde kullanılan sanal altyapıların güvenli yönetimi için kabiliyetleri kapsar.
    - Depolama Ünitesi Yönetimi
        - Kurum BT altyapısında bulunan depolama ünitelerinin yaşam döngüsü boyunca güvenli bir şekilde yönetimi için kabiliyetleri kapsar.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

BTS: BT SİSTEMLERİ

BTS.1.G SUNUCU YÖNETİMİ

TEMEL BİLEŞEN REHBERİ

BTS.1.G SUNUCU YÖNETİMİ
TEMEL BİLEŞEN

1 AÇIKLAMA

1.1 TANIM

Sunucu; BT altyapısında, istemcilerin ve diğer ağ bileşenlerinin kullanımına açık kaynakları ve hizmetleri (FTP, e-posta, veritabanı vb.) sunan bilgisayar sistemlerine verilen genel isimdir. "Sunucu Yönetimi Rehberi", sunucuların tüm yaşam döngüsünün güvenli bir şekilde yönetilebilmesi için gereksinimleri içermektedir.

1.2 HEDEF

Bu rehberin amacı; işletim sistemi ne olursa olsun, sunucu üzerinde oluşturulan, okunan, düzenlenen, saklanan veya paylaşılan verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaya yönelik bilgileri sunmaktır.

1.3 KAPSAM DIŞI

Sunucu sistemleri üzerinde, belirli güvenlik gereksinimleri olan işletim sistemleri çalışır. Sunucu tarafından sunulan farklı hizmetlerin (aktif dizin, e-posta, DNS vb.) güvenliğiyle ilgili bilgiler, bu rehberin kapsamında değildir. Farklı sunucu hizmetleri için bu rehbere ek olarak, hizmet özelinde sunulan rehberlerden faydalanılabilir.

2 RİSK KAYNAKLARI

Aşağıda belirtilen güvenlik açıkları ve tehditler, rehber kapsamında öncelikli olarak dikkat edilmesi gereken hususlardır.

2.1 YAZILIM AÇIKLARI VE HATALARI

Yazılım güvenlik açıkları, yazılım geliştiricisi tarafından bilinmeyen ancak BT sistemi için güvenlik riski oluşturan istem dışı programlama hatalarıdır. Yazılım açıkları, saldırganlar tarafından BT sistemlerine erişmek, sistemlerin işlevini bozmak ve sistemlerdeki kritik bilgileri toplamak gibi çeşitli amaçlar için kullanılır. Bu açıklar ve hatalar derhal tespit edilip düzeltilmezse, uygulama sırasında geniş kapsamlı olumsuzluklara sebep olabilir. Ayrıca, yaygın olarak kullanılan standart yazılımlardaki açıklıklar, bu yazılımları kullanan kurumlarda güvenlik riskini artırmaktadır.

Özellikle, sunuculardaki yüklü bulunan yazılımlardaki hatalar ve açıklar ciddi sonuçlar doğurabilir. Sunucunun sunduğu hizmet internete açık ise dünyanın herhangi bir yerindeki saldırgan bu açıklıktan faydalanabilir.

2.2 VERİ KAYBI

Sunuculardan hizmet alan kullanıcılar, sunucu üzerinde depoladıkları verilerin merkezi olarak saklanıp korunacağına güvenirler. Dolayısıyla, sunucuda yaşanacak bir veri kaybı, kurumun iş süreçlerinde aksamalara ve iş gücü kayıplarının yaşanmasına sebep olabilir.

Birçok kurumda, kurumsal verilerin, yerel istemciler yerine merkezi bir depolama alanında tutulmasına yönelik politikalar bulunmaktadır. Merkezi depolama alanında tutulan verilerde bütünlüğün bozulması, bundan doğabilecek maliyetlere ek olarak müşteriler ve paydaşlar arasında güven kaybına neden olabilir. Böyle bir durum hukuki sonuçlar doğurabilir ve kamu düzeninde olumsuz bir etkiye de sebep olabilir.

2.3 HİZMETLERİN ENGELLENMESİ

"Hizmet engelleme" (DOS, DDOS) olarak adlandırılan bir tür erişilebilirliği engelleme saldırısı, sunucu tarafından sağlanan hizmetlerin, süreli veya süresiz olarak aksatılmasını ve bu hizmetlerin hizmet edinenler tarafından kullanılamamasını hedefler. Bu saldırılar genellikle, kullanıcıların edindikleri hizmetlerin veya bu hizmetlerin bağımlı oldukları diğer dağıtık kaynakların, saldırganın bu kaynakları tüketmesi sonucunda, artık erişilemez duruma gelmesine sebep olur.

2.4 İŞLETİM SİSTEMİNE DAİR GEREKSİZ BİLEŞEN VE UYGULAMALARIN KURULUMU

Sunuculara, işletim sistemiyle birlikte birçok yan uygulama ve hizmet yüklenebilmektedir. Bu hizmet ve uygulamaların bir kısmı hiçbir zaman kullanılmayacağı gibi bir kısmı da belirli bir süre kullanıldıktan ya da test edildikten sonra kullanılmayabilir. Sunucu üzerinde kurulu olan ancak kullanılmayan bu tür hizmetler ve uygulamalar unutularak sunucu üzerinde gereksiz yük oluştururlar. Ayrıca bu uygulamalar ve hizmetler güvenlik açıkları içerebilir. Unutulan yüklü uygulamalar güncellenmezse güvenlik zafiyeti oluşturabilir.

2.5 SUNUCULARIN AŞIRI YÜK ALTINDA ÇALIŞTIRILMASI

Sunucuların kapasitesi yeterli olacak şekilde planlanmamışsa, bir noktadan sonra sunucular gereksinimleri karşılayamayacak seviyeye gelir. Bu tip sunucularda, çalışan uygulama ve hizmetlere bağlı olarak hizmet kesintisi ve veri kaybı gibi çeşitli sorunlar yaşanabilir.

Karmaşık BT mimarilerinde, tek bir sunucuda yaşanabilecek aşırı yük altında çalıştırılma durumu, hizmet kapsamında çalışan diğer sunucularda da sorunlara veya kesintilere neden olabilir.

BT sistemlerinde yaşanan aşırı yük oluşması nedenleri;

- Yanlış yapılandırılma sonucunda uygulama ve hizmetlerin gereksiz yere bellek tüketmesi,
- Mevcut depolama kapasitesinin aşılması,
- Anlık yüksek sayıda mesaj ya da isteğin gelmesi ile işlemcinin bu istekleri işleyememesi,
- Yük dengelemesinin yapılmamış olması,

şeklinde sıralanabilir.

3 GEREKSİNİMLER

"BTS.1 Sunucu İşletimi Rehberi"nin özel gereksinimleri aşağıda listelenmiştir. Temel olarak, BT operasyon ekibi bu gereksinimlerin karşılanmasından sorumludur. Buna ek olarak, Bilgi Güvenliği Birimi her zaman stratejik kararlarda yer almalıdır. Bilgi Güvenliği Birimi tüm ihtiyaçların belirlenen güvenlik politikasına uygun olarak karşılanmasını ve doğrulanmasını sağlamaktan sorumludur. Ayrıca, gereksinimlerin uygulanmasında ilave sorumlulukları olan başka roller de olabilir. Bunlar daha sonra ilgili gereksinimlerin başlığında köşeli parantez içinde açıkça listelenecektir.

Tablo 2. Sunucu Yönetimi Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Operasyon Ekibi
Diğer Sorumlular	Bina Hizmetleri, BT Yöneticisi, BT Mimari

3.1 1.SEVİYE GEREKSİNİMLER

Sunucuların işletimi için aşağıdaki gereksinimler öncelikli olarak dikkate alınmalıdır.

BTS.1.G1 Uygun kurulum [Bina Hizmetleri]

Sunucular, sadece yetkili kişilerin erişebileceği yerlerde işletilmelidir. Bu nedenle, sunucular veri merkezlerine, sistem odalarına veya kilitlenebilir sunucu kabinlerine yerleştirilmelidir. Sistem odalarına veya sunucu kabinlerine kimlerin erişim sağlayabileceği belirlenmelidir. Sunucular, istemci rolünde kullanılmamalıdır. Sunuculara, sunucuya özgü hangi çevresel envanterin bağlanabileceği netleştirilmelidir.

Asıl sunucu ile yedek sunucu kurumun ihtiyaçları doğrultusunda, fiziksel olarak ayrı konumlandırılmalıdır (örn. ayrı kabin, sistem odası, bina vb.). Bu sayede olası bir afet durumunda oluşan fiziksel hasarın etkisi azaltılmış olur.

BTS.1.G2 Kullanıcı kimlik doğrulaması

Sunucuya erişmek isteyen kullanıcıların kimlik denetiminden geçmesi zorunlu olmalıdır. Kullanıcıların ve sistem yöneticilerinin parolaları, kurumun parola politikasına uygun olarak oluşturulmalıdır. Parola politikasında, parolaların yeteri kadar karmaşık olmasına ve belirli aralıklarla değiştirilmesine yönelik düzenlemeler yer almalıdır.

BTS.1.G3 Kısıtlayıcı hakların tahsisi

Sunucularda saklanan verilere erişim kısıtlanmalıdır. Her kullanıcı sadece görevini gerçekleştirmek için ihtiyaç duyduğu verilere erişebilmelidir.

Sistem dizinleri ve dosyaları için verilen erişim haklarının kurum güvenlik politikasına uygun olup olmadığı, düzenli aralıklarla kontrol edilmelidir. Sistem dosyalarına, mümkünse yalnızca sistem yöneticileri erişebilmelidir.

BTS.1.G4 Rollerin ayrıştırılması

Yönetici haklarına sahip yetkilerin, yalnızca yönetim görevleri için kullanıldığından emin olunmalıdır. Sistem yöneticilerine, yönetim dışı görevleri gerçekleştirmeleri için sınırlı haklara sahip ek kullanıcı profilleri oluşturulmalıdır. Bu gibi durumlar dışında ek kullanıcı hesabı oluşturulmamalıdır.

BTS.1.G5 Yönetim arayüzlerinin korunması

Sunucuların yönetimi için yapılan bağlantı türüne (yerel, uzak veya merkezi) göre, uygun güvenlik önlemleri alınmalıdır. Bu güvenlik önlemleri güvenlik politikasında belirtilmelidir.

Kimlik denetimi, sunucuların güvenlik gereksinimlerine göre belirlenebilir. Mümkün olduğunca, merkezi, ağ tabanlı kimlik doğrulama yöntemleri tercih edilmelidir.

Yönetim amaçlı yapılan erişimler, güvenli protokoller kullanılarak gerçekleştirilmelidir. Bu erişimlerin, ayrı bir yönetim ağı üzerinden gerçekleştirilmesi tavsiye edilir.

BTS.1.G6 Gereksiz servislerin ve hesapların devre dışı bırakılması

Başta ağ hizmetlerinde olmak üzere, bu hizmetlerin sunumunda kullanımı gerekli olmayan bütün servisler, sunucu üzerinde devre dışı bırakılmalı veya kaldırılmalıdır. Gereksiz kullanıcı kimlikleri silinmeli veya en azından bu kullanıcı hesapları ile sisteme giriş yapılamayacak şekilde söz konusu hesaplar devre dışı bırakılmalıdır. Sunucularda bulunan standart kullanıcı hesap adları mümkün olduğunca değiştirilmelidir. Standart hesapların varsayılan parolaları değiştirilmelidir. Sunuculara erişim yetkileri sadece kullanıcılar için değil, aynı zamanda uygulamalar için de uygun bir şekilde sınırlandırılmalıdır.

Gereksiz servislerin ve hesapların devre dışı bırakılması veya silinmesine yönelik alınan kararlar anlaşılabilir bir şekilde belgelendirilmelidir. Böylece, ihtiyaç olması halinde sunucularda devre dışı bırakılan servis ve hesaplar tekrar yapılandırılabilir.

BTS.1.G7 Ürün yazılımı, işletim sistemi ve uygulamaları için güncellemeler ve yamalar

Sistem yöneticileri; işletim sistemlerinde, uygulamalarda ve hizmetlerde bilinen güvenlik açıklarını düzenli olarak kontrol etmelidirler. Tespit edilen güvenlik açıkları, saldırganlar tarafından istismar edilemeyecek şekilde mümkün olan en kısa sürede kapatılmalıdır. Yamalar ve güncellemeler yalnızca güvenilir kaynaklardan elde edilmelidir.

Güvenlik açıkları ile ilgili yamaların henüz mevcut olmadığı durumda ise, bu açıkların ve tehditlerin ciddiyetine bağlı olarak sistemi korumak için başka uygun önlemler alınmalıdır.

BTS.1.1.G8 Düzenli yedekleme

Güvenlik gereksinimlerine uygun olarak, kritiklik seviyesi yüksek olan sunucuların yedekleri düzenli aralıklarla alınmalıdır. Bunun yanı sıra, sunucuya yeni bir uygulama kurulumundan ve büyük ölçekteki konfigürasyon değişikliklerinden önce mutlaka veri yedeklemeleri yapılmalıdır. İhtiyaç durumunda yedeklerden tekrar sağlıklı bir şekilde geri dönülebileceği test edilmelidir.

BTS.1.G9 Zararlı yazılımlardan koruma programlarının kullanımı

Kurulan işletim sistemini, sağlanan hizmeti ve diğer koruma mekanizmalarını da dikkate alarak sunucuda zararlı yazılımlardan koruma programı kullanılmasının gerekip gerekmediğine karar verilmelidir. Zararlı yazılımlardan koruma programının veri tabanı düzenli aralıklarla güncellenmelidir. Tercih edilen zararlı yazılımlardan koruma programı, anlık ve düzenli aralıklarda tarama özelliklerine ek olarak, sıkıştırılmış ve şifrelenmiş dosyaları da tarayabilmedir.

BTS.1.G10 Loglama

Sunucuda hangi bilgilerin kayıt altına alınacağına, bu kayıtların nerede, ne kadar süre tutulacağına ve hangi şartlar altında kimler tarafından görüntülenebileceğine karar verilmelidir. Karar verilirken, veri koruma gereksinimleri dikkate alınmalıdır. Genel olarak, güvenlikle ilgili tüm sistem olaylarının kayıtlarının alınması zorunlu tutulmalıdır. Kayıt içeriğinde en azından aşağıdaki bilgiler mevcut olmalıdır:

- Sistemin ilk kez veya yeniden başlatılması,
- Başarılı veya başarısız oturum açma işlemleri (işletim sistemi ve uygulama yazılımı),
- Başarısız ve yetkisiz oturum açma denemeleri,
- Engellenen veri akışları (ACL'lerin veya güvenlik duvarı kurallarının ihlali),
- Kullanıcılar, gruplar ve yetkilendirmelerde yapılan değişiklikler,
- Güvenlikle ilgili hata mesajları (ör. donanım hataları, kapasite sınırlarının aşılması vb.),

- Güvenlik ve koruma yazılımlarından gelen uyarı mesajları (ör. zararlı yazılımlardan koruma programı).

3.2 2.SEVİYE GEREKSİNİMLERw

1.seviye gereksinimler sonrasında, sunucuların işletimini daha iyi bir seviyeye getirmeyi düşünen kurum veya organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

BTS.1.G11 Sunucular için bir güvenlik politikasının oluşturulması

Kurumun genel güvenlik politikasına dayanarak, sunucular için de bir güvenlik politikası oluşturulmalıdır. Politika, sunucuların tedarik ve işletilmesinde yer alan tüm yöneticiler ve çalışanlar tarafından bilinmelidir. Politikanın uygulanması düzenli olarak kontrol edilmeli ve sonuçları belgelendirilmelidir.

BTS.1.G12 Sunucu kurulumunun planlanması

Sunucu kurulumlarının planlanmasında aşağıdaki maddeler dikkate alınmalıdır:

- Donanım altyapısı, işletim sistemi ve üzerine kurulacak uygulamaların seçimi,
- Donanım kapasitelerinin belirlenmesi (işlemci, bellek, bant genişliği, disk, güç vb.)
- İletişimi sağlayacak ara yüzlerin tiplerinin ve sayılarının belirlenmesi (ör. ağ adaptörleri, depolama ağı adaptörleri)
- Güç tüketimi, oluşturduğu ısı yükü ve fiziksel olarak kapladığı alan,
- Yönetim ara yüzlerinin korunması (bkz. BTS.G5),
- Sunucuya yapılacak erişim sayısı,
- Log kayıtlarının tutulması (bkz. BTS.1.G10),
- Sistemlerin güncellenmesi (bkz. BTS.1.G7),
- Veri yedekleme, güvenlik ve koruma sistemlerine entegrasyonu (virüs koruması, IDS, vb.)

Planlama aşamasında alınan tüm kararlar, anlaşılır bir şekilde belgelendirilmelidir.

BTS.1.G13 Sunucuların tedarik edilmesi

Sunucu tedarik edilmeden önce, piyasada bulunan ürünleri değerlendirmek için bir gereksinim listesi oluşturulmalıdır.

BTS.1.G14 Kullanıcı ve yönetici kavramlarının oluşturulması

Sunucularda yapılacak yönetimsel işler için yönetici profili, normal işler için ise standart kullanıcı profili oluşturulması yaklaşımı benimsenmelidir. Farklı roller arasındaki görev ayrımının detayları, oluşturulacak kullanıcı-yönetici kavramı içinde yer almalıdır.

BTS.1.G15 Kesintisiz güç kaynağı [bina hizmetleri]

Sunucular kesintisiz güç kaynağı (UPS) ile beslenmelidir. Kesintisiz güç kaynağı, güç ve besleme süresi bakımından doğru bir şekilde ölçeklendirilmelidir. Güç tüketimini artırma yönünde herhangi bir değişiklik olduğunda (yeni sunucu ve donanım ilavesi gibi), besleme gücünün yeterli olup olmadığı tekrar gözden geçirilmelidir. Hem UPS hem de sunucuların aşırı gerilim korumasına sahip olması gerekmektedir.

UPS akülerinin gerçek kapasitesi ve azami besleme süresi düzenli olarak test edilmelidir. Ayrıca, UPS'lerin periyodik bakımları zamanında yapılmalıdır. Anlık kontrol ve izleme için UPS, uzaktan izleme ve yönetim sistemine entegre edilmelidir.

BTS.1.G16 Sunucuların güvenli kurulumu ve temel yapılandırılması

Sunucular, kullanım amacına uygun, sadece ihtiyaç olan servisler ile, gerekli yetkinliğe sahip sistem yöneticileri tarafından kurulmalıdır. Sunucu kurulumu, önceden tanımlanmış bir kurulum planına göre yapılmalıdır. Kurulum için kullanılan dosyalar, güvenli kaynaklardan temin edilmelidir. Benzer özelliklere sahip, tekrarlayan sunucu kurulumları için imajlar oluşturulmalı ve kullanılmalıdır. Tüm kurulum adımları, eksiksiz bir şekilde belgelenmelidir.

Sunucuların varsayılan ayarları gözden geçirilmeli ve gerekirse güvenlik politikasına göre yeniden yapılandırılmalıdır. Sunucu istenilen ağa ancak kurulum ve yapılandırma tamamlandıktan sonra dâhil edilmelidir.

BTS.1.G17 Uygulama kurulumu

Sunucu, canlı sisteme ve canlı ağa dâhil edilmeden önce, bir onay mekanizmasından geçmelidir. Onay işlemlerinin uygun bir şekilde belgelendirilmesi tavsiye edilmektedir. Onay sürecinde, kurulum ve yapılandırma belgeleri ile sistemin işlevselliği yetkili bir kişi tarafından test ortamında test edilmelidir.

BTS.1.G18 İletişim bağlantılarının şifrelenmesi

Sunucu tarafından sunulan servislerde şifrelenmiş bağlantı seçeneğinin kullanılabilir ve uygulanabilir olup olmayacağı kontrol edilmelidir. Mümkün olduğu durumlarda, şifrelenmiş bağlantı kullanılması tavsiye edilmektedir.

BTS.1.G19 Güvenlik duvarı yapılandırması

Kurum güvenlik politikası çerçevesinde yerel güvenlik duvarı kullanılarak; gelen ve giden iletişim isteklerinin sadece izin verilen paydaşlar ile izin verilen protokoller, portlar ve ara yüzlerden gerçekleşmesinin sağlanması tavsiye edilir.

BTS.1.G20 Ağ üzerinden erişimin kısıtlanması

Yetkisiz erişimlere karşı, kurumun bütün haberleşme ağı bir güvenlik ağ geçidi kullanılarak korunmalıdır. Dışarıya hizmet veren sunucular, bir DMZ (DeMilitarized Zone) ağında hizmet vermelidir.

Sunucular ile istemciler farklı IP bloklarında bulunmalıdır. Sunucuların yer aldığı IP bloğu, istemcilerin yer aldığı IP bloğundan en azından bir yönlendirici (router) ile ayrılmalıdır.

BTS.1.G21 İşletimin belgelenmesi

Sunucu üzerinde gerçekleştirilen operasyonel işlemler anlaşılır bir şekilde belgelenmelidir (kim, ne zaman, ne için, vb.). Özellikle, yapılandırma değişiklikleri ve güvenlik ile ilgili gerçekleştirilen işler (örn. yeni sabit disklerin takılması) yazılı kayıtlar üzerinden izlenebilir olmalıdır. Bu belgeler yetkisiz erişimlere karşı korunmalıdır.

BTS.1.G22 Acil durum eylem planlaması

Sunucular acil durum eylem süreçlerine dâhil edilmelidir. Bu amaçla, acil durum eylem planları yapılmalı ve uygun tedbirler alınmalıdır.

BTS.1.G23 Sistem izleme

Sunucular; sistem durumlarını, işlevselliklerini ve üzerinde çalışan servisleri sürekli takip eden; hatalı durumları, tanımlanmış eşik değerini aşan anormallikleri ilgili personellere raporlayan bir izleme sistemi ile izlenmelidir.

BTS.1.G24 Güvenlik kontrolleri

Sunucuların güvenlik gereksinimlerine uygunluğunu doğrulamak ve sunucularda herhangi bir güvenlik açığının olup olmadığını saptamak için düzenli olarak güvenlik testleri yapılmalıdır. Bu kontrolün uygulanması, kurum dışına hizmet veren sunucular için daha da önem arz edebilir.

BTS.1.G25 Sunucunun denetimli hizmet dışı bırakılması

Sunucular hizmet dışı bırakılmadan önce üzerindeki veriler kontrol edilmeli, sunucu diskleri üzerinde hassas veri kalmadığından emin olunmalıdır. Ayrıca, hizmet dışı bırakılacak sunucunun verdiği hizmet başka bir sunucu üzerinden sağlanmaya devam edilecekse, bu hizmetin yeni sunucu üzerinde sorunsuz bir şekilde sunulabildiği teyit edilmelidir.

Sunucuları hizmet dışı bırakırken bir kontrol listesi kullanılması tavsiye edilmektedir. Bu kontrol listesi, veri yedekleme, servis geçişi ve tüm verilerin güvenli bir şekilde silinmesiyle ilgili kontrolleri mutlaka içermelidir.

3.3 3.SEVİYE GEREKSİNİMLER

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

BTS.1.G26 Çok faktörlü kimlik doğrulama (G)

Yüksek koruma gereksinimlerinin olması durumunda, sunucuya güvenli erişimde sertifika, akıllı kart veya kimlik işareti (token) kullanılarak iki veya daha fazla faktörlü kimlik doğrulama yöntemleri kullanılmalıdır. Bu durumda, sunucuya yapılacak tüm yönetimsel erişimlerde çok faktörlü kimlik doğrulama yönteminin kullanılması tavsiye edilir.

BTS.1.G27 Sunucu tabanlı saldırı tespit sistemleri (BE)

Saldırı algılama sistemleri (IDS) sayesinde, BT sistemlerinde yapılan olağan dışı durumlar ve hatalı kullanımlar takip edilebilir. Meydana gelebilecek bu anormal durumların olumsuz etkileri Saldırı Önleme Sistemi (IPS) yardımı ile asgari düzeye indirilir. Kullanılan IDS/IPS mekanizmaları uygun şekilde seçilmeli, kapsamlı bir şekilde test edilmeli ve saldırı tespiti durumunda sorumlu personeli ivedilikle bilgilendirilecek şekilde yapılandırılmalıdır.

İşletim sistemi veya uygun ek ürünler yardımıyla, sistem dosyalarına ve yapılandırma ayarlarına erişimler kısıtlanmalı, değişiklikler izlenmeli ve bu değişiklikler hakkında ilgili birimler bilgilendirilmelidir.

BTS.1.G28 Yedeklilik (E)

Yüksek erişilebilirliğine ihtiyaç duyulan sunucular, yaşanabilecek olası sorunlara karşı uygun bir şekilde korunmalı ve yedekli bir yapıda kurulmalıdır. Bakım sözleşmelerine yedek sunucular da dâhil edilmelidir.

Farklı coğrafi bölgeler arasında otomatik yük devretme (failover) mimarileri gibi ileri düzey gereksinimlere ihtiyaç olup olmadığı kontrol edilmelidir.

BTS.1.G29 Test ortamınının oluşturulması (GBE)

Sunucuda yapılacak değişiklikleri, canlı ortamdaki çalışmayı tehlikeye atmadan test edebilmek için, uygun test ortamları oluşturulmalıdır. Test ortamı, canlı ortam ile mümkün olduğunca benzer olmalıdır (özellikle yazılım sürümleri, yapılandırma açısından). Uygulama sunucuları için yapılacak testlerde, canlı ortamdaki gizli ve kişisel bilgileri içermeyen test verileri oluşturulmalıdır.

BTS.1.G30 Sunucu üzerinde tek hizmet sunulması (GBE)

Sunucuların koruma gereksinimlerine bağlı olarak, sunulan hizmetlerin güvenlik riskini azaltmak için her bir sunucudan yalnızca bir hizmet sunulmalıdır.

BTS.1.G31 Uygulama beyaz listesi (GB)

Uygulama beyaz listesi oluşturularak, sunucu üzerinde yalnızca izin verilen uygulamaların çalıştırılması sağlanmalıdır. Bunun için izin verilen uygulamaların bulunduğu paylaşım adresleri tanımlanmalıdır.

BTS.1.G32 Ayrıcalıklı hesapların korunması (GB)

Yönetimsel hesapların parolaları, birden fazla parçaya ayrılarak her bir parçanın farklı kişiler tarafından bilinmesi sağlanmalıdır. Kritik operasyonel çalışmaların birden fazla sistem yöneticisinin katılımı ile gerçekleştirilmesine dikkat edilmelidir. Ayrıca, yönetimsel hesapların birden fazla hatalı giriş denemesi sonucunda kilitlenerek kullanılamaz hale getirilmesi prensibi uygulanmalıdır.

BTS.1.G33 Kök sertifikaların yönetimi(GB)

Sunucunun hizmet sunabilmesi için hangi kök sertifikalarına sahip olması gerektiği belirlenmeli, belgelenmeli ve düzenli olarak kontrol edilmelidir.

BTS: BT SİSTEMLERİ

BTS.1.U SUNUCU YÖNETİMİ

UYGULAMA REHBERİ

BTS.1.U SUNUCU YÖNETİMİ

UYGULAMA

1 AÇIKLAMA

1.1 TANIM

Bu rehber, BT sistemlerine hizmet sağlayan sunucular için genel güvenlik gereksinimlerini kapsar. Veri tabanı, e-posta veya yazıcı hizmetlerinin güvenli bir şekilde işletimi için de bu rehberden temel seviyede faydalanılabilir.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

Veri merkezine, mevcut sunucu alt yapısını etkileyecek yeni bir fiziksel sunucu ilave edilmesi durumunda; öncelikli olarak bir sunucu kurulum planı hazırlanmalıdır. Bu planda; sunucunun hangi amaç için kullanılacağı, sunucuda hangi işletim sistemi ve uygulamaların kurulacağı, hangi servislerin açılacağı yer almalıdır. Kurulumda yeni bir ağ yapısı oluşturulacak ise ağın genel mimarisi tasarlanmalı ve hazırlanan planda tanımlanmalıdır. Planlama süreci sonunda alınan kararlar belgelendirilmelidir.

Yeni bir ağ yapısı oluşturulacak ise ağın ayrıntılı yapısı, sonraki çalışmalar için faydalanılmak üzere detaylı olarak planlanmalıdır. Kurulumu hedeflenen sunucuların sayısı, görevleri, sunucular arasındaki etkileşimin nasıl olacağı ve sunucuların istemciler tarafından nasıl kullanılacağı belirlenmelidir. Erişilebilirlik gereksinimleri göz önünde bulundurularak, yedeklilik yapısı oluşturulmalıdır. Altyapı için gerekli olan klima, güç kaynağı vb. çevre elemanları da bu plana dâhil edilmelidir (bkz. *"BTS.1.U15 Kesintisiz güç kaynağı"*). Buna paralel olarak, sunucular için genel bir güvenlik politikası oluşturulmalıdır *(*bkz. *"BTS.1.U11 Sunucular için bir güvenlik politikasının oluşturulması"*).

Tedarik

Bir sonraki adım, gerekli olan donanımların ve ek yazılımların temin edilmesidir. Uygulama senaryolarına göre, tedarik edilecek ürünler için gereksinimler belirlenmeli ve buna bağlı olarak uygun ürünlerin seçimi yapılmalıdır.

Uygulama

Kullanıcılar ve sistem yöneticileri sunucunun güvenliği üzerinde önemli bir etkiye sahiptir. Dolayısıyla, sunucu canlı ortamda devreye alınmadan önce, kullanıcılara ve sistem yöneticilerine gerekli eğitimler verilmelidir. Planlama ve yönetimin karmaşıklığından doğabilecek sorunların azaltılması ve sistem yönetiminin tutarlı ve doğru bir şekilde yapılabilmesi için, sistem yöneticilerinin kapsamlı bir eğitim almaları önemlidir.

Kullanıcılara ise, mevcut güvenlik mekanizmalarının nasıl kullanılacağı hakkında bilgiler verilmelidir.

Planlama ve hazırlık çalışmaları tamamlandıktan sonra, sunucunun kurulumu ve devreye alınması işlemleri gerçekleştirilebilir.

Kurulum sırasında aşağıdaki önerilere uyulmalıdır:

- Sonradan telafisi zor olan hataları önlemek için, sunucunun kurulumu ve temel yapılandırması, sürecin başında dikkatli bir şekilde yapılmalıdır. Kurulum yapılırken bu rehberde açıklanan genel önlemlere ek olarak, ilgili işletim sistemiyle alakalı makalelerde önerilen ilave önlemler de dikkate alınmalı ve uygulanmalıdır (bkz. "*BTS.1.G16 Sunucuların güvenli kurulumu ve temel yapılandırılması*").
- Sunucunun, ilk kurulumu ve temel yapılandırılmasından sonra, daha üst düzey yönetim yapılandırılması gerekebilir. Örneğin bir dosya sunucusu, yazıcı sunucusu ya da terminal sunucusunda iş gereksinimlerine göre daha özelleştirilmiş bir yapılandırma gerekebilir. Bu noktada, gerek duyulmayan hizmetlerin ve hesapların devre dışı bırakılması, sunucuların kontrol edilebilir bir şekilde çalışmasını sağlamak açısından önemlidir (bkz. "*BTS.1.G6 Gereksiz servislerin ve hesapların devre dışı bırakılması*").
- Sunucunun kurulumu ve temel yapılandırması tamamlandıktan sonra, asıl kullanılacak uygulamalar kurulabilir. Uygulamaların kurulumundaki gerekli adımlar, uygulamanın türüne ve amacına bağlı olarak değişkenlik gösterebilir. Genel prensip olarak, sunucu üzerine kurulacak uygulamanın kurulum ve yapılandırmasında aşağıdaki hususlar dikkate alınmalıdır:
    - Bir kurulum konseptinin oluşturulması,
    - Benzer uygulamalara ve yapılandırmaya sahip birkaç sunucu kurulumu isteniyorsa referans sunucunun kurulması,
    - Kurulum, temel yapılandırma, güncelleme ve güvenlik açısından sıkılaştırma işlemlerinin yapılması,

İleri düzey koruma gerektiği durumlarda penetrasyon, vb. testlerinin yapılması.

İşletim

İlk kurulum yapılıp, gerekli testler tamamlandıktan sonra sunucuda normal çalışma başlatılır. Güvenlik açısından, çalışma esnasında aşağıdaki hususlar dikkate alınmalıdır:

- İstemci-sunucu ağlarında iş gereksinimlerinden dolayı sıkça değişiklik meydana gelebilmektedir. Yapılan bu değişiklikler, sunucunun güvenliğinde herhangi bir zafiyet oluşturmamalıdır. Yetkilendirme ve veriye dair yapılan değişiklikler sonrasında mevcut durumdaki veri ve erişim yetkilendirme bilgilerinin güncel olduğundan emin

olunmalıdır. Rehberin ilgili bölümlerinde, sunucu işletiminde güvenliğin sağlanmasıyla ilgili hususlar, detaylı olarak ele alınmıştır (bkz. "*BTS.1.G3 Kısıtlayıcı hakların tahsisi" ve* "*BTS.1.G21 İşletimin Belgelenmesi")*.

- Sunucunun güvenliğinin sağlanması için sistem bileşenlerini izlemek gerekmektedir. Güvenlik açıklarından ve bu açıklara karşı yapılan saldırılardan sistem yöneticileri anında haberdar edilmeli ve bu saldırılara karşı hızlı bir şekilde önlem alınmalıdır. Konuyla ilgili öneriler *"BTS.1.G7 Ürün yazılımı, işletim sistemi ve uygulamaları için güncellemeler ve yamalar"*, *"BTS.1.G10 Loglama"* ve *"BTS.1.G23 Sistem izleme"* modüllerinde bulunabilir.

Kullanım Dışı Bırakma

Sunucular, ilgili paydaşlara bilgi verilmeksizin devre dışı bırakılmamalıdır. Kesinti ve veri kaybını önlemek için, kullanıcılara doğrudan etkisi olan sunucular kullanım dışı bırakılmadan önce, kullanıcılar bilgilendirilmelidir. Detaylı bilgiler "*BTS.1.G25 Sunucunun denetimli hizmet dışı bırakılması"* kısmında verilmiştir.

Sunucuları devre dışı bırakmadan önce, üzerinde korunması gereken herhangi bir bilginin kalmaması sağlanmalıdır. Üzerinde hassas bilgi barındıran diskleri yeniden biçimlendirmek, bu bilgileri disk üzerinden tamamen silmek için yeterli değildir. Hassas verilerin istenmeyen kişiler tarafından tekrar elde edilmesini önlemek için, kapatılacak sunucu üzerinde bulunan diskler en az bir kez tamamen yeniden yazılmalıdır. Sadece mantıksal bir silmenin ve aynı zamanda kurulu işletim sistemi aracılığıyla diski yeniden biçimlendirmenin, veriyi tamamen ortadan kaldırmayacağı, bu yüzden, verinin uygun bir yazılımla kolay bir şekilde yeniden erişilebilir hale getirilebileceği göz önünde bulundurulmalıdır.

Sunucunun devre dışı bırakıldığı belgelendirilmelidir. Sistem ve sunucu ağı, son duruma göre yeniden yapılandırılmalı ve güvenlik konsepti de bu yönde güncellenmelidir.

Acil Durum Hazırlık Planı

Kapsamlı ve düzenli bir veri yedekleme yönetimi sayesinde; verinin kasıtlı veya kasıtsız silinmesi, donanım arızalarının oluşması, vb. gibi durumlarda yedekten dönüş yapılarak verinin kaybolması engellenir.

Acil durumlara hazırlıklı olmak, sistemleri koruma anlamında önemli bir rol oynamaktadır. Böylece, acil durumlarda meydana gelebilecek hasarlar en aza indirilebilir. Sunucu acil durum hazırlığıyla ilgili detaylı bilgiler "*BTS.1.U22 Acil durum eylem planlaması"* bölümünde yer almaktadır.

2 UYGULAMALAR

Aşağıdaki uygulamaların tüm sunucularda öncelikli olarak ele alınması önerilmektedir.

2.1 1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların tüm sunucularda öncelikli olarak ele alınması önerilmektedir.

BTS.1.U1 Uygun kurulum [Bina hizmetleri]

Sunucu, mümkünse bir sistem odasına veya en azından kilitli bir sunucu kabinine kurulmalıdır. Sunucu kabinlerine veya sistem odasına kimler tarafından erişim yapılabileceği belirlenmiş ve kayıt altına alınmış olmalıdır. Sunucu kabini ve sistem odası gereksinimlerini yerine getirirken "Veri Merkezi Rehberi" referans alınabilir. Ayrıca, sunuculara yalnızca belirlenmiş çıkarılabilir depolama aygıtlarının bağlanabilmesi sağlanmalıdır.

Arayüzlerin korunması

Çoğu işletim sistemi, harici depolama ortamlarını otomatik olarak tanımaktadır. Bu durum, aşağıdaki güvenlik sorunlarına neden olabilir.

- Sunucu, bağlantısı yapılan sürücü üzerinden başlatılabilir.
- Bu tür sürücüler aracılığıyla sunucuya, kontrolsüz bir şekilde uygulama yüklenebilir.
- Sunucu üzerindeki veriler dışarıya çıkarılabilir veya izinsiz şekilde kopyalanabilir.

Çıkarılabilir bir medyadan önyükleme yaparken veya üçüncü taraf bir yazılım yüklenirken; BT sisteminin kötücül yazılımlardan etkilenme riski vardır. Sistemlerin güvenliğinden sorumlu uzmanlar, bu tür tehlikeleri kurum politikalarına uygun teknik güvenlik önlemleri ile gidermelidirler. Bu tür tehlikelere karşı alınabilecek önlemler ile önlemlerin avantajları ve dezavantajları aşağıda kısaca belirtilmiştir:

Sürücüleri çıkarma

Çıkarılabilir medya bağlantı sürücülerini sunucudan çıkarmak, yukarıda belirtilen tehditlere karşı en güvenli korumayı sağlar. Sunucu için özel güvenlik gereksinimleri alınması gerekiyor ise bu çözüm düşünülebilir.

BIOS veya işletim sisteminde devre dışı bırakma

Çoğu sunucu BIOS'da, hangi sürücüden önyükleme yapılacağı ile ilgili yapılandırma seçenekleri sunar. BIOS ayarları parola ile korunarak, sistemin çıkarılabilir medyalar üzerinden kontrolsüz başlatılması önlenebilir.

Şifreleme

Yalnızca kurum tarafından izin verilmiş taşınabilir diskler ile sunuculara erişimi mümkün kılan yöntemdir. Ayrıca ilgili diskler de şifrelenerek içindeki bilgiler korunabilir.

Kullanım kuralları

Kullanıcılar, kullanım politikası kapsamında, işletim sistemindeki sürücüleri depolama alanı olarak kullanabilirler. Dolayısıyla bu sürücüler sökülmemeli, kilitlenmemeli veya devre dışı bırakılmamalıdır. BIOS'ta sadece çıkarılabilir medyaların ön yüklenmesi devre dışı bırakılmalıdır. Varsayılan sürücü ve depolama alanlarını kullanma yönergeleri, mümkün olduğu kadar açık bir şekilde tanımlanmalıdır. Örneğin, sadece herkese açık olan belgelerin kopyalanmasına izin verilebilir. Oluşturulan bu politikalar tüm kullanıcılar tarafından bilinmeli; kullanıcıların bu politikalara uyup uymadıkları izlenmeli ve kontrol edilmelidir. Çıkarılabilir bir medya üzerinden sisteme aktarılan programların yüklenmesi ve başlatılması yasaklanmalı ve teknik olarak engellenmelidir. Bu önlemlerin yanında, özellikle e-posta ve internet ağı üzerinden yapılan veri alışverişlerinin kontrol edilmesi gerekmektedir..

BTS.1.U2 Kullanıcı kimlik doğrulaması

BT sistemleri ve uygulamalarına yapılacak olan erişimlerde kullanılacak kimlik doğrulama mekanizmaları, kullanıcıları benzersiz bir şekilde tanımlayacak ve doğrulayacak şekilde tasarlanmalıdır. Kimlik doğrulama ve yetkilendirme işlemi, kullanıcı ile BT sistemi arasında herhangi bir etkileşim olmadan önce gerçekleşmelidir. Kullanıcılar başarıyla doğrulandıktan sonra erişim için yetkilendirilmelidir.

Kullanıcı kimlik doğrulaması için kullanılan çeşitli teknikler vardır. Bunlardan en çok bilinenler:

- PIN
- Parola
- Akıllı kart
- Biyometrik kontrol (parmak izi, yüz tanıma, retina tarama)

Kritik uygulamalar için parolanın yanı sıra, tek seferlik parola veya akıllı kart gibi iki veya daha fazla kimlik doğrulama tekniği birlikte kullanılarak, kimlik doğrulama güvenlik seviyesi artırılabilir. Bu yöntem, genellikle iki faktörlü kimlik doğrulama veya çok faktörlü kimlik doğrulama olarak adlandırılır. Kullanılan kimlik doğrulama teknikleri güncel teknolojiye uygun olmalıdır.

Parola Kullanımı

Kimlik doğrulama için parolalar kullanılıyorsa, BT sisteminin erişim güvenliği büyük ölçüde parolaların doğru kullanılmasına bağlıdır. Bunun için, parola kullanımına özel bir kılavuz oluşturulmalı ve bu kılavuz yayınlanmalıdır. Ek olarak, kullanıcılar farkındalık eğitimleri aracılığı ile bu konuda düzenli olarak bilgilendirilmelidir.

Kimlik doğrulama yöntemi olarak parolalar kullanıldığında, BT sisteminde aşağıdaki koşulları sağlayan mekanizmalar oluşturulmalıdır:

- Her kullanıcının bireysel parola kullanması sağlanmalıdır. Kullanıcı bu parolayı kendisi oluşturmalıdır.
- Tüm parolaların önceden tanımlanmış (ör. minimum uzunluk, karmaşıklık, özel karakterler, vb.) parola belirleme politikasına uygunluğu kontrol edilmelidir.
- BT sistemi, tanımlanan özellikleri sağlayan parolaları otomatik üretebilmeli ve bu parolaları kullanıcıya önermelidir.
- BT sistemleri, kullanıcıları parolalarını düzenli aralıklarla değiştirmeye zorlamalıdır. Parolaların ömrü ayarlanabilir olmalıdır.
- Parolayı değiştirirken eski parolaların tekrar kullanılması sistem tarafından engellenmelidir.
- Parola girilirken ekranda gösterilmemelidir.

Sistem yöneticileri yeni bir kullanıcı oluşturduktan veya mevcut kullanıcının parolasını yeniledikten sonra, kullanıcı ilk girişte parola değişikliğine zorlanmalıdır.

BTS.1.U3 Kısıtlayıcı hakların tahsisi

Sunucu yapılandırılırken, sunucuda saklanan veriye erişim hakları olabildiğince kısıtlanmalıdır. Kullanıcılara, yalnızca görevlerini gerçekleştirebilmeleri için ihtiyaç duydukları dosyalara erişim izni verilmelidir.

Genelde, bir dizine erişim hakkı tanımlandığında bu dizine ait tüm alt dizinlere de erişim hakkı otomatik olarak verilir. Bu nedenle, üst dizine erişim yetkisi çok kısıtlı durumlarda verilmelidir. Özellikle yeni yazılım kurulumu yapılırken, hakların atanması sıkı kontrollere tabi tutulmalıdır. Ayrıca, sunucu depolama alanı kısıtlıysa, bir kullanıcının sunucuda kullanabileceği maksimum depolama miktarı sınırlandırılabilir.

Erişim yetkilendirmeleri

Erişim ayrıcalıkları; yetkili bir kullanıcının belirli BT sistemlerini, sistem bileşenlerini veya ağlarını kullanmasına izin verir. Erişim yetkileri mümkün olduğunca kısıtlı bir şekilde verilmelidir. Görevlerin ayrılması ilkesi göz önünde bulundurularak, her yetkiliye görev

gereksinimlerine uygun asgari düzeyde erişim yetkisi tanımlanmalıdır. Ayrıca, personelde ve görevlerde meydana gelebilecek değişiklikler gecikmeksizin dikkate alınmalı ve kullanıcı yetkileri yeni duruma göre güncellenmelidir.

BT sistemlerine veya uygulamalarına erişim, yalnızca, yetkili kullanıcının tanımlanması (ör. kullanıcı adı, akıllı kart vb.), kimliğinin doğrulanması (parola) ve bu erişimin loglara kaydedilmesinden sonra mümkün kılınmalıdır.

Kullanıcı kimlikleri veya akıllı kartlar gibi erişim araçlarının verilmesi ve geri alınması işlemleri belgelenmelidir. Erişim ve kimlik doğrulama araçlarının (ör. çipli kart, parola) kullanımına ilişkin yönergeler de oluşturulmalıdır. Erişim hakkı olan herkes, erişim araçlarının doğru kullanımı ile ilgili bilgilendirilmelidir.

BT sistem ve uygulamalarına geniş kapsamlı erişim yetkilerine sahip sistem yöneticileri gibi kullanıcıların, hastalık veya izin durumlarında yetkilerinin geçici olarak kaldırılması önerilmektedir.

Sistem yöneticilerinin tanımlanması

Sunucu sistemlerinin çoğunda hiçbir kısıtlamaya tabi tutulmamış bir yönetici rolü bulunur. Olası hataları önlemek için, sadece gerektiğinde yönetici hesabı ile giriş yapılmalıdır. Diğer rutin işler, yönetici hesabı ile değil, normal kullanıcı hesabı ile gerçekleştirilmelidir. Ancak, bazı uygulamalara sadece yönetici hesabı ile erişilebilir. Bu uygulamalara erişim için, ilgili sistem yöneticisine rol bazlı yönetim amaçlı farklı bir hesap oluşturularak erişim yetkisi tanımlanmalıdır.

Görevlerin paylaştırılması, yapılacak düzenlemeler ve karşılıklı mutabakatlar ile, sistem yöneticilerinin tutarsız veya eksik işlemler yapması engellenmelidir. Örneğin, bir dosya aynı anda birden fazla sistem yöneticisi tarafından düzenlenemez ve değiştirilemez olmalıdır.

Sistem yöneticileri için, yalnızca sınırlı erişim haklarına sahip, yönetim görevlerini yerine getirmelerini sağlayan ek kullanıcı kimlikleri oluşturulmalıdır. Oluşturulan ek kullanıcı hesabı, sistem yöneticisinin kişisel hesabından farklı bir isimde açılmalı ve tüm yetkiler sistem yöneticisinin kişisel hesabına değil bu ek hesaba tanımlanmalıdır. Yönetim dışı rutin çalışmalar için sistem yöneticileri kişisel hesaplarını kullanmalıdır. (Bkz. *"BTS.1.U14 Kullanıcı ve yönetici kavramının oluşturulması"*)

BTS.1.U4 Rollerin ayrıştırılması

Temel olarak, normal kullanıcılar ve sistem yöneticilerinin yetkilerinde ayrım yapılmalıdır. Sistem yöneticileri BT sistemlerini yönetme yetkilerine sahipken, normal kullanıcı hesapları yalnızca işleri ile ilgili standart görevlerini yerine getirme haklarına sahip olmalıdır. Normal

kullanıcı hesapları ile ihmalkârlık sonucunda veya kasıtlı olarak BT sistemlerinde değişiklik yapılmasının önlenmesi için, bu hesaplara BT sistemlerini yönetme yetkisi verilmemelidir.

Bazı kullanıcıların; sistemlerde yedek alma, yeni kullanıcı oluşturma, parola sıfırlama gibi belli görevleri olabilir. Bu tür kullanıcılar için BT sistemlerinde tüm alanları yönetme yetkisi vermek yerine, görevlerine göre kısıtlı yetkilendirme yapılmalıdır. Bu kullanıcıların görevleri bittiğinde verilen kısıtlı yetkiler de kaldırılmalıdır.

BTS.1.U5 Yönetim arayüzlerinin korunması

Sunucuları yönetmek için farklı erişim seçenekleri bulunur. Kullanılan erişim türüne bağlı olarak, bu hususta bir dizi güvenlik önlemi alınmalıdır. Büyük ağ yapılarında, sunucuların yönetim amacı ile merkezi bir yönetim ağına dâhil edilmesi tavsiye edilir. Aksi takdirde, güvenli ve verimli bir yönetim garanti edilemez. Yönetim için kullanılan yöntemler güvenlik politikasında tanımlanmalı ve yönetim sadece güvenlik politikasına uygun olarak yapılmalıdır.

Bir sunucu aşağıdaki yöntemler kullanılarak yönetilebilir;

- Yerel konsol bağlantısı,
- Ağ üzerinden uzaktan bağlantı,
- Merkezi yönetim sistemi üzerinden yönetim.

Hangi yönetim işlemlerinin hangi bağlantı yöntemi kullanılarak gerçekleştirileceği tanımlanmalıdır.

Yerel konsol bağlantısı

Sunucu, bir sistem odasına veya en azından kilitlenebilir bir kabine kurulmalıdır. Konsolda yapılması gerekli işlemler için konsola kimlerin hangi haklar ile erişebileceği bir form aracılığıyla yazılı halde saklanmalıdır. Konsola erişimde hangi tip kimlik doğrulama yönteminin kullanılacağı ve diğer gereksinimler de dikkate alınmalıdır.

Ağ üzerinden uzaktan bağlantı

Sunucular, genellikle konsol üzerinden değil de ağ üzerinden uzak bir iş istasyonundan yönetilir. Böyle bir yönetimde, saldırganlar tarafından bir açıklık bulunarak sisteminin manipüle edilmesini önlemek için bağlantı, güvenli protokoller üzerinden yapılmalıdır. (Telnet yerine SSH, HTTP yerine HTTPS/TLS kullanımı gibi.) Diğer bir seçenek olarak, yönetim ağı diğer ağlardan ayrılmalıdır. Uzaktan yönetim, asla güvensiz bir ağ üzerinden yapılmamalıdır. Güvenlik politikası oluşturulurken de bu durum dikkate alınmalıdır. Ayrıca, iç ağda mümkün olduğu kadar, güvenli olmayan protokoller kullanılmamalıdır.

Merkezi yönetim sistemi üzerinden yönetim

Sunucunun yönetimi için merkezi bir yönetim sistemi kullanılacaksa; uzaktan yönetim için olduğu gibi bu erişim kanalı için de benzer hususlar dikkate alınmalıdır. Ayrıca, merkezi yönetim sisteminin kendisinin de buna göre yapılandırılması ve uygulanması önemlidir.

Güvenli kimlik doğrulama

Genel ilke olarak, BT sistemlerine erişmek isteyen tüm kullanıcılar, kimliklerini doğrulamak zorunda olmalıdır. Bu doğrulama işlemi, yetkisiz kişilerin sistem tarafından sunulan hizmetlere veya sistemde depolanan verilere erişimlerini engellemenin tek yoludur.

Genelde, sunucular bir ağ bağlantısı üzerinden yönetilir. Ağ tabanlı kimlik doğrulaması için gereken bilgiler bir LAN veya WAN üzerinden iletilir. Bu nedenle iletilen bu bilgilerin başkaları tarafından okunamaması ve değiştirilememesi garanti edilmelidir.

Ayrıca, bir saldırganın kayıtlı kimlik bilgilerini kullanarak giriş yapabilmesi engellenmelidir. Bu nedenle, sunucu ve istemci arasında kimlik doğrulaması için kullanılan parola kayıt edilmemelidir.

Kimlik doğrulama başarılı bir şekilde tamamlandıktan sonra; kullanıcıların yalnızca erişim izinlerine sahip oldukları hizmetlere ve verilere erişebilmeleri sağlanmalıdır.

Terminallerin iletişim veri yolunun dinlenme tehlikesi varsa, yöneticiler sadece konsol erişimi aracılığıyla işlemlerini gerçekleştirmelidir. Böylece parolalar ağ üzerinden ele geçirilemez. SSH ve yönetim amacıyla gerçekleştirilecek diğer bağlantılar, şifreli şekilde yapılmalıdır. Bu sayede uzaktaki sunucular güvenli bir şekilde yönetilebilir.

BTS.1.U6 Gereksiz servislerin ve hesapların devre dışı bırakılması

Bir işletim sisteminin standart kurulumu, normalde gerekli olmayan ve bu sebeple güvenlik açığına neden olabilen bir dizi uygulama ve servis içerebilir. Kurulumdan sonra, sistemde hangi servislerin kurulduğu ve aktif olduğu kontrol edilmelidir. Gereksiz servisler devre dışı bırakılmalı veya tamamen kaldırılmalıdır.

İşletim sisteminin kurulumundan sonra sistemde hangi servislerin çalıştığı, işletim sisteminin kendi araçları ile kontrol edilebilir. Ek olarak, sistemde hangi portların açık olduğu taranmalı ve kullanılmayan portlar kapatılmalıdır.

Güvenli oturum açma

Sunuculara güvenli oturum açma için aşağıdaki şartlar sağlanmalıdır:

- Her kullanıcının kendi kimliği ve parolası olmalıdır. Kullanıcı adı veya parolası var olmadan sunucuya erişim mümkün olmamalıdır. Kullanıcı parolası yerine, e-imza benzeri yöntemler kullanılabilir.
- Başarısız oturum açma sayısı sınırlandırılabilir olmalıdır. Belirli sayıda başarısız denemeden sonra, kullanıcı hesabı ve/veya terminal engellenmelidir. Bu uygulama, sistem yöneticileri için de geçerli olmalıdır. Konsoldan yapılan erişim denemelerinde de aynı şekilde belirli sayıda başarısız oturum açma işleminden sonra belli bir süre kullanıcı hesabı engellenmelidir.
- Son başarılı oturum açma saati, oturum açmış kullanıcıya bildirilmelidir.
- Başarısız oturum açma denemeleri, oturum açmış kullanıcıya bildirilmelidir. Bu mesajı, takip eden birkaç giriş için tekrarlamak gerekebilir.
- Son oturum kapatma saati, oturum açmış kullanıcıya bildirilmelidir.
- Şifrelenmemiş ağlar üzerinden oturum açmak için, parolaya ek olarak tek seferlik oluşturulan doğrulama kodları (PIN) kullanımı önerilir.

Gereksiz hesapları ve terminalleri engelleme ve silme

Uzun süre kullanılmayan hesaplar, eğer herhangi bir risk yoksa önce pasife çekilmeli ve sonra silinmelidir. Kaldırılan hesap ile ilişkilendirilmiş dosyaların silinmediği durumlarda, bu dosyaların yetkisiz hesaplar ile ilişkilendirilme riski oluşur.

Kullanıcıların kök dizinleri, silinmeden önce yedeklenmelidir. Bir hesap silinmeden önce veya herhangi bir durumda hesap engellendiğinde, etkilenen kullanıcı bilgilendirilmelidir. Hesaplar silinirken, kuruma ait olan dosyalar silinmeli veya diğer kullanıcılara atanmalıdır. Ayrıca, devam eden işlemlerin ve zamanlanmış görevlerin silinmesini veya başka bir kullanıcıya atanmasını sağlamak önemlidir.

Benzer şekilde, uzun bir süre kullanılmayan terminaller engellenmeli ve sonra kaldırılmalıdır.

Yeni oluşturulan bir kullanıcının hesabına, sınırlı bir süre için ihtiyaç duyuluyorsa, bu hesap yalnızca sınırlı bir süre için oluşturulmalıdır. Hesapların sadece sınırlı bir süre için açılması ve gerektiğinde düzenli aralıklarla (örneğin yıllık olarak) yenilenmesi önerilmektedir.

Sunucuda kota uygulaması

Bir sunucunun tedarik edilmesi sırasında hali hazırda yeterli depolama alanına sahip olunduğundan emin olunsa bile, uzun süreli kullanımlarda depolama alanı er ya da geç azalacaktır. Farklı kullanıcılar tarafından kullanılan BT sistemlerinde, verimli bir çalışma için mevcut kaynakların tüm kullanıcılar için bölümlenmesi gerekir.

Kullanıcılarda, çoğunlukla kendi gereksinimlerini karşılayacak depolama alanlarından daha fazlasına sahip olmak isteği gözlemlenir. Log kayıtlarının diskte yer kaplamasına ek olarak, çoğu kullanıcının eski ve gereksiz dosyalarını arşivlemeye isteksiz olması da depolama alanının gereksiz verilerle dolmasına neden olur. Bu durumun önüne geçmek için depolama alanında sınırlandırma yapılmalı ve arşivleme konusunda kullanıcılar bilgilendirilmelidir. Böylece, kullanıcı kota aşımı engellenebilir.

Talep geldikçe daha fazla depolama alanı sağlamak, basit bir çözüm olacaktır. Ancak, bu yöntem her zaman mümkün değildir. Kullanıcılar depolama alanı ile ilgili bilgilendirilmiş olsalar da gereksiz dosyaları önemli olarak görebilirler.

Kullanıcılarda olduğu gibi uygulamalar için de disk sınırlandırması tanımlanabilir. Disk sınırlandırma değerinin belirlenmesi farklı açılardan önem arz eder. Örneğin, eğer tüm kullanıcılar aynı depolama alanını kullanacaklar ise; gerekli boyut, kullanılacak depolama alanını kullanıcı sayısına bölerek hesaplanabilir. Depolama boyutu belirlenirken, kullanıcılar için çok küçük alanların tahsis edilmesi bir risk oluşturabilir. Küçük boyutta depolama alanları tahsis edildiğinde, kullanıcılar kısıtlamaları aşmak için verileri belirtilen dizinlerin dışında başka alanlarda saklamaya çalışabilirler.

Tamamlanmış projelerden elde edilen veriler düzenli bir şekilde arşivlenmeli ve canlı sistemlerde tutulmamalıdır. Öte yandan, çeşitli kullanıcı gruplarına ve uygulamalarına ne kadar depolama alanı sağlandığı belirlenmelidir. Ayrıca, bir stok rezervi planlanmalı ve gerektiğinde kullanıcılara nasıl daha fazla depolama alanı tahsis edilebileceği de belirlenmelidir. Yapılandırılan değerler belgelenmelidir. Bu dokümanlar düzenli olarak gözden geçirilmeli ve güncellenmelidir.

Disk sınırlandırma boyutu belirlendiğinde, daha yüksek bir disk alanı talebine yanıt verilip verilmeyeceği ve yanıt verilecekse ne şekilde yanıt verileceği kararlaştırılmalıdır. Bu karar, disk boyutu sınırlandırma türünün seçimine de bağlıdır. Bu sınırlandırma türleri sabit ve esnek kota olarak adlandırılabilir. Sabit kota; kullanıcıların belirlenen depolama boyutundan daha fazla alan kullanamayacağı şekilde ayarlanır. Diğer yandan, esnek kota ile kullanıcıların belirli bir süre ve belirtilen bir sınır değere kadar disk boyutunu aşmalarına izin verilir. Kullanıcılar, kendilerine ayrılan disk boyutlarını aşmaları durumunda bilgilendirilmelidir. Ayrıca, bireysel kullanıcılara ek depolama alanı tahsis edilip edilmeyeceği ve bunun nasıl yapılacağı belirlenmelidir. Bu yöntem, anlaşılır bir prosedür olarak düzenlenmeli ve bu durumlar haricinde depolama boyutları talep bazında artırılmamalıdır.

Birçok güncel işletim sistemi disk sınırlandırma boyutlarını yönetmek için varsayılan araçlar içerir. Ancak, disk sınırlandırma boyutunun ayarlanması ve yönetilmesi için ek araçlara gerek olup olmadığı değerlendirilmelidir.

BTS.1.U7 Ürün yazılımı, işletim sistemi ve uygulamaları için güncellemeler ve yamalar

Çoğu zaman, ürünlerdeki açıklar saldırganlar tarafından tespit edilir. Tespit edilen bu açıklar, sunucularda bilgi güvenliği zafiyetine sebep olabilir. Açıklar; donanımı, ürün yazılımını, işletim sistemlerini ve uygulamaları etkileyebilir. Bu güvenlik açıklarına karşı mümkün olan en kısa zamanda tedbir alınması gerekir. Bu şekilde, iç veya dış saldırılar tarafından istismar edilmeleri engellenebilir. Sistemler internete bağlı olduğunda açıkların ivedi bir şekilde ele alınmış olması özellikle önemlidir. İşletim sistemi veya yazılım bileşeni üreticileri genellikle hataları/açıkları düzeltmek için BT sistemlerine yüklenmesi gereken yamaları veya güncellemeleri yayımlarlar.

Diğer yazılımlar gibi yamaların ve güncellemelerin de yalnızca güvenilir kaynaklardan temin edilmesi önemlidir. Her sistem veya yazılım ürünü için, güvenlik güncelleştirmelerinin ve yamaların bulunduğu yerler bilinmelidir. Ayrıca, kurulu olan ürünlerin bütünlüğünü ve orijinalliğini veya dâhil edilecek güvenlik güncellemelerini ve yamaları doğrulamak da önemlidir. Kurulumdan önce, zararlı yazılımlardan koruma programı kullanılarak gerekli kontroller yapılmalıdır. Bu yöntem, bütünlüğü ve kaynağı doğrulanmış olan paketler için de uygulanmalıdır. Sistem yöneticileri bilinen güncel açıklıklarını düzenli olarak takip etmelidirler.

Güvenlik güncellemeleri veya yamalar canlı ortama hemen kurulmamalı, önce test edilmelidir. Bu testler her zaman, yüklemenin yapılacağı canlı ortamdaki sistem ile benzer bir test ortamı üzerinde yapılmalıdır. Kritik bileşenlerle veya programlarla bir çakışma ortaya çıkması durumunda, güncelleme canlı sistemin bozulmasına neden olabilir. Gerekirse, güvenlik açığından etkilenen sistemler, bu testler tamamlanana kadar başka yöntemler ile korunmalıdır. Otomatik güncelleme mekanizmaları ile içe aktarılan güncellemelerin de test edilmesi sağlanmalıdır.

Bir güncelleme veya yama yüklenmeden önce, sistemin her zaman yedeklenmesi gerekir. Böylece, sorun çıkarsa sistemin orijinal durumuna geri dönülebilir. Zaman kısıtı veya uygun bir test sisteminin eksikliğinden dolayı ayrıntılı testlerin yapılamadığı durumlarda, sistemlerin yedeklerinin alınması özellikle önem arz eder.

Her durumda, yama ve güncellemelerin kim tarafından ve hangi sebeple yapıldığı belgelenmelidir. Belge, sistemin mevcut sürüm bilgisini içermelidir. Böylece sistemin güvenlik açığından etkilenip etkilenmediği kolayca anlaşılabilir.

Bir güvenlik güncellemesinin veya yamanın, bir başka ana bileşenle veya programla uyumsuz olduğu ya da yüklenmesinin sorunlara neden olduğu saptanırsa; çalışma ile ilgili ilerlenip ilerlenmeyeceğine karar verilmesi önemlidir. Ortaya çıkan sorunlar nedeniyle bir yamanın kurulmayacağına karar verilirse, bu karar her halükârda belgelenmelidir. Ayrıca bu durumda, sistemlerdeki güvenlik açıklarının istismar edilmesini önlemek için, hangi önlemlerin alındığı açıkça belirtilmelidir. Böyle bir karar sadece sistem yöneticileri tarafından alınmamalı, karara dair üst yönetim ve bilgi güvenliği birimi ile mutabık kalınmalıdır.

Yazılım paketlerinin bütünlüğünü ve güvenilirliğini sağlamak

"Güvensiz" kaynaklardan indirilen programları dikkatsizce çalıştırmak büyük zararlara neden olabilir. Kötü amaçlı yazılımlar; parola casusluk programları veya truva atları yükleyebilir, arka kapı açabilirler. Böylece, veriler kolayca bozulabilir veya silinebilir.

Bu tür kötü amaçlı yazılımların tipik kaynakları, kendilerini ekran koruyucular, virüs tarayıcılar veya diğer yardımcı programlar olarak gösteren ve e-postalara eklenmiş eklentiler olabilir. Bunlar, çoğu zaman, aynı anda birçok alıcıya sahte e-posta adresleri tarafından gönderilir. Bu tür zararlı yazılımlar çoğunlukla internetten indirilir ve herhangi bir inceleme yapılmadan kurulurlar.

Genel prensip olarak yazılımlar, güvenilir adres ve kaynaklardan indirilmelidir. Özellikle internetten indirilmesi gerekli yama ve güncellemeler için de bu durum geçerlidir. Çoğu üretici ve dağıtıcı, bir paketin bütünlük açısından kontrolüne olanak sağlar. İndirilen paketlerin değişip değişmediğini anlamak amaçlı yapılacak bu kontrol için gerekli veri, genellikle üreticilerin web sitelerinde yayınlanır veya e-posta ile gönderilir. İndirilen bir program veya arşiv dosyasının bütünlüğü bu veri ile karşılaştırılarak teyit edilir. Bir yazılım paketi için bu imkân varsa, paket kurulmadan önce kontrol işlemi tamamlanmalıdır.

Özgünlük, bütünlük kontrolü ile yapılamaz. Bu nedenle, birçok durumda, programlar veya paketler için dijital imzalar sunulur. Buna karşılık, imzayı doğrulamak için gereken genel anahtarlar çoğunlukla üreticinin web sitesinde veya genel anahtar sunucularındadır. Anahtarlar genellikle PGP (Pretty Good Privacy) veya GnuPG (GNU Privacy Guard) programlarından biriyle üretilir.

Bazen, ilgili işletim sisteminin veya yazılımların kendi varsayılan güncelleme mekanizmaları bile, paketlerin teyidine imkân sunmayabilir. Ancak, mümkün olduğunca her bir yazılım paketini içe aktarmadan önce bir bütünlük kontrolü yapılmalıdır. Dijital imzaların güvenilirliği bütünlük sağlamalarına kıyasla daha yüksektir. Bir yazılım paketi için dijital imzalar mevcutsa, paketi yüklemeden önce kontrol edilmelidir.

Dijital imzaların kullanımı ile ilgili temel bir sorun, kullanılan anahtarın gerçekliğinin doğrulanmasıdır. Ortak anahtar, bilinen güvenilir bir kişi veya kuruluşun imzasını taşımazsa, gerçek bir güvenlik sağlamaz. Özel anahtarla oluşturulan imzaların, yazılım paketinin geliştiricisi, üreticisi veya dağıtıcısından gelmesi gerekmektedir. Bu nedenle, eğer onaylanmamışsa, ortak anahtarlar tercihen yazılım paketinden farklı bir kaynaktan, örneğin bir üreticinin CD-ROM'undan, paketin indirilebileceği başka bir ayna sunucudan veya ortak anahtar sunucusundan temin edilmelidir.

Bütünlük sağlamaları ve dijital imzaları kontrol etmek için, ilgili programlar yerel olarak mevcut olmalıdır. Sistem yöneticileri, bütünlük sağlaması ve dijital imzaların geçerliliğini kontrol etmelidir.

Farklı sebeplerden dolayı, yamaların ve güncellemelerin e-postalar ile alınması önerilmez. E-postaların kaynağının güvenirliğini ek güvenlik araçları kullanmadan belirlemek zordur ve kurumlardaki alıcı adresleri genellikle tahmin edilmesi kolay bir şekilde oluşturulur. Yamalar ve güncellemeler çok yüksek boyutlu olabilir. Birçok şirket ve kamu kurumu, e-posta eklerinin boyutunu sınırlandırmıştır ve ayrıca yürütülebilir eklerin e-posta yoluyla iletimini de yasaklayabilir. Ayrıca, büyük miktarda veri, e-posta sunucunda gereksiz yer işgal eder. Bu nedenle, özellikle kritik olabilecek güvenlik yamalarının ve yazılım güncellemelerinin e-posta yoluyla alınması uygun bir yöntem olmayabilir.

Ayrıca bazı üreticiler, güncelleme ve yama paketlerini müşterilerine doğrudan taşınabilir medyalar ile gönderme seçeneği sunabilirler. Taşınabilir medyalarda bulunan üretici logoları kolayca taklit edilebileceği için, yamalar ve güncelleme paketleri/dosyaları, bütünlük kontrolleri veya dijital imzalar ile doğrulanmalıdır.

Güncellemelerin orijinal olup olmadığını doğrulamanın bir başka yolu, üretici web sitesinde veya benzer kanallarda yayınlanan ilgili haberler olabilir. Bazı üreticiler, genellikle sistematik olarak güncellemeler hakkında bilgi yayınlarlar.

BTS.1.U8 Düzenli yedekleme

Kötü amaçlı yazılımların, donanım arızalarının, kasıtlı veya kasıtsız silme işlemlerinin ortaya çıkması durumunda dahi tüm kayıtlı verilerin kullanılabilir olması, sadece düzenli ve kapsamlı alınmış bir yedekleme işlemi ile sağlayabilir.

BTS.1.U9 Zararlı yazılımlardan koruma programlarının kullanımı

Zararlı yazılımlardan korunmak için tüm BT sistemlerinde bir güvenlik yazılımı kullanılmalıdır.

BTS.1.U10 Loglama

Sunucudaki önemli olaylar için log tutma etkinleştirilmeli ve sunucuda yer alan loglar periyodik olarak kontrol edilmelidir. Özellikle, aşağıda belirtilen güvenlik ile ilgili olaylar mutlaka kaydedilmelidir.

- Kullanıcı kimliğini kilitleyecek sayıda yanlış parola denemeleri,
- Yetkisiz erişim girişimleri,
- Güç kaybı veya ani kapanmalar,
- Ağ kullanımı ve ağdaki sorunlar ile ilgili veriler.

Günlüğe kaydedilen olayların sayısı, ilgili BT sistemlerinin koruma gereksinimlerine de bağlıdır. Koruma gereksinimi ne kadar yüksek olursa, günlükte tutulan kayıt miktarı da o kadar fazla olabilir.

Log dosyaları zaman içerisinde hızlı bir şekilde artış göstereceğinden, bu kayıtların değerlendirilmesi zorlaşacaktır. Dolayısıyla, anlamlı bir değerlendirme için, log günlüklerini değerlendirme aralıkları kısa seçilmelidir. Ayrıca değerlendirme yapılabilmesi için log kayıtlarında işlem numarası, kullanıcı kimliği, tarih ve saat bilgisi, işlem yapılan sunucu bilgisi mutlaka yer almalıdır.

Log dosyalarının saklama sürelerinin belirlenmesinde hangi yasa veya sözleşmelerin dikkate alınacağı kontrol edilmelidir. Eylemlerin izlenebilirliğini sağlamak için, asgari bir saklama süresi öngörülebilir. Ancak gizlilik nedenlerinden dolayı logların silinme yükümlülüğü de olabilir.

2.2 2. SEVİYE UYGULAMALAR

1.seviye gereksinimler sonrasında, sunucu yönetimini daha iyi bir seviyeye getirmeyi düşünen kurumlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

BTS.1.U11 Sunucular için bir güvenlik politikasının oluşturulması

Sunucular için güvenlik gereksinimleri, kurumsal güvenlik politikasını temel almalıdır. Genel güvenlik politikasına bağlı olarak, bir sunucu veya sunucu grubu için gereksinimler sunucu güvenlik politikasında belirtilmelidir. Kurum genelinde uygulanan güvenlik politikasına ek olarak, BT yönergeleri, parola yönergeleri veya internet kullanım yönergeleri gibi daha belirli yönergeler de dikkate alınmalıdır.

Güvenlik politikası, sunucuların satın alınması ve işletilmesi ile ilgili tüm kişi ve gruplar tarafından bilinmeli ve bu grupların çalışmalarının temelini oluşturmalıdır. Tüm

yönergelerde olduğu gibi, politikanın içeriği ve uygulanması daha üst düzey bir denetim ile düzenli olarak gözden geçirilmelidir.

Güvenlik politikasında, sağlanması hedeflenen güvenlik seviyesi belirtilmeli ve sunucunun işletimi hakkında temel prensipler yer almalıdır. Daha rahat anlaşılabilmesi için farklı uygulama alanlarına özel güvenlik yönergeleri geliştirmek yararlı olabilir.

Her şeyden önce, bir genel yapılandırma ve yönetim stratejisi tanımlanmalıdır. Sunucuyla ilgili alınacak kararlar öncelikle bu stratejiye bağlı olmalıdır.

Verileri sadece normal koruma gereksinimleriyle saklayan ve işleyen sunucular için, birçok durumda yapılandırma ve yönetimi basitleştiren, nispeten özgürlükçü bir strateji seçilebilir. Bununla birlikte, stratejinin her zaman için yalnızca "gerektiği kadar özgür" kılınacak şekilde oluşturulması önerilmektedir.

Hassas verileri depolayan veya işleyen sunucular için ise genellikle kısıtlayıcı bir strateji tavsiye edilir. Üç temel değerden (gizlilik, bütünlük, erişilebilirlik) biriyle ilgili özel koruma ihtiyaçları olan sunucular için kısıtlayıcı bir yapılandırma ve yönetim stratejisi uygulanmalıdır.

Bu konuda göz önünde bulundurulması gereken bazı önemli noktalar ve yararlanılabilecek çeşitli sorular aşağıda belirtilmiştir:

- Fiziksel erişim kontrol düzenlemeleri:
    - Bir sunucu her zaman bir sistem odasında veya kilitlenebilir sunucu kabininde barındırılmalıdır.
    - Sunucuya fiziksel erişimle ilgili düzenlemeler, sunucu yönetiminden sorumlu olan kişiler tarafından yapılmalıdır.
- Sunucunun sanallaştırılmasının gerekip gerekmediğine karar verilmelidir.
- Sistem yönetimi ve denetiminden sorumlu olan kişilerin çalışmalarıyla ilgili düzenlemeler:
    - Yönetim hakları hangi yönergeye göre verilir? Hangi yönetici hangi hakları kullanabilir ve bu hakları nasıl edinebilir?
    - Yöneticiler ve denetçilerin sistemlere erişim için kullanacakları araçlar (örneğin, yalnızca konsol erişimi, özel bir yönetim ağı üzerinden veya şifrelenmiş bağlantılar üzerinden erişim) nelerdir?
    - Hangi süreçlerin belgelenmesi gerekiyor? Dokümantasyon hangi biçimde oluşturulup korunur?
    - Belirli değişiklikler için en az iki kişinin onayı gerekli midir?
- Kurulum ve temel yapılandırma için özellikler:
    - Kurulum için hangi tür medyalar kullanılmalı?

- Merkezi kimlik doğrulama hizmeti mi kullanılmalı, yoksa yerel kimlik doğrulama mı yapılmalı?
- Kullanıcı ve rol yönetimi için yönetmelikler, yetkilendirme yapıları (kimlik doğrulama ve yetkilendirme süreci ve yöntemleri, kurulum için yetkilendirme, güncelleme, yapılandırma değişiklikleri vb.) belirlenmelidir. Mümkünse, yönetim için bir rol tabanlı yetkilendirme model geliştirilmelidir.
- Yüklenecek yazılım paketlerinin temel ayarları belirlenmelidir.

- Sunucu, dosya sisteminin bölümlerini şifrelemek üzere programlanmışsa, şifrelemenin nasıl yapılması gerektiğini belirlemek için aşağıdaki sorulardan yararlanılabilir:
  - Dosya sisteminin hangi bölümleri şifrelenmeli?
  - Şifreleme için hangi mekanizma kullanılmalıdır?
  - Hangi şifreleme algoritmaları ve anahtar uzunlukları kullanılmalıdır?
  - Şifrelenmiş dosya sistemlerinde hangi veriler saklanmalıdır?
  - Şifrelenmiş dosya sistemleri yedeklemeye nasıl dâhil edilir?
- Belgelerin oluşturulması ve bakımı için düzenlemeler yapılmalıdır.
- Güvenli operasyon için gereksinimler:
  - Hangi kullanıcı grubunun sistemde yerel olarak oturum açmasına izin verilir?
  - Hangi kullanıcılar ağ üzerinden erişebilir? Hangi protokoller kullanılabilir?
  - Kullanıcılar hangi kaynaklara erişebilir?
- Parola kullanımı için gereksinimler:
  - Parola oluşturulması ve yenilenmesi ilgili kurallar nelerdir?
  - Sistemi kimler kapatabilir?
- Ağ iletişimi ve hizmetleri ile ilgili düzenlemeler:
  - Yerel bir paket filtreleme programı kurulmalı mı?
  - Sunucu tarafından hangi ağ hizmetleri sunulmalı?
  - Sunulan hizmetler için hangi kimlik doğrulama yöntemleri seçilmeli?
  - Bilgisayardan hangi dış ağ servislerine erişilebilmeli?
  - Dağıtık bir dosya sistemi entegre edilecekse kullanıcı verilerinin şifrelenmemiş olarak aktarıldığı dağıtık dosya sistemleri sadece iç ağda kullanılmalıdır. Dağıtık dosya sistemi güvenli olmayan bir ağ üzerinden kullanılacaksa, ek önlemlerle (şifreli olarak korunan VPN, tünelleme) güvence altına alınmalıdır.
- Loglama ile ilgili yapılandırmalar:
  - Hangi olaylar kayıt altına alınır?
  - Log dosyaları nerede saklanmalı? Yerel olarak mı depolanmalı yoksa bu amaçla merkezi bir sunucu mu kullanılmalı?
  - Loglar nasıl ve hangi aralıklarla değerlendirilmeli?

- Log dosyalarına kimlerin erişimi olmalı?
- Kişisel verilere yetkisiz kişilerce erişilemeyeceği garanti edildi mi?
- Log dosyaları ne kadar süre saklanmalı?

Yukarıda belirtilen noktalara dayanarak, denetimlerde kullanılmak üzere bir kontrol listesi oluşturulabilir.

Güvenlik politikasının sorumluluğu, bilgi güvenliği yönetim kurulundadır. Politikada yapılacak değişiklikler ve sapmalar sadece kurul ile koordineli olarak yapılabilir.

Bir güvenlik politikası oluştururken, sistemlerin güvenliği için en yüksek gereksinim ve en olumsuz koşullar temel alınarak ilerlenmelidir. Bunlar, daha sonra gerçek koşullara uyarlanabilir. Böylece gerekli tüm unsurların dikkate alınmasını sağlanabilir.

BTS.1.U12 Sunucu kurulumunun planlanması

Bir sunucunun güvenli bir şekilde çalışması için temel gereksinimler yeterli düzeyde planlanmalıdır.

Bir sunucunun kullanımı için planlama, yukarıdan aşağıya tasarım ilkesine göre birkaç adımda gerçekleştirilebilir. Planlama tüm sistem için üst seviye bir bakış açısıyla, alt bileşenler için ise daha somut adımlar içerecek şekilde yapılmalıdır. Planlama, yalnızca güvenlik ile ilgili klasik hususları değil, aynı zamanda rutin işleri de kapsamalıdır.

Temel olarak aşağıdaki sorular üst seviye bir bakış açısıyla ele alınabilir:

- Sunucunun planlanan görevleri nelerdir? Sunucu hangi hizmetleri sağlamalıdır? Sistemin kullanılabilirliği, saklanan veya işlenmiş verilerin gizliliği ve bütünlüğü ile ilgili özel gereksinimler var mıdır? Bu spesifikasyonlar genel planlamadan gelir ve genel hedefleri belirler. Genel koşullar ne kadar kesin olarak bilinir ve gereksinimler ne kadar kesin olarak formüle edilirse, takip eden planlama adımları da o kadar kolaylaşır.
- Sistemde belirli donanım bileşenleri mi kullanılmalıdır? (Bu durum işletim sisteminin seçimi için önemli olabilir.)
- Donanımlar için hangi gereksinimler (CPU, ana bellek, veri ortamının kapasitesi, ağ kapasitesi, vb.) temel gereksinimlerdir?
- Sunucu nasıl bir ağa dâhil edilecek?
- Kurulacak sunucu eski veya mevcut olanın yerini mi alıyor? Veriler ve donanım bileşenleri eski sistemden aktarılmak istenir mi?
- Veriler yerel olarak mı saklanacak, yoksa bir SAN (depolama alan ağı) sisteminde mi depolanmalı?
- Sanal sunucu kullanılacak mı?

Sunucu dağıtımını planlarken aşağıdaki konular ve sorular dikkate alınmalıdır:

- Kimlik Doğrulama ve Kullanıcı Yönetimi

  Sistemde nasıl bir kullanıcı yönetimi ve kullanıcı kimlik doğrulaması yapılacaktır? Kullanıcılar sadece yerel olarak mı yönetilmeli yoksa merkezi yönetim sistemi mi kullanılmalıdır? Erişim denetimi merkezi, ağ tabanlı bir kimlik doğrulama servisiyle mi yoksa yerel kimlik doğrulama sistemiyle mi yapılmalıdır?
- Kullanıcı ve grup kavramı

  Organizasyon bazında kullanıcı, haklar ve rol tabanlı yetkilendirme kavramına dayanarak, sistem için uygun kurallar oluşturulmalıdır.
- Yönetim

  Sistem nasıl yönetilmelidir? Tüm ayarlar yerel olarak mı yapılmalı yoksa merkezi yönetim ve konfigürasyon yönetimi ile mi yapılmalıdır?
- Disk yapılandırma ve dosya sistemi

  Planlama aşamasında, disk alanı ihtiyacı ortaya konmalıdır. Yönetim ve bakım kolaylığı için, işletim sistemini (sistem dosyaları ve yapılandırması), uygulama programlarını ve verilerini (ör. veri tabanı sunucusu ve verileri) kullanıcı verilerinden olabildiğince ayırmanız önerilir. Çeşitli işletim sistemleri bunun için farklı mekanizmalar sunar (Windows işletim sisteminde disklerin yapılandırılması, Unix işletim sistemlerinde dosya sistemleri).
- Gizlilik gereksinimi yüksek olan veriler sunucuda saklanırsa, şifrelenmiş dosya sistemlerinin kullanılması şiddetle önerilir. Her zaman tüm dosya sistemini şifrelemek gerekmeyebilir, bazı durumlarda verilerin saklandığı dosya sisteminin belirli kısmını şifrelemek yeterli olabilir. Uygun bir planlama ile bu işlem kolaylıkla gerçekleştirilebilir. Planlama aşamasında alınan kararlar belgelenmelidir.
- Ağ Hizmetleri ve ağ bağlantısı

  Sunucuda saklanan veya işlenen veriler için gizlilik, bütünlük ve erişilebilirlik gereksinimlerine bağlı olarak, sunucunun ağ bağlantısı planlanmalıdır. Genel olarak sunucunun, sunucudan hizmet alan istemcilerle aynı IP bloğuna konumlandırılması önerilmez. Sunucu istemcilerden en az bir yönlendirici ile ayrıştırılırsa, erişimi denetlemek ve olası sorunları tespit edebilmek açısından ağ trafiği anomalilerini algılamak daha kolay olacaktır.

  Yüksek düzeyde gizlilik veya bütünlük koruması gerektiren verileri depolayan veya işleyen bir sunucu, kendine has bir IP bloğunda bulunmalıdır veya en azından ağın geri kalanından bir güvenlik duvarı ile ayrılmalıdır. Çok yüksek koruma gereksinimi olan bu tür sunucular için uygulama seviyesinde güvenlik sağlayan bir ağ geçidi kullanımı da ayrıca önerilir.

Normal koruma gereksinimlerinin olduğu durumda, yalnızca iç ağdaki istemciler tarafından kullanılan bir sunucu, istisnai bir durum olarak istemciler ile aynı ağda bulunabilir. Ancak, bu durumda, ağ yapısında değişiklikler yapılacağı zaman sunucunun ayrı bir ağa yerleştirilmesi tavsiye edilir.

Sunucunun, planlanan amacına bağlı olarak, ağdaki belirli hizmetlere (Web, dosya paylaşımı, veri tabanı, DNS veya e-posta gibi) erişmesi gerekebilir. Bu durum, planlamanın bir parçası olarak dikkate alınmalıdır, böylece yetersiz iletim kapasiteleri veya aradaki güvenlik ağ geçitleri sebebi ile oluşabilecek sorunların en baştan önüne geçilmiş olur.

Bir sunucunun üzerine kurulan asıl servise ek olarak, sunucuyu verimli bir şekilde kullanmak ve yönetmek için genellikle başka servisler de kurulabilir. Örneğin, ağ üzerinden yapılacak uzaktan yönetim güvenli bir erişim (ör. SSH) gerektiriyor veya dosyalar ağ üzerinden web sunucusuna aktarılıyor olabilir. Yapılan bu işlemler güvenli olmayan ağlar üzerinden gerçekleşecekse, verilerin şifreli bir şekilde iletildiği uygun güvenli protokoller kullanılmalıdır. Ayrıca, bu tür bağlantılar yalnızca yetkili kullanıcılar ve bilgisayarlar için kullanılabilir hale getirilmelidir. Bu yetkilendirme, bir güvenlik duvarı veya diğer güvenlik mekanizmaları kullanılarak gerçekleştirilebilir. Özellikle gerekmedikçe, internet gibi güvensiz bir ağda hiçbir hizmet verilmemelidir.

Planlama aşamasında, ağ bağlantısı için gerekli olacak servisler ve bağlantı tipleri belirlenmelidir. Genel olarak bu aşamada, çalışacak olan sistemin ağ bağlantısına olan bağımlılığını hesaba katmak büyük önem taşır.

- Tünel veya VPN

  Planlama aşamasında, sisteme güvensiz ağlar üzerinden erişilmesi gerektiği öngörülebilir ise uygun çözümler önceden araştırılabilir. Örneğin, bir VPN çözümü geliştirilebilir.
- Sunucuların İzlenmesi

  Sistemin ve sunulan hizmetlerin erişilebilirliğini ve kullanım durumunu takip etmek için, bir izleme sistemi kullanılabilir. Genellikle, bir izleme hizmeti, izlenmesi istenen sistemlere yüklenmiş bir ajanın izlenecek verileri gönderdiği başka bir sunucuya kurulur. Harici sistemlerin sunduğu ağ hizmetlerinin aktivitelerini izlemek de mümkündür. Böylece olası yaşanacak bir sorun durumunda sistem yöneticileri otomatik olarak uyarılabilir.
- Log yönetimi

  Sistemlerden gelen mesajların ve kullanılan hizmetlerin loglanması, arızaların tespitinde, düzeltilmesinde, siber saldırıların tespitinde ve bu sorunların

çözümlenmesinde önemli bir rol oynar. Planlama aşamasında hangi bilgilerin loglanması gerektiğine ve bu logların ne kadar süreyle saklanacağına karar verilmelidir. Ayrıca, logların sistem üzerinde yerel olarak mı yoksa ağdaki bir log sunucusunda merkezi olarak mı depolanacağına karar verilmelidir. Log verilerinin hangi sıklıkla ve nasıl değerlendirileceğini önceden belirlemek faydalı olacaktır.

- Yüksek Erişilebilirlik
  Eğer sunucunun sağladığı hizmetlerde bir kesinti yaşanmaması gereksinimi varsa, planlama aşamasında bu ihtiyacın ne şekilde karşılanacağı da analiz edilmelidir.

Planlama aşamasında alınan tüm kararlar uygun ve anlaşılabilir bir şekilde belgelenmelidir.

BTS.1.U13 Sunucuların tedarik edilmesi

Sunucunun tedarik süreci, sunucuyla ilişkili donanım ve yazılımları etkilediğinden bu sürecin iyi yönetilmesi gerekmektedir. Bu süreçte meydana gelebilecek olası hatalar, sunucu aracılığıyla verilen hizmetin güvenliğinde ciddi sorunlar doğurabilir. Çünkü donanım ve yazılımla uyumlu olmayan bir sunucu, arzu edilen güvenlik seviyesine ulaşılmasını zorlaştıracaktır.

Bir sunucu temin edilmeden önce, piyasadaki ürünlerin değerlendirileceği bir gereksinim listesi oluşturulmalıdır. Bu değerlendirmeye dayanarak, tedarik edilecek sunucunun pratikteki çalışma koşullarını karşıladığından emin olunmalı ve satın alma kararı, teyit işlemi sonrasında verilmelidir.

Sunucuların işlevsel özellikleri de bilgi güvenliği açısından etkili olabilir. Örneğin bir sunucu, bellek kapasitesi yetersizliğinden dolayı istenen sürelerde yanıt veremez ise erişilebilirliği etkilenmiş olur. Buna ek olarak, güvenlik açıkları ile ilgili yamalar üretici tarafından derhal sağlanmazsa sistem, saldırılara karşı korunmasız hale gelebilir.

Bilgi güvenliği açısından sunucudaki temel gereksinimler aşağıda belirtilmiştir:

- Donanım ve yazılım; sunucu erişilebilirliği ve veri bütünlüğü gereksinimlerini karşılamalı,
- Sunucunun güvenli protokollerle yönetimi mümkün olmalı,
- Kullanıcı yönetimi, kurum genelinde uygulanan rol tabanlı yetkilendirme modeline göre yapılandırılabilir olmalı,
- Özellikle hassas veriler şifrelenebilir olmalıdır.

Sunucuları tedarik ederken dikkate alınması gereken bazı gereksinimler ve bu gereksinimlere ilişkin sorular şunlardır:

- Temel fonksiyonel gereksinimler
    - Sunucu gerekli tüm donanım ara yüzlerini destekliyor mu?
    - Sunucu üzerinde gelecek yazılımlar gerekli protokolleri ve veri türlerini destekliyor mu?
    - Güvenlik gereksinimlerini sağlıyor mu?
    - Sistem yönetimi için güvenli protokolleri destekliyor mu?
- Bakım
    - Üretici, donanım ve yazılımda meydana gelen arızaların çözümünde yeterli destek sağlıyor mu?
        - Üretici, kullanım süresi boyunca, sunucu desteğini sağlamalıdır
    - Üretici, ürün yazılımı için güvenlik yamaları ve güncellemeleri düzenli olarak sağlıyor mu?
        - Üreticinin bilinen güvenlik açıklarına karşın derhal tepki vermesi önemlidir.
    - Ürün, bakım sözleşmesi seçeneği sunuyor mu?
        - Üreticinin sağladığı güncellemelerden ve destek hizmetlerinden faydalanmak çoğu zaman bir bakım sözleşmesiyle mümkün olabilir.
    - Bakım sözleşmesinde, sunucuda meydana gelen problemlerin çözümü için geçerli maksimum süreler belirlenmiş mi?
        - Sunucuda bir problem yaşandığında; üreticinin çağrılara yanıt süreleri, ürünü tekrar devreye alma süreleri ve çözümün kabul edilmesi için asgari gereksinimler bakım sözleşmesi içerisinde mevcut olmalıdır.
    - Üretici, problem yaşanması durumunda yardımcı olmak üzere bir teknik destek hizmeti (telefon hattı vb.) sunuyor mu?
        - Bu madde bakım sözleşmesinde mutlaka bulunmalıdır. Sözleşmeyi imzalarken, üreticinin hangi dili kullanarak destek vereceğine dikkat edilmeli ve uygun dil seçimi yapılmalıdır.
- Güvenilirlik / Yüksek Erişilebilirlik
    - Donanım ve yazılımın güvenilirliği yetkin kuruluşlar tarafından onaylanmış mı?
    - Üretici yüksek erişilebilirlik çözümleri sunuyor mu?
        - Bakım sözleşmesi ile yüksek erişilebilirlik gereksinimleri tam olarak karşılanamıyorsa, sistemin kendisinde yüksek erişilebilirlik mimarisi için çözümler bulunmalıdır.
- Kullanıcı dostu
    - Ürün kolayca kurulabilir, yapılandırılabilir, yönetilebilir ve kullanılabilir mi?

- Ürünün kullanımı ile ilgili eğitim sunuluyor mu?

- Maliyetler
  - Donanım ve yazılım için başlangıç maliyetleri nelerdir?
  - Beklenen işletme maliyetleri (bakım, işletme, destek, vb.) nelerdir?
    - Bu aşamalar, satın alma sürecinde dikkate alınmalıdır. Bakım ve destek sözleşmelerinin içeriği kontrol edilmelidir (çözüm süreleri, telefonla destek hattı, destek personeli nitelikleri, vb.).
  - Personel için beklenen maliyetler hesaplandı mı?
  - Ek yazılım veya donanım bileşenlerinin satın alınması gerekiyor mu?
    - Bu sorunun, planlama aşamasında yanıtlanması gerekmektedir. Örneğin, hali hazırda kullanımda olan bir sisteme yeni bir cihaz alınacaksa; tedarik edilecek cihazın mevcut sistem ile uyumluluğu kontrol edilmelidir. Ek olarak, mevcut bir altyapıya entegrasyon için harcanacak efor da göz önünde bulundurulmalıdır.
  - Sistem yöneticilerinin eğitim maliyeti ne kadar?
  - Kapasite artırma gereksinimi nedeniyle donanımın yükseltilmesi gerekiyorsa ne gibi maliyetler öngörülüyor?
    - Böyle bir durumda beklenen maliyet, donanıma sahip olma maliyetinden daha yüksek olabilir. Çünkü yeni bir donanım, yeni bir lisans gerektirebilir.

- Log yönetimi
  - Hangi loglama seçenekleri mevcut?
  - Sunulan loglama seçenekleri güvenlik politikasında asgari düzeyde belirtilen gereksinimleri karşılamalıdır. Özellikle, aşağıdaki hususlar dikkate alınmalıdır:
    - Logların ayrıntı düzeyi yapılandırılabilir mi?
    - Tüm ilgili veriler kaydedilebiliyor mu?
    - Sistem, merkezi log tutmayı destekliyor mu (ör. syslog)?
    - Log tutma işlemi, bilginin korunması yönündeki gereklilikleri yerine getirerek mi yapılıyor?
    - Uyarı özellikleri destekleniyor mu?

- Altyapı
  - Sunucu ebatları kabinlerin boyu ile uyumlu mu?
    - Bir sunucunun boyutları satın alma sırasında dikkate alınmalıdır.
    - Sunucunun mevcut kabinler ile kullanılabilir olup olmadığı dikkate alınmalıdır (ağırlık, ebat, vb.).

- Güç ve ısı yükü hesaba katıldı mı?
  - Üretici, sunucunun güç tüketimi ve ortam sıcaklığı gereksinimleri hakkında bilgi sağlamalıdır. Sunucun bağlı bulunduğu güç kaynağı ve UPS'in yeterliliği kontrol edilmelidir. Mevcut olan soğutma kapasitesinin de gerekli çalışma ortam koşullarını sağlayıp sağlayamayacağı kontrol edilmelidir.

Tedarik sürecinde verilen kararlar, gerekçeleri ile birlikte, anlaşılır şekilde belgelenmelidir.

BTS.1.U14 Kullanıcı ve yönetici kavramının oluşturulması

BT sistemlerinde bulunan yönetici ve kullanıcıların görevleri; süreçler, koşullar ve gereksinimler bakımından farklılık göstermektedir. Dolayısıyla sistemlerde yönetici ve kullanıcılar için farklı roller oluşturulmalıdır. Rollere atanan kullanıcılar mutlaka belgelendirilmeli ve bu belgelerde aşağıdaki bilgiler mevcut olmalıdır.

Yetki verilen kullanıcılar:

- Verilen yetkinin türü (Eğer gerekli ise kullanıcının standart yetkilendirme profilinden farkları),
- Yetkinin verilmesine neden olan gerekçeler ve varsa istisnai durumlar,
- Atanan yetkinin başlangıç ve bitiş tarihleri.

Yetki verilen gruplar:

- İlişkili kullanıcılar,
- Yetkinin atanma zamanı ve nedeni,
- Atanan yetkinin sona erdirileceği tarih.

BTS.1.U15 Kesintisiz güç kaynağı [bina hizmetleri]

Kesintisiz güç kaynakları (UPS), BT sistemlerini, kısa süreli enerji kesintilerinin olumsuz sonuçlarına karşı korur. UPS'ler küçük BT yapıları için, yerel olarak, ilgili donanıma özel bir şekilde kullanılabileceği gibi büyük BT yapılarında, yerleşkedeki tüm bina için de kullanılmak üzere merkezi olarak kurulabilirler.

UPS'lerin besleme süresi, bağlı cihazların ihtiyaç halinde açma ve kapama süreleri göz önünde bulundurularak hesaplanmalıdır. Eğer UPS arkasında bir jeneratör var ise, UPS için 15 dakikalık besleme süresi yeterli kabul edilebilir.

UPS ile beslenen BT altyapısında, donanımsal olarak herhangi bir değişiklik yapıldığında, UPS'in mevcut besleme süresinin yeterli olup olmadığı kontrol edilip, tekrardan hesaplanmalıdır.

UPS'ler, ani kesintilere karşı koruması olmayan offline UPS ve kesintilere karşı her an koruma sağlayan online UPS olarak kullanımda farklılık gösterebilir.

UPS'ler aşırı gerilime karşı tam anlamıyla koruma sağlayamazlar. Bunun için, aşırı gerilim koruma sistemleri mevcuttur. Diğer elektrikli cihazlar gibi, UPS'ler de aşırı gerilimlere karşı korunmalıdır.

Topraklamayla ilgili yaşanabilecek olası sorunlardan kaçınmak için; UPS ile beslenen BT donanımları, UPS'den beslenmeyen BT donanımlarına bağlanacaksa, bu bağlantı korumalı kablolarla yapılmalıdır.

UPS akülerinin çalışması için en uygun sıcaklık aralığı 20-25°C'dir. UPS aküleri bu sıcaklık aralığında bulundurulmadığı durumlarda akülerin ömrü, azami dayanma süresi olan 5 yıldan daha az olacaktır. Bu çalışma süresi boyunca, aküler sürekli olarak güç kaybederler. Bu yüzden, beklenen besleme süresini tam anlamıyla sağladığından emin olmak için, yılda en az bir kez UPS'lerin besleme süresi ve gücü hesaplanmalıdır. Bazı UPS'ler, varsayılan test mekanizmalarına sahiptir.

Diğer tüm elektrikli donanımlarda olduğu gibi, UPS sistemlerinin de üreticisi tarafından belirtilen sıcaklık aralıklarında çalışmasına dikkat edilmelidir. Bu durum, UPS için kullanılacak iklimlendirme sisteminin ölçeklendirilmesi esnasında dikkate alınmalıdır.

BT sistemlerini elektrik kesintisine karşı koruyan önemli unsurlardan biri UPS'ler olduğundan, BT sistemlerinin erişilebilirliği için büyük öneme sahiptirler. Dolayısıyla, bir UPS, beslediği BT sistemleri ile aynı koruma gereksinimlerine sahip olmalıdır. Beslediği BT sistemleri yedekli ise, UPS sistemleri de yedekli olmalıdır.

Buna ek olarak UPS, yetkisiz kişilerin erişimine, yangın ve suya karşı korunmalıdır. Yangına karşı tam anlamıyla koruma sağlamak için, yedekli UPS ünitelerini ayrı yangın bölmelerinde tutmak gerekir.

UPS'lerin bakımları üreticisi tarafından önerilen bakım aralıklarına uyularak, düzenli olarak yapılmalıdır.

Yüksek gerilim koruması

Elektrik şebekesindeki bazı cihazlar ve yıldırım düşmesi, başlıca karşılaşılan yüksek gerilim sebepleridir.

TS EN 62305 "Yıldırımdan korunma" standardı yapıların yıldırımdan korunmasıyla ilgili genel başvuru kaynağı olarak kullanılabilir. Yüksek gerilimden koruma sağlamak için, bu standart temel alınarak yıldırım ve yüksek gerilimden koruma önlemleri alınmalıdır.

TS EN 62305 standardının 2. bölümünde yer alan "Risk Yönetimi" genel anlamda risk odaklı yıldırım ve yüksek gerilimden korunmanın yollarını tanımlar. Bölüm 3, "Binalarda Elektrik ve Elektronik Sistemler" ile ilgiliyken bölüm 4 ise "Yapıların ve Kişilerin Korunması" ile ilgilidir.

BTS.1.U16 Sunucuların güvenli kurulumu ve temel yapılandırması

Sunucuyla ilgili bütün planlamalar tamamlanıp bir güvenlik politikası oluşturulduktan sonra, sunucu kurulumlarına başlanabilir.

Sunucu kurulumları sadece yetkin kişiler tarafından yapılmalıdır (sistem yöneticileri veya sözleşmeli alt yükleniciler). Kurulumu yapacak sistem yöneticileri ve ilgili çalışanlar, dikkatli bir şekilde seçilmelidir. Yönetimsel görevleri yerine getirmek için belirlenen hesaplar konusunda üst yöneticiler bilgilendirilmelidir. Teknik personeller; donanım, yazılım ve sunucu üzerinden verilen hizmetlerin sunulmasında önemli rol oynamaktadır. Bu sebeple, bu personellerin yokluğunda yaşanabilecek olumsuz bir durumda, hizmetin devamlılığı için gereken önlemler hesaba katılmalı ve önceden planlanmalıdır. Bunun için, sunucu hizmetlerinde görev alan tüm personeller, mevcut mimariye hâkim olmalı ve bu yapıyı yönetmek için gerekli olan parolalara ve anahtarlara erişebilmelidirler.

Fonksiyonel gereksinimlere ve güvenlik yönergelerine bağlı kalınarak öncelikle temel bir kurulum planı oluşturulması tavsiye edilmektedir. Kurulumun iki aşamada yapılması önerilir:

- Temel olarak belirlenen sistemlerin kurulup yapılandırılması,
- Gerekli diğer hizmetlerin ve uygulamaların kurulması.

Benzer adımların her bir sunucu için tekrar tekrar yapılmasına gerek kalmamalıdır. Sunucu kurulumuyla ilgili gerekli adımlar belirlenmeli; belirlenen bu adımlar, bir referans sistemi üzerinde özenle uygulanarak, sistem yapılandırılmalıdır. Sonraki süreçte, kurulumu tamamlanan referans sistem gerektiği kadar çoğaltılabilir. Bu sayede, sürekli tekrarlamadan kaynaklı oluşabilecek hata riski en aza indirilir.

Kurulum ve yapılandırma adımları hassas bir şekilde belgelenmelidir. Böylece, ilgili işletim sistemi için özelleştirilmiş bir kurulum planı elde edilmiş olur. Bu kurulum planının kontrol edilerek, gerektiğinde (hizmet paketleri, güncelleme sürümleri, vb.) güncellemelerin yapılmasına dikkat edilmelidir.

Yukarıda anlatılan kurulum planı, sanal sunucular için de uygulanabilir. Referans olarak hazırlanmış bir sanal sunucu, bir sanal sunucu şablonuna (template) dönüştürülür. Sonraki süreçlerde, hazırlanan bu şablon, tekrar tekrar kopyalanarak, üzerine istenilen servisler, uygulamalar ve yazılım paketleri kurulabilir. Ayrıca, sık talep edilen servis ve

uygulamalara özel, daha özelleştirilmiş bir sanal sunucu şablonu oluşturulabilir. Böylece, tekrar eden operasyon yükü en aza indirilmiş olur. Sanal sunucu altyapılarının; esneklik, operasyonel iş yükünün azaltılması, verimlilik ve hız anlamında avantaj sağladıkları için kullanılmaları tavsiye edilmektedir.

Kurulum

Bu bölüm, sunucu kurulumlarında takip edilmesi önerilen temel adımları içermektedir, ileri düzey ve özelleştirilmiş kurulum adımlarını içermemektedir. Belirli bir amaca yönelik kurulumlarda, temel düzeyin dışındaki adımlar, sunucu üzerine kurulacak servis ve uygulamaya göre farklılıklar gösterebilir.

Sunucu kurulumlarında, daha sonraki süreçlerde sorunlara neden olabilecek adımlar çok iyi düşünülmeli ve net bir şekilde belirlenmelidir. Bu sebeple, sunucu kurulumlarının temel adımları için bir kontrol listesi hazırlanmalıdır. Kurulumun ileri düzey adımları olan ağ ayarları, performans ayarları gibi ayarlar ise haricen belirtilebilir. Tamamlanan yapılandırma adımları, kontrol listesi üzerinden işaretlenerek kuruluma devam edilmelidir. Kontrol listesinde, tercihen görsel ve video içerikler de kullanılabilir.

Kurulum sonunda, gerçekleştirilen yapılandırmalar belgelenmelidir. Hazırlanan dokümanlar; yetkinlik seviyesi daha az olan kişiler tarafından da okunabileceği için, dokümanlarda her düzeyden kişinin anlayabileceği bir dil ve biçim kullanılmalıdır.

Sunucu kurulumlarında, DVD'ler veya benzer taşınabilir medyalar kullanılacaksa, yüklemenin ve temel yapılandırmanın çevrimdışı veya güvenli bir ağda gerçekleştirilmesi önerilir.

İşletim sisteminin kurulum dosyalarının güvenli bir kaynaktan temin edilmesi önemlidir. Bu durum, kurulum dosyaları internetten indirildiğinde daha da önem kazanmaktadır. İnternetten temin edilen kurulum dosyalarının bütünlüğünü ve orijinalliğini dijital imzalar yardımıyla kontrol etmek gereklidir. Dijital imza veya bütünlüğünün doğrulanma imkânı bulunmayan dosyalar ve imajlar, mümkünse kullanılmamalıdır.

Disk bölümleri yapılandırılırken, tasarım aşamasında oluşturulan plan uygulanmalıdır. Şifrelenmiş bir dosya sistemi kullanılacaksa, veri kopyalanmadan önce disk bölümü şifrelenmelidir. Ayrıca diskler, RAID (Redundant Array of Independent Disks) olarak yapılandırılacaksa, bu yapılandırma, dosya sistemleri kurulmadan önce gerçekleştirilmelidir.

Sistem olaylarının kayıt altına alınması daha önceden aktif hale getirilmedi ise, temel kurulum tamamlandıktan sonra aktif hale getirilmelidir. Kurulum ve yapılandırma sırasında sorun yaşanması durumunda, ilgili kayıtlar sorunların çözümü için kritik bilgiler sağlayabilir.

Güncelleme

Sunucu sisteminin kurulumu CD, DVD veya çevrimdışı bir medya ile yapılmış ise, kurulumdan sonra herhangi bir güncellemenin veya güvenlik yamasının üretici veya dağıtıcı tarafından yayınlanıp yayınlanmadığı kontrol edilmeli ve gerekli durumlarda referans sistem (veya şablon) güncellenmelidir. Bu sayede, kurulumu gerçekleştirilen sistem, en güncel hali ile hizmete alınmış olacaktır.

İlgili sunucu servislerinin ve uygulamaların kurulumu

İşletim sistemi kurulup, temel yapılandırma ve güncellemeler tamamlandıktan sonra sunucu üzerine istenilen servisler ve uygulamalar kurulabilir. Sunucuların uzaktan yönetimi için bazı ayarların yapılması gerekir. Hizmete almadan önce işletim sisteminin güvenlik sıkılaştırılmalarının yapılması önerilir.

BTS.1.U17 Uygulama kurulumu

Sunucu canlı ortama alınmadan önce, üzerinde çalışacak uygulamaların kurulumları tamamlanmalı ve yapılan işlemler belgelenmelidir. Kurulumun doğru yapılıp yapılmadığı, kurulum sonrası işlevsellik testleriyle tespit edilmelidir. Bu işlemler, kurumda bunu yapmaya yetkili bir grup veya birim tarafından haricen yürütülebilir.

Bir güvenlik güncellemesinin veya yamanın sistemde herhangi bir soruna neden olduğu tespit edilirse, ne yapılması gerektiği önceden belirlenmelidir. Olası bir problemden dolayı, güncellemenin kurulamayacağına karar verilecek olursa, bu karar ilgili birimlerin onayıyla yazılı hale getirilmelidir. Ayrıca, eğer uygulanmamasına karar verilen güncelleme bir güvenlik açığıyla ilgiliyse, güncelleme uygulanmadığı durumda bu açığa karşı nasıl önlem alınacağı da belirlenmelidir. Bu gibi kararlar güvenlik açısından yüksek risk barındırdığı için kurumda konuyla ilgili olan diğer birimler ve yöneticilerle birlikte çalışılmalıdır.

BTS.1.U18 İletişim bağlantılarının şifrelenmesi

Sunucular arası ve sunucuya yapılan bütün bağlantılar mümkünse şifrelenmelidir. Ağ hizmetlerini şifrelemenin en yaygın yollarından biri Taşıma Katmanı Güvenliği (TLS) kullanımıdır.

TLS ve Güvenli Soket Katmanı (SSL) birer şifreleme protokolüdür. TLS, SSL'in gelişmiş halidir. Günümüzde, alt yapının desteklediği her durumda, sistemler ve uygulamalar arasında yapılan veri alış-verişlerinde bu şifreleme tekniği kullanılmalıdır.

SSL/TLS kullanmak için sunucularda ek ayarların yapılması gerekebilir. Dolayısıyla bu şifreleme tekniklerinin kullanılması hedefleniyorsa, bunun ne tür bir maliyetle uygulanabilir olduğu değerlendirilmelidir. Değerlendirme sonucunda, şifreleme protokollerinin kullanımı uygulanabilir olarak görülüyorsa, her sunucu hizmeti için SSL/TLS mutlaka kullanılmalıdır.

Güvenilir sertifika otoritesinin seçimi

Güvenli veri alışverişi yapan sistemler arasında (sunucu-istemci veya sunucu-sunucu) SSL/TLS bağlantısı kurulur iken, anahtar değişimi, şifreleme ve bütünlük kontrolü açısından kullanılacak şifreleme algoritmaları konularında mutabık kalınır. Buna ek olarak sunucu ve istemci, hangi SSL/TLS versiyonunun kullanılacağı konusunda da anlaşırlar. Sunucu istemciye x.509 sertifikasını gönderir. Bu şifreleme ve sertifika alış-verişi sayesinde, tarafların kimlikleri teyit edilir. Bu işlem sırasında, sertifikalarda bulunan genel anahtarların (public key) üçüncü bir taraf aracılığıyla doğrulanması gerekmektedir. Bu üçüncü tarafa sertifika otoritesi (CA) denir. Sertifika otoritesi, genel anahtarın sahibini doğrular. Sertifikanın değeri, hangi bilgilerin sertifika otoritesi tarafından kontrol edildiğine bağlıdır. Bunun yanında, sertifika otoritesinin güvenilirliği de çok önemlidir. Bu yüzden sertifika otoritesi seçimi önemli bir adımdır.

Sertifika sağlayıcılar çok fazla olduğu için, sertifika otoritesi seçiminde aşağıdaki hususlara dikkat edilmelidir:

- Sertifika otoritesinin sağladığı kök sertifikanın, istemcilerin sertifika otoritesi listesinde olup olmadığı, (örneğin tarayıcı)
- Sertifikasyon kuruluşunun yeri, yasal statüsü ve teknik ofisinin bulunduğu yer,
- Sertifika kuruluşunun sunduğu hizmetin; şirketin veya kurumun ana işi olup olmadığı,
- Teknik desteğin kapsamı ve kalitesi,
- Sağladığı sertifikaların maliyetleri.

Bir sertifikanın maliyeti hiçbir şekilde tek başına belirleyici bir kıstas olmamalıdır. Sunucu hizmeti, sınırlı sayıda kullanıcı tarafından kullanılıyorsa, örneğin bir sunucu sadece bir LAN içerisindeyse, bir sertifika otoritesi olmadan bile bir sertifika oluşturulabilir, imzalanabilir ve sunucu hizmetinin kullanılacağı tüm istemciler tarafından doğrulanabilir.

Genişletilmiş doğrulama sertifikaları

Sahte web sitelerinden gelen saldırıları engellemek ve çeşitli sertifika otoritelerinin SSL/TLS sertifikalarını her zaman güvenli bir şekilde kontrol edebilmesini sağlamak için, Genişletilmiş Doğrulama Sertifikaları (Extended Verification Certificate) kullanılmaktadır. Genişletilmiş doğrulama ile sertifika otoritesi, alan adını kontrol etmekle kalmayıp, ayrıca söz konusu alan adının kimin tarafından kaydedildiğini de doğrulamaktadır. Standart X.509 SSL/TLS sertifikalarından farklı olarak, genişletilmiş doğrulama sertifikaları, sertifika sahibinin kimliğini de doğrulamaktadır.

Bunu yaparken, sertifika otoriteleri ve tarayıcı üreticileri aşağıdakileri dikkate almaktadır:

- Başvuru sahibinin kimlik belgesi ve adresi,

- Başvuru sahibinin, alan adının tek sahibi olduğunun ispatı,
- Başvuru sahibinin, başvuruyu yapma hakkına sahip olduğunun teyidi,
- İletişim noktasının belirlenmesi.

Bir EV sertifikası alımında ek maliyetlerin çıkacağı hesaba katılmalıdır. Buna ilave olarak, sertifikalandırma otoritesi tarafından ek bilgiler gözden geçirildiği için, başvuru süreci genellikle daha uzun sürer. Bütün bunlara rağmen, gizlilik ve bütünlük ile ilgili daha yüksek koruma gereksinimleri olan servislerin çalıştığı sunucularda, EV sertifikaları tercih edilmelidir.

Ortak alan adı

Bir web sayfasının sertifikasında kayıtlı genel alan adı, sunucunun web üzerinden hizmet sunacağı tam etki alanı adıyla eşleşmezse, tarayıcılar bir güvenlik uyarısı verirler. Bu nedenle, ortak alan adının, sunucuyla iletişim kurmak için kullanılan URL ile eşleşmesi sağlanmalıdır. Mümkünse, birden çok alt alan adını aynı anda kapsayan sertifika kullanımından (*.ornek.com.tr gibi) kaçınılmalıdır.

Tam sertifika zinciri

Tüm ara sertifikalar, tarayıcı tarafından hiyerarşik sertifika zincirinin kontrolü için gerekli olduğundan, yalnızca sunucunun SSL sertifikası yeterli değildir. Bu nedenle, sunucu, bağlantı esnasında istemciye tüm gerekli sertifikaları gönderecek şekilde yapılandırılmalıdır. Sertifika zinciri, buna uygun olacak şekilde sunucuda saklanmalıdır.

Eksik olan sertifikalara ek olarak, geçerlilik süresi sona ermiş veya iptal edilmiş sertifikaların da sertifika zincirini doğrulayamadığı dikkate alınmalıdır. Yalnızca, tüm sertifikalar geçerliyse ve bağlantı kurulduğunda karşı tarafa aktarılmışsa, sertifika zinciri başarıyla kontrol edilebilir.

SSL / TLS protokol sürümü

Günümüzde kullanılan SSL/TLS protokollerine ait beş farklı versiyon vardır. Bunlar: SSL v2, SSL v3, TLS v1.0, TLS v1.1 ve TLS v1.2. Sistemler arasında güvenli bir bağlantıdan emin olmak için TLS 1.2 kullanılmalıdır. SSL v2 ve SSL v3 yeterli güvenlik sağlamadığı için artık kullanılmamaktadır.

Güvenli şifre paketleri

SSL/ TLS, HTTPS bağlantısının ne kadar güvenli olduğunu belirleyen şifre paketlerini kullanır. Her paket belirli modüller içerir. Eğer bir modülün güvensiz veya zayıf olduğuna karar verilirse, şifreleme paketini değiştirmek, daha güvenli bir modüle geçmenizi sağlar.

Kriptografik algoritmalar ve anahtar uzunlukları hakkında daha fazla bilgi için bu konuya özel hazırlanmış dokümanların incelenmesi tavsiye edilmektedir.

Web sunucusuna özgü durumlar

Web sitelerinin yayınlanmasında SSL/TLS sertifikası kullanılıyorsa, web sitesinde barındırılan tüm sayfalar şifreli olmalıdır. Yeni nesil tarayıcılar karma içerikli, yani kısmi olarak şifrelenmemiş web sitelerini görüntülerken, hata kodu üreterek kullanıcıları uyarırlar. Bu durum da web sayfasının hizmet kalitesini düşürmektedir. Web tarayıcılarının, bu hatayı üretmesinin asıl nedeni, ortadaki adam saldırısı (man-in-the-middle) düzenleyen bir saldırganın, HTTPS oturumunu ele geçirmek için şifrelenmemiş web sayfası içeriklerini kullanarak saldırı düzenleyebilmesidir.

HTTP Sıkı Aktarım Güvenliği (HSTS), SSL'in bilinen zayıflıklarına karşı koruma sağlayan başka bir yöntemdir. Bu yöntem; bir web sitesi ziyaretçisinin, sunucu tarafındaki yapılandırma eksikliklerinden veya bir saldırıdan ötürü, güvenli bir sayfadan güvenli olmayan başka bir sayfaya yönlendirilmesini zorlaştırır. Örneğin bir saldırı, hedef seçilen sistem ile aynı kablosuz ağ (WLAN) içerisinden gerçekleştirilebiliyor ise, saldırgan oturum çerezlerini okuyabilir ve böylece HTTPS oturumlarını ele geçirebilir. HSTS'yi etkinleştirmek için, HSTS üstbilgisi sunucuda yapılandırılmalıdır.

Özel sunucu anahtarının korunması

SSL/TLS kullanımında dikkat edilmesi gereken en önemli hususlardan birisi özel anahtarın korunmasıdır. Bu nedenle, özel anahtarın, istenmeyen kişiler tarafından ele geçirildiğinden şüpheleniliyorsa, sertifika iptal edilmelidir.

Onaylama

Sunucudaki yapılandırma değişikliklerinin oluşturabileceği etki, her zaman tam anlamıyla tahmin edilemeyebilir. Yazılım güncellemeleri bile bazen beklenmeyen değişikliklere neden olabilir. Bu nedenle, SSL/TLS yapılandırmasını canlı ortamda aktif etmeden önce, ortaya çıkabilecek olumsuzlukları görebilmek için test ortamında testler yapılmalıdır. Yapılan testler sonucunda, ancak güvenlik kontrollerinden geçen değişiklikler, canlı ortama aktarılmalıdır.

BTS.1.U19 Güvenlik duvarı yapılandırılması

Bir kurumun tüm ağı, uygun bir güvenlik duvarı ile korunmalıdır. Dışarıya hizmet veren sunucular, DeMilitarized Zone (DMZ) ağında konumlandırılmalıdır. Yine de her sunucu için uygulama veya ağ düzeyinde uygun erişim kısıtlamaları kurulması önerilir.

Yerel güvenlik duvarı uygulaması aynı alt ağdan yapılacak saldırıların dahi engellenmesini sağlayabilir. Ayrıca, bu tür bir güvenlik duvarında servise özel kurallar yazılarak, daha

ayrıntılı bir erişim kontrolü uygulamak da mümkündür. Buna ek olarak, yerel güvenlik duvarı, ele geçirilmiş olan sistemden dışarı yönlü iletişimi de engelleyebilecektir. Böylece, saldırganlar tarafından ele geçirilmiş bir sistem ile verilebilecek zararlar sınırlandırılabilir. Bu koruma, sunucunun tamamen ele geçirilmesinden sonra, saldırgan tarafından devre dışı bırakılabilse de en azından saldırıyı yavaşlatacaktır. Bu sayede, saldırının tespiti ve olası engelleme çalışmaları için önemli miktarda zaman kazanılabilir.

Ayrıca, bir güvenlik duvarının loglama fonksiyonu, belirli saldırıların tespit edilmesine yardımcı olacaktır.

Hemen hemen tüm işletim sistemleri, belirli kurallara göre, alınan/gönderilen tüm paketleri inceleyen ve işleyen filtreler tanımlama yeteneğine sahiptir. Filtreleme seçenekleri, işletim sistemleri bazında farklılıklar gösterebilir. Bununla birlikte, aşağıdaki filtreler çoğu işletim sisteminde mevcuttur.

- Paketin kaynak ve hedef adresi,
- Kullanılan protokol türü (TCP / IP, UDP / IP, ICMP, vb.),
- Kaynak veya hedef portu.

Örneğin, paket filtreleme kuralları yardımıyla, belirli bilgisayarlardan veya belirli alt ağlardan gelen paketler kolaylıkla engellenebilir.

Bazı sunucu uygulamalarında, bahsedilen paket filtreleri haricinde, IP adresleri veya adres aralıkları için izin verme ve engelleme mekanizmaları da vardır. Bu mekanizmaların aksine, işletim sistemi seviyesindeki güvenlik duvarları, en başta devreye girerek, hizmeti tehlikeye atabilecek olası saldırılara karşı koruma sağlar.

Prensip olarak, yüksek koruma gereksinimleri olan tüm sunucular, bir güvenlik duvarı ile korunmalıdır.

Güvenlik duvarı kullanımında iki genel strateji vardır:

Kara liste stratejisi: (İzin verici strateji) "Her şeye izin verilir, engellenenler açıkça belirtilir". Belli sınırlandırma kriterlerine uymayan bağlantıların tamamına izin verilir. Bunun avantajı, yönetim ve sorun giderme işlemlerinin daha düşük çaba ile yerine getirilebilmesidir. Bu uygulamanın ciddi bir dezavantajı ise; güvenli olmayan ağ hizmetlerine erişime izin veren unutulmuş kuralların, sunucuya karşı gerçekleştirilebilecek bir saldırı için zemin oluşturabilmesidir.

Beyaz liste stratejisi: (Kısıtlayıcı strateji) "Tüm bağlantılar, açıkça izin verilmediği müddetçe yasaklanmıştır". Beyaz listede bulunmayan her türlü hizmet engellenir.

Beyaz liste stratejisi, daha yüksek bir güvenlik seviyesi sunar. Bu nedenle, farklı özel bir sebep yok ise bu stratejinin kullanımı tavsiye edilmektedir. Dezavantajları ise, yönetim maliyetlerinin daha yüksek olmasıdır. Çünkü sistem erişim gereksinimlerinde meydana gelecek her değişiklikte, yeni kuralların tanımlanması gerekecektir.

Temel yapılandırmanın bir parçası olarak; tüm sunucuların, dışardan yapılacak bağlantı taleplerinin reddedildiği bir güvenlik duvarının arkasına alınması tavsiye edilir. Sistem, canlıya alındığında bu politika aktif olmalıdır. Bu güvenlik politikasının bir parçası olarak, sunucuda bütün protokol ve portların, varsayılan olarak kapalı olması gerekmektedir. Sunulacak hizmete bağlı olarak, sunucu yapılandırıldıktan sonra, yalnızca gerekli olan protokoller ve portlar açılmalıdır.

Güvenlik duvarları, genellikle ağ trafiğinin ayrıntılı bir şekilde kaydedilmesine olanak tanımaktadır. Böylece, güvenlik duvarı tarafından elde edilen bilgiler, saldırıların tespit edilmesinde yardımcı olabilir. Ağ trafiği kayıt altına alınırken, hiçbir gizlilik politikasının ihlal edilmediğinden emin olunmalıdır. Gerektiği durumlarda politika süreçlerine, ilgili taraflar da dâhil edilmelidir.

ICMP (Internet Control Message Protocol) sorunsalı

ICMP, IP paketlerinin iletilmesi ile ilgili kontrolleri sağlamak ve ortaya çıkan hataları bildirmek için kullanılır. Örneğin, bir paketin göndericisine, hedef ağın ulaşılamayacağını veya paketin hedef sisteme iletilmek için çok büyük olduğunu belirten mesajlar üretir. “Ping” ve “traceroute” araçlarının işlevselliği de ICMP'ye dayanmaktadır.

Birçok kullanışlı özelliğine ek olarak, saldırganların bir ağ hakkında önemli bilgiler elde etmesine ve bu bilgileri saldırı amacı ile kullanmalarına izin veren bazı ICMP mesaj türleri de vardır. Güvenlik duvarı üzerinde ICMP'yi tamamen engellemeye yönelik radikal yaklaşımlara gidilirse, bu durum öngörülemeyen başka sorunlara da neden olabilir. ICMP filtrelemesi yaparken, sistemin ya da istemcinin ihtiyaçları göz önünde bulundurulmalıdır. Örneğin, iç ağ için harici ağdan daha fazla sayıda ICMP mesaj türüne izin verilebilir.

Uygulama ve gözden geçirme

Filtreleme ve loglama seçenekleri, işletim sistemine bağlı olarak değişiklik gösterebilir. Bir güvenlik duvarı yapılandırılmadan önce, üreticinin mevcut dokümanlarını gözden geçirmek faydalı olacaktır.

Ağ üzerinde çalışan bir sisteme dair bir kural oluşturulurken yapılacak bir hata, çalışan sistemdeki servisin erişilememesi veya sistem yöneticisinin artık bütünüyle sunucuya erişememesi gibi sorunlara yol açabilir. Dolayısıyla; oluşturulacak kuralların, çalışan sistem üzerinde aktif hale getirilmeden önce, test sistemleri üzerinde denenmesi gerekir.

Güvenlik duvarını aktif ettikten sonra, gerekli servislerin hala ulaşılabilir olup olmadığı kontrol edilmelidir. Gerekli portların açık, kullanılmayan portların ise kapalı olup olmadığını kontrol etmek için bir port taraması yapılmalıdır.

BTS.1.U20 Ağ üzerinden erişimin kısıtlanması

Bir güvenlik ağ geçidinin kullanımı ve uygun ağ bölümlemesi, sunucunun saldırıya uğrama riskini azaltır. Bu uygulama, ağ planlaması sırasında göz önünde bulundurulmalı ve mutlaka belgelenmelidir.

BTS.1.U21 İşletimin belgelenmesi

Sorunsuz bir işletim için sistem yöneticilerinin elinde, sistem mimarisinin genel bir özetinin olması gerekir. Yöneticilerin sistem üzerinde yaptıkları değişiklikler, mümkünse otomatik olarak belgelenmelidir. Özellikle sistem dizinleri ve dosyalarında yapılan değişiklikler mutlaka kayıt altına alınmalıdır.

Yeni işletim sistemleri kurarken veya mevcut işletim sistemini güncellerken, yapılan değişiklikler dikkatli bir şekilde belgelenmelidir. Yeni sistem parametrelerini oluşturmak veya mevcut sistem parametrelerini değiştirmek, bir BT sisteminin davranışını (özellikle güvenlik fonksiyonları ile ilgili) önemli ölçüde değiştirilebilir.

BTS.1.U22 Acil durum eylem planlaması

Sunucunun, kurum içi iş akışlarının ayrılmaz bir parçası olması ya da dış dünyaya hizmet ediyor olması (e-ticaret veya e-devlet uygulamalarında olduğu gibi) durumunda, kısmi veya tamamen devre dışı kalması, ciddi problemlere neden olabilir.

Bu nedenle, acil durumlara hazırlık bağlamında, yaşanabilecek bir olumsuzluğun sonuçlarının nasıl en aza indirilebileceği ve böyle bir durumda hangi aksiyonların alınacağı ile ilgili bir plan ve prosedür hazırlanmalıdır.

Plan hazırlanırken aşağıdaki hususlar dikkate alınmalıdır:

- Sunucu için oluşturulacak acil durum planlaması, mevcut acil durum planına entegre edilmelidir.
- Sunucuda meydana gelebilecek bir hata, veri kaybına yol açabilir. Bu nedenle, genel yedekleme prosedürünün bir parçası olarak, sunucu için de bir veri yedekleme prosedürü oluşturulmalıdır. Bu prosedür oluşturulurken sunucu tekil olarak düşünülmemeli, sunucunun verdiği hizmete dair diğer bileşenler ve bileşenlerin bağımlılıkları da göz önünde bulundurulmalıdır.
- Bakım ve servis sözleşmeleri kapsamında (belli bir zaman içerisinde) sunucu için yedek parça temini sağlanmalıdır. Böylece, sunucunun devre dışı kalma süresi kabul

edilebilir bir seviyeye indirilebilir. Kritiklik seviyesi yüksek sunucular için, yüksek erişilebilirlik çözümlerinin tercih edilmesi gerekmektedir.

- Sistem yapılandırması belgelenmelidir. Bu sayede, sistemin yapılandırması hakkında önceden bilgi sahibi olunmasa bile, acil bir durumda tüm sistem geri yüklenebilir. Dokümantasyonun elektronik ortamda yer almasının yanı sıra kontrol listesi kâğıt formunda da barındırılabilir. Gerekirse, yapılandırma dosyaları farklı bir veri depolama alanında da saklanabilir.
- Sistemin kontrollü başlatılmasını sağlamak için bir kurtarma planı yapılmalıdır. Bu amaçla, bir önyükleme ortamı önceden oluşturulmalıdır.
- Gerekli tüm prosedür açıklamaları düzenli olarak kontrol edilmeli ve test edilmelidir. Farklı işletim sistemleri için farklı yöntemlerin uygulanabileceğine dikkat edilmelidir.

Sabit sürücü arızası ya da kötü amaçlı bir programın sisteme zarar vermesi halinde kullanılmak üzere, sistemi başlatmak ve kurtarmak için bir önyükleme ortamı, sunucunun ilk kurulumu esnasında oluşturulmalıdır. Ön yükleme için hazırlanan bu taşınabilir medya, işletim sistemleri kurulurken hazırlanabileceği gibi, daha sonra da oluşturulabilir.

Acil durum önyükleme ortamı, aşağıdakine benzer sorunların oluşması durumunda kullanılabilir:

- İşletim hataları nedeniyle veri kaybı,
- Kullanımı ve yeniden başlatmayı engelleyen işletim ve yönetim hataları,
- Sistemin zararlı programlardan etkilenme durumu (ör. bilgisayar virüsleri),
- Sistemin bir saldırgan tarafından ele geçirilmesi,
- Donanım sorunları.

İdeal durumda kurtarma önyükleme ortamı, sunucunun hizmet vermeye devam edebilmesi için gerekli tüm programları ve verileri içermelidir.

Acil durum önyükleme ortamı için aşağıdaki programlar "temel yapılandırma" olarak önerilmektedir:

- Güncel imzalara sahip virüsten koruma programları,
- Sistemin yapılandırma dosyalarını veya veri tabanlarını düzenlemek için gerekli programlar (dosyalar, kayıt defteri veya benzerleri için ilgili editörler),
- Önyükleme ortamını ve sistem diskinin MBR'sini (Ana Önyükleme Kaydı) geri yükleme programı,
- Yedekleme / kurtarma programları,
- Donanım hatalarını analiz etmek için tanılama programları.

Yukarıdaki listeye, adli soruşturmada olduğu gibi, ileri düzey analiz için gerekli olabilecek farklı programlar da eklenebilir.

Tüm programların ve uygulama kütüphanelerinin yalnızca önyükleme ortamından yüklenilebilir olması önemlidir. Hata durumunda, sistemdeki tüm bileşenlerin kullanılamaz olabileceği göz önünde bulundurulmalıdır. Önyükleme ortamını oluştururken, bilgisayarın sabit disklerine erişmek için gereken tüm programlar da önyükleme ortamına dâhil edilmelidir. (Ör. sabit disk denetleyicileri, özellikle RAID denetleyicileri için, sürücüler ve sabit disk şifreleme veya sabit disk sıkıştırma için programlar vb.)

Önyükleme medyasında, sistem yapılandırma dokümanının güncel olarak bulunması, hata ayıklama verimliliğini artırabilir.

Acil durum önyükleme ortamı virüslerden ve diğer kötü amaçlı programlardan arınmış olmalıdır. Bu nedenle, sadece güvenilir kaynaklardan (örneğin doğrudan üreticiden) gelen veya dijital imzası kontrol edilen programlar kullanılmalıdır. Önyükleme ortamını oluştururken ve bu ortamda her değişiklik yapıldığında ortam, bir zararlı yazılımlardan koruma programı ile kontrol edilmelidir.

Her sistem için ayrı bir önyükleme ortamı oluşturmak kesinlikle gerekli değildir. Çok sayıda farklı sistem için uygun şekilde esnek bir önyükleme ortamı yeterli olabilir.

İşletim sistemi veya yapılandırmasının güncellenmesi gerekirse, acil durum önyükleme ortamı ve üzerinde saklanan belgeler de güncellenmelidir.

Acil durum önyükleme medyasının sistem yöneticileri tarafından hızlıca erişilebilir olması gerekir. Böylece, bir arıza durumunda zaman kaybı yaşanmasının önüne geçilir. Öte yandan, yetkisiz kişilerin bu bilgilere erişimi engellenmelidir.

BTS.1.U23 Sistem izleme

Kritik sistem olayları karşısında hızlı aksiyon alabilmek için, tüm veri merkezi için uygun bir sistem izleme mimarisi oluşturulmalı ve sunucular da bu mimariye dâhil edilmelidir. Sunucular açısından bu izleme işlemi temelde; sistemin genel durumu, sunucuların işlevselliği, sunucuların üzerinde çalıştırılan servislerin durumunu içermelidir.

Sunucularda hatalar oluşursa veya izlenen değerler tanımlanmış limit değerlerinin altına iner ya da üstüne çıkarsa; ilgili olaylar, otomatik olarak sunucunun işletiminden sorumlu personele bildirilmelidir. Bu bildirme e-posta, mesajlaşma uygulaması, SMS, telefon araması gibi birçok farklı yöntemle yapılabilir.

BTS.1.U24 Güvenlik kontrolleri

Düzenli aralıklarla (ör. ayda bir kere) sunucunun güvenlik kontrolü yapılmalıdır.

Güvenlik kontrolünde aşağıdaki durumlara dikkat edilmelidir:

- Parola kullanmayan hesaplar var mı?
- Sunucularda uzun zamandır aktif olmayan kullanıcılar var mı?
- Parolası, gereken şartları karşılamayan kullanıcılar var mı?
- Hangi kullanıcılar yönetici haklarına sahip?
- Sunucunun sistem programları ve sistem yapılandırması değişmemiş ve tutarlı mı?
- Sunucuda hangi ağ servisleri çalışıyor? Bunlar güvenlik politikasına göre yapılandırılmış mı?
- Aşağıdaki konularda güvenlik politikasının gerekliliklerine uygun olarak yetkilendirmelere dikkat edilmiş mi?
    - Sistem yazılımları ve sistem yapılandırma verileri,
    - Uygulama yazılımları ve veriler,
    - Kullanıcı dizinleri ve veriler.

Düzenli bir güvenlik kontrolünde, penetrasyon testleri sunucunun hizmet verdiği alt ağlarda uygulanabilir. Bu penetrasyon testlerinin seviyesi değişebilir (örneğin haftalık basit otomatik kontroller, aylık kısmen manuel gerçekleştirilecek daha kapsamlı test, yılda bir kez tüm ağın temel testi).

Sistem yöneticileri, güvenlik kontrolünü gerçekleştirirken, uyguladıkları adımları takip edebilecekleri bir kontrol listesi oluşturmalıdır. Yapılan güvenlik kontrollerinin sonuçları belgelenmelidir. Kontrol sonucunda, hedef durumdan sapmaların sebebi araştırılmalı ve düzenleyici faaliyetler ile gerekli iyileştirmeler yapılmalıdır.

BTS.1.U25 Sunucunun denetimli hizmet dışı bırakılması

Sunucu hizmet dışı bırakılmadan önce mutlaka bir hazırlık yapılmalı ve kullanıcılara sunucunun kapatılacağı hakkında bildirimde bulunulmalıdır. Ayrıca hizmet dışı bırakma öncesinde, aşağıda belirtilen önlemler alınmalıdır;

- Önemli bir verinin kaybedilmeyeceği teyit edilmelidir,
- Sunucuya bağımlılığı bulunan servislerin veya sistemlerin olup olmadığı kontrol edilmelidir,
- Sunucuda hassas bir veri kalmadığı teyit edilmelidir.

Sunucuda hangi verilerin depolandığı ve nerelerden erişildiği özellikle gözden geçirilmelidir.

Yukarıdaki sorular sonrasında elde edilen bilgilere dayanarak, sunucunun hizmet dışı bırakılması öncesinde bir plan yapılmalıdır. Bu planda aşağıdaki noktalar dikkate alınmalıdır:

- Veri yedeklemesi

  Sunucun hizmet dışı bırakılmadan önce, sunucunun hizmet dışı kalmasından sonra da ihtiyaç duyulacak verilerin harici olarak yedeklenmesi, arşivlenmesi veya bir yedek sisteme aktarılması gerekir. Yedeklemeden sonra, verilerin bütünlüğünden emin olunmalıdır.

- Sunucunun yerine yeni bir sunucu kurulması

  Sunucu tarafından sağlanan hizmetlere hala ihtiyaç duyulursa, sunucu üzerinde bulunan servis ve verilerin başka bir sunucuya aktarılması sağlanmalıdır. İlgili planlamada, tedarik ve devreye alma için uygun kaynakların olup olmadığı kontrol edilmelidir.

- Kullanıcıların bilgilendirilmesi

  Eğer sistemi kullanan farklı kullanıcılar varsa, öncesinde bilgilendirilmeli ve bu kullanıcılara kendi verilerini kaydetme fırsatı verilmelidir.

- Referans kayıt ve bağlantıların güncellenmesi

  Bir sunucuyu devre dışı bırakırken, sunucuya daha önceden yapılan referans bağlantılar ve referans kayıtlar güncellenmeli veya silinmelidir. Örneğin: DNS kaydı, dizin hizmetleri girdileri, web sayfası bağlantıları ve oluşturulan diğer referanslar.

- Kapatılacak sistemdeki verilerin silinmesi

  Sunucu disklerinde değerli bilgilerin kalmaması sağlanmalıdır. Üzerinde hassas bilgi barındıran diskleri yeniden biçimlendirmek, bu bilgileri disk üzerinden tamamen silmek için yeterli değildir. Hassas verilerin istenmeyen kişiler tarafından tekrar elde edilmesini önlemek için, kapatılacak sunucu üzerinde bulunan diskler en az bir kez tamamen yeniden yazılmalıdır. Sadece mantıksal bir silmenin ve aynı zamanda kurulu işletim sistemi aracılığıyla diski yeniden biçimlendirmenin, veriyi tamamen ortadan kaldırmayacağı, bu yüzden, verinin uygun bir yazılımla kolay bir şekilde yeniden erişilebilir hale getirilebileceği göz önünde bulundurulmalıdır

- Sunucu yedeklerinin silinmesi

  Bir sistemi devre dışı bıraktıktan sonra, üzerinde saklanan verilere artık ihtiyaç duyulmayacaksa; ilgili yedekleme ortamından da sunucuya ait bilgilerin silinmesi ve yedeklemenin de devre dışı bırakılması gereklidir.

- Diğer verilerin kaldırılması

  Sunucular üzerinde; sunucu adı, IP adresi ve diğer teknik bilgiler gibi bazı özel bilgiler bulunmaktadır. Bu bilgiler, istenmeyen üçüncü tarafların eline geçme ihtimaline karşı, sunucu devre dışı bırakılmadan önce kaldırılmalıdır.

Yukarıda verilen bilgileri de dikkate alarak, sunucuların hizmet dışı bırakılması esnasında kullanılmak üzere bir kontrol listesi oluşturulması tavsiye edilir. Böylece, ilgili adımlar tek tek takip edilerek herhangi bir kontrolün unutulması önlenebilir.

Sunucu göçü

Kaldırılan sunucunun verdiği hizmetler, başka bir sistem üzerinde sunulmaya devam edilecekse; bu geçişin planlanması gerekir. Hizmetin yüksek erişilebilirlik gereksinimi varsa, bu konuda dikkatli bir planlama gereklidir.

Eğer bir sunucu göçü yapılacaksa bunun genellikle, normal çalışma saatlerinin dışında yapılması önerilir. Bu planlama mümkün değilse, verinin kaybolmamasını sağlamak ve uzun sürecek arıza sürelerinden kaçınmak için önlemler alınmalıdır.

Bu nedenle, önemli sunucuların göçü için önceden uygun bir göç prosedürü oluşturulmalıdır. Prosedür oluşturulurken aşağıdaki hususlar özellikle dikkate alınmalıdır:

- Verinin taşınması ve yapılandırılması

  Yeni sisteme geçildikten sonra, verilerin tamamen ve doğru bir şekilde aktarılıp aktarılmadığı kontrol edilmelidir.

  Yeni sistemde, sunucu sistem yazılımının yeni bir sürümü kullanılacaksa; yeni sürümün mevcut verileri doğru şekilde işleyebilmesi sağlanmalıdır. Burada dikkat edilecek konu, yalnızca eski sürümden verilerin doğru bir şekilde içe aktarılması değil, bu verilerin bütünlüğü bozulmadan düzenlenebiliyor veya yeni veri kayıtlarının düzgün bir şekilde eklenebiliyor olmasıdır. Özellikle bu gibi durumlarda problemler ortaya çıkabileceği için, kapsamlı testlerin yapılması tavsiye edilir.

- Servislerin uyumluluğu

  Yeni kullanılacak sistemdeki servislerin, göç ettirilecek sunucudaki servislerle uyumlu olması sağlanmalıdır. Eski sürüme sahip istemcilerle, yeni kurulacak sunucuya erişilmeye devam edilecekse, bu duruma özellikle dikkat edilmelidir. Üretici ya da geliştirici, yeni kullanılacak sistemin önceki sürümlerle tam bir uyum içinde çalıştığını garanti etse dahi, göç öncesinde gerekli testlerin yapılması mutlaka önerilmektedir.

- Şifreleme anahtarları

Sunucu dosya sisteminin belli kısımları şifrelenmiş ise ve bu durum yeni sistemde de devam edecekse; şifreleme anahtarlarının yeni sisteme güvenli bir şekilde aktarılması ve saklanması oldukça önemlidir. Aksi halde yeni sunucudaki şifreli verilere erişim mümkün olmayacaktır.

- İsim ve adreslerin değiştirilmesi

  Eğer sunucunun verdiği hizmete sadece sunucu IP'si ya da DNS adıyla erişiliyorsa, göç işlemi genellikle daha az sorunlu olur çünkü yeni sunucunun, eski sunucunun IP'sini alması genellikle yeterli olacaktır. DNS adı göç ile birlikte değişmeyen ancak sunucu IP'si değiştirilen göç işlemlerinde, DNS kaydı değişiklikleri bazen istemciler tarafından geç algılandığından bu istemcilerin hizmete erişiminde gecikmeler yaşanabilir. Bu durum, planlamada göz önünde bulundurulmalıdır.

  Bazen uygulama geliştiriciler, sunucu IP adresi ya da DNS adını uygulamanın içine ya da istemcilerin konfigürasyon dosyalarına işlemiş olabilirler. Bu durumda, tüm istemcilerin yeniden yapılandırılması gerekebilir. Bu durum, göç işlemi süresini önemli ölçüde artırabileceğinden göç öncesinde planlanmalıdır.

- Kalıcı bağlantılar

  Bazı veri tabanı uygulamalarında olduğu gibi, eğer hizmete, istemci tarafından uzun süreli veya kalıcı bağlantılar oluşturulmuşsa bu bağlantılar, göç işlemi öncesinde sonlandırılmalıdır.

Göç prosedürü kapsamında, göç sırasında adım adım takip edilebilecek bir kontrol listesi oluşturulması tavsiye edilir. Geçişi planlarken ve kontrol listesini oluştururken, her adımın önceki adımlara bağlı olduğuna dikkat edilmelidir.

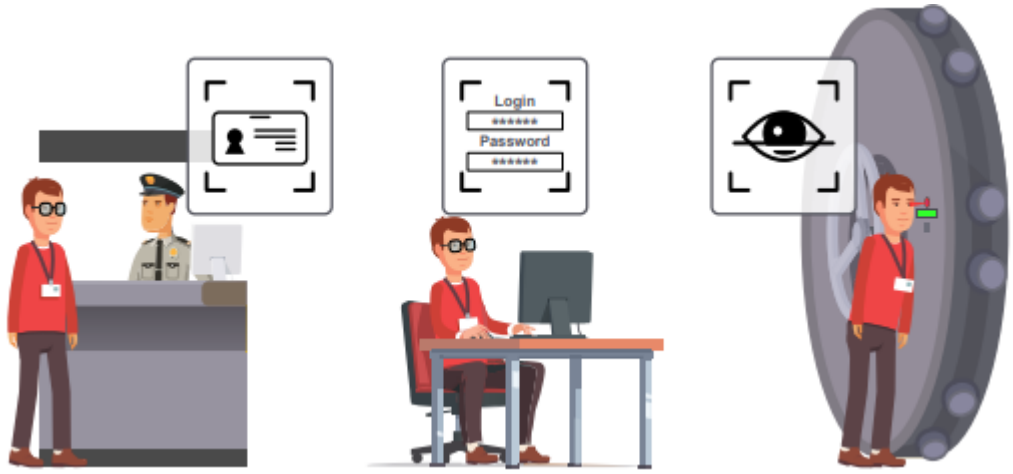
Hizmetin yüksek erişilebilirlik gereksinimi olduğu durumda, olası tüm sorunları erken aşamada tespit edip ortadan kaldırmak için tüm geçişin, mümkün olan en gerçekçi koşullara sahip olan bir test ortamında, önceden test edilmesi gerekmektedir.

2.3 3. SEVİYE UYGULAMALAR

Aşağıdaki öneriler, standart koruma seviyesinin ötesine geçen ve arttırılmış koruma ihtiyaçları için göz önünde bulundurulması gereken önlemlerdir. Parantez içindeki harfler, önlem özelinde hangi temel değerler için öncelikli koruma sağlandığını gösterir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

BTS.1.U26 Çok faktörlü kimlik doğrulama (G)

Bilgi, sahiplik ve biyometrik faktörlere dayanan, farklı kimlik doğrulama yöntemleri bulunmaktadır. Daha yüksek koruma gereksinimleri için, aşağıda belirtilen üç faktörden en az ikisi kullanılarak çok faktörlü kimlik doğrulaması uygulanması önerilmektedir.



Sahiplik (fotoğraflı erişim kartı)	Bilgi (kullanıcı adı ve parola)	Biyometrik (göz tanıma sistemi)

Şekil 9 Mantıksal Kimlik Doğrulama Örnekleri

İki faktörlü doğrulamanın en yaygını, bilgi ve sahiplik faktörlerinin bir arada kullanılmasıdır. Örneğin kritik bir sunucuya erişimde çipli bir kart ve sonrasında PIN numarası kullanılabilir.

Alternatif olarak, dijital imzalara ve asimetrik kriptografi tekniklerine dayalı bir Ortak Anahtar Altyapısı (Public Key Infrastructre) kullanılması tavsiye edilir. Bu yöntemde imzaların geçerliliği, güvenilen bir sertifika otoritesi tarafından kontrol edilmelidir.

BTS.1.U27 Sunucu tabanlı saldırı tespit sistemleri (BE)

Sunucu tabanlı Saldırı Tespit Sistemleri (IDS) kullanılarak, anomali durumlar ve hatalı kullanımlar tespit edilebilir. Kullanılan IDS mekanizmaları uygun şekilde seçilmeli, yapılandırılmalı ve kapsamlı bir şekilde test edilmelidir. Saldırı tespiti durumunda, IDS anlık olarak alarm üretmeli ve ilgili personeli bilgilendirmelidir.

Düzenli bütünlük kontrolü

Beklenmedik değişiklikleri tespit etmek için dosya sisteminin periyodik olarak kontrol edilmesi; dosya öznitelikleri, işlem bilgileri ve sistem yapılandırmasının diğer önemli unsurlarındaki (ör. Windows Kayıt Defteri) tutarsızlıkları tespit etmeye yardımcı olur. Bu tutarsızlıkların tespiti ve düzeltilmesi, sistemin daha istikrarlı bir şekilde çalışmasını sağlar. Ayrıca bu kontrol sayesinde, saldırılar zamanında tespit edilebilir. Eğer herhangi bir saldırı

mevcutsa saldırganın yaklaşımı, bu yapılan kontroller ile anlaşılabilir ve saldırganın sonradan erişmek için bilgisayara kurmuş olabileceği gizli arka kapıların tespit edilmesi sağlanabilir.

Kriptografik doğruluk sağlamasının hesaplanması

Dosyalarda yetkisiz yapılan değişikliklerin algılanması için sistem dosyalarının çoğunda, doğruluk sağlaması yapılır. Doğruluk sağlaması için kullanılan programların merkezi olarak yönetilmesi ve izlenilmesi önerilmektedir.

Bazı programlar, dosya sisteminde sadece değişiklik yapılıp yapılmadığını tespit edebilir. Tespit için; erişim haklarının, son gerçekleşen değişikliğin tarihinin veya ilgili dosyanın içeriğinin değiştirilip değiştirilmediğini kontrol ederler. Değişiklikler, önceden oluşturulmuş doğrulama sağlama toplamı ile hesaplanan doğruluk sağlaması toplamı karşılaştırılarak tespit edilir. Bu tür programlarda yapılacak özel bir ayar aracılığıyla, dosyaya salt okunur bir erişimin gerçekleştirildiği dahi tespit edilebilir.

Doğruluk sağlama dosyasının korunması

Bir saldırgan tarafından değiştirilmesinin engellenmesi için, doğruluk sağlama dosyalarının salt okunur bir ortamda saklanmaları gerekir. Dosya sisteminde değişikliğe izin verildiği durumda doğruluk sağlama dosyalarının CD, DVD veya taşınabilir disklerde saklanması önerilir. Bununla birlikte bu dosyalar, sistemin bulunduğu ağdan farklı, daha güvenli ortamlarda salt okunur şekilde de saklanabilir.

Test gerçekleştirme aralığı ve test kapsamı

Bütünlük kontrol testleri düzenli olarak yapılmalıdır. Uygun bir test gerçekleştirme aralığının seçimi büyük ölçüde, ilgili BT sisteminin veya ortamının amaçlanan kullanımına bağlıdır. Bütünlük testleri gerçekleştirilirken, doğruluk sağlamalarının kontrolü için gereken bellek ve hesaplama süresi de dikkate alınmalıdır. Bütünlük kontrol testi, düzenli olarak işleyen diğer BT operasyonlarına engel olmamalıdır.

Büyük çaplı BT sistemlerinin işletiminde, sistem dosyalarında günlük olarak sürekli değişiklikler yapılır. Bu nedenle, bu tür büyük çaplı BT sistemlerinde kullanılan bütünlük kontrol programının bu durum dikkate alınarak yapılandırılması ve sadece gerekli dosyaların bütünlük kontrolünden geçirilmesi tavsiye edilir. Aksi takdirde, normal iş süreçlerinden kaynaklanan ve bir saldırı girişimine delil teşkil etmeyecek çok sayıda değişiklik bildiriminin alınması riski vardır. Bu çok sayıda bildirimin analiz edilmesi de zor olacaktır.

Bellekteki işlem bilgileri

Dosya tabanlı yapılan bütünlük kontrollerine ek olarak ana bellek üzerinden işlem bilgileri de, izin verilen işlemler temelinde kontrol edilebilir. Bu sayede, dosya sisteminde hiçbir iz bırakmayan manipülasyonlar da tespit edilebilir. Öte yandan işlemlerin kendilerini direkt etkilemeyen, sadece bu işlemlerin konfigürasyonlarını değiştiren bazı manipülasyonlar da olabilir. Bu tür manipülasyonlar, konfigürasyon dosyalarının bütünlük kontrolü yapılarak tespit edilebilir. İşlem bilgisini kontrol etmenin bir diğer avantajı da, daha hızlı yapılabilmesi ve sistem kaynaklarını daha verimli kullanıyor olmasıdır. Dolayısıyla, dosya tabanlı yapılan kontrollere göre bu kontrol daha sık uygulanabilir. Bu sayede istenmeyen programların çalıştırılması durumu, dosya tabanlı yapılan bütünlük kontrollerine göre daha hızlı bir şekilde tespit edilebilir.

Bildirimler

Saldırı tespiti için yapılan kontrollerin sonuç bildirimi, herhangi bir değişiklik tespit edilmemiş olsa bile, e-posta veya başka bir iletişim kanalı ile otomatik olarak yapılmalıdır. Bütünlük kaybının tespit edildiği durumda hangi önlemlerin alınması gerektiği önceden planlanmalıdır. Örneğin, otomatik mi yoksa manuel eylemlerin mi gerçekleştirileceğinin bilinmesi önemlidir.

BTS.1.U28 Yedeklilik (E)

İş süreçlerinin, uygulamaların ve hizmetlerin erişilebilirliği genellikle merkezi bir sunucunun erişilebilirliğine bağlıdır. Bir sunucuda çalışan birden fazla kritik uygulama varsa, sunucunun yüksek erişilebilirlik yapısına sahip olması gerekir. Sunucuda, çeşitli donanımlardan kaynaklanan herhangi bir nedenden dolayı sorun yaşanabilir ve bu sorun hizmet kesintisine neden olabilir. Sunucunun onarılması ciddi zaman alabilir. Bunun yerine, aşağıdaki alternatif çözümler, bir sistemin erişilebilirliğini artırmak için değerlendirebilir;

- Sunucu yedekleme (cold/warm/hot standby),
- Sunucu kümesi (Cluster),
- Yük dengeleyiciler (Load balancer),
- Yük devretme.

Bu tekniklerin her biri, farklı erişilebilirlik seviyeleri sunar ve genellikle farklı maliyetler oluşturur. Bazı durumlarda, sözü edilen sunucular sanallaştırılmışsa daha yüksek seviyede bir erişilebilirlik elde edilebilir.

Yedeklilik mimarisi birkaç farklı yöntemle oluşturulabilir. Bunlar genel olarak cold-standby, warm-standby ve hot standby olarak adlandırılır.

Cold Standby: Yedek sistem (ikincil sistem) kapalı şekilde bekler, aktif sistem (birincil sistem) bozulduğunda ikincil sistem manuel olarak kurulur ve yapılandırılır. Bu mimaride aktif sistemde bir sorun çıkması durumunda ikincil sistem açılır ve birincil sistemden alınan son yedek verileri, ikincil sisteme yüklenir. Bu yedekleme türünde, birincil sistemden alınan yedek veriler bir depolama sisteminde tutulur ve sadece gerektiğinde ikincil sisteme geri yüklenir ve servisler, genellikle birkaç saatlik süre sonunda tekrar hizmet vermeye başlayabilirler.

Cold Standby çözümünün avantajları:

- Bu çözümde, sistemin genel karmaşıklığı artmaz, kurulumu diğer çözümlere göre daha basittir.
- Maliyet yönünden en uygun olan çözümdür.
- Hizmetin erişilebilirliğinde herhangi bir kesinti olmadan, sistem yeniden başlatılabilir veya sistemde değişiklikler gerçekleştirilebilir. Birincil sistemde yapılacak bir değişiklik ikincil sisteme hizmet kesintisi olmadan aktarılabilir.

Cold Standby çözümünün dezavantajları:

- Mevcut sisteme ilaveten ikincil bir sistem gereklidir.
- İkincil sistem, birincil sistem ile aynı konfigürasyon ve yamalara sahip olmalıdır.
- Bu çözümde ikincil sisteminin manuel olarak etkinleştirilmesi gerektiğinden, sistem yöneticileri, birincil sistemi anlık olarak izlemeli ve acil durumlarda gerekli müdahaleyi yapmalıdırlar.
- Eğer birincil sistemin verileri, ikincil bir sistem tarafından doğrudan erişilebilecek harici bir depolama alanında tutulmuyor ise; ikincil sistem devreye alınmadan önce, birincil sistemin verileri ikincil sisteme taşınmalıdır.

Bu çözüm, kısa veya uzun süreli hizmet kesintisi yaşanması durumunda herhangi sorun oluşturmayacak hizmetler için önerilmektedir.

Warm Standby: Aktif sistemde kurulu bütün yazılım bileşenleri ve servisler aynı zamanda ikincil sisteme de kurulur ve kullanılabilir durumdadır. İkincil sistem açık ve çalışır durumda bekletilir. Birincil sistemde bir arıza olması durumunda, yazılım bileşenleri ve servisler ikincil sistemde başlatılır. Bu işlem genellikle bir yazılım kullanılarak otomatikleştirilebilir. Birincil sistemdeki veriler, disk tabanlı replikasyon veya paylaşımlı diskler kullanılarak ikincil sisteme düzenli aralıkla yedeklenir. Bu yöntem kullanılarak birkaç dakika içinde yedek sistem üzerinden hizmet vermeye başlanabilir.

Hot Standby: Yazılım bileşenleri ve servisler hem birincil hem de ikincil sistemlerde kurulu ve çalışır durumdadır. İkincil sistemdeki yazılım bileşenleri ve servisler çalışır durumdadır

ancak isteklere yanıt vermez ve verileri işlemez. Veriler neredeyse gerçek zamanlı olarak ikincil sisteme aktarılır ve her iki sistem yaklaşık aynı verilere sahip olur. Veri replikasyonu genellikle bir yazılım aracılığıyla yapılır. Bu yöntem kullanılarak birkaç saniye içinde yedek sistem üzerinden hizmet vermeye başlanabilir.

Hot – Standby çözümünün avantajları:

- Kesinti süresi Cold Standby çözümüne göre çok daha kısadır.
- Rehberin ilerleyen kısımlarında bahsi geçen yüksek erişilebilirlik yöntemlerine göre daha az maliyetli bir çözümdür.
- İkincil sistem de çalışır durumda olduğu için, anlık olarak birincil sistemdeki verileri üzerine alabilir.
- Hizmetin erişilebilirliğinde herhangi bir sorun yaşanmadan, sistemi yeniden başlatmak ve sistem üzerinde değişiklik yapmak mümkündür. Bu tarz bir durumda, çalışan servisler ikincil sistem üzerinden hizmet vermeye devam ederler.

Hot – Standby çözümünün dezavantajları:

- Bu çözümde mevcut donanımın sadece belli kısmı aktif olarak kullanılır.
- İkincil sisteminin, birincil sistem ile aynı verilere sahip olması gerekmektedir. Dolayısıyla ikincil sistem sürekli olarak güncellenmelidir.
- Eğer ikincil sistemin devreye girmesi için manuel müdahale gerekecek bir yapılandırma ayarı yapılmış ise; sistemler herhangi bir acil durum için sürekli olarak sistem yöneticileri tarafından izlenmelidir.

Bu çözüm, kısa süreli hizmet kesintisi yaşanması durumunda bir sorun oluşturmayacak hizmetler için önerilmektedir. Çözümün planlanmasında, izleme ve ikincil sisteme geçiş operasyonlarının gerekliliği göz önünde bulundurulmalıdır. Bu çözümün olası kullanım alanları şunlardır;

- Sık değişen içeriğe sahip web sunucuları,
- Çeşitli uygulama sunucuları, e-posta sunucuları,
- Veri tabanı sunucuları ve dosya sunucuları.

Yukarıda bahsi geçen tüm çözümlerde genel prensip olarak, yedek sistemin hizmete başlama süresini azaltmak için;

- Yedek sistem üzerinde çalışan işletim sistemi ve uygulamaların önceden hazır halde tutulması,
- Aktif sistemde yapılan güncellemelere paralel olarak yedek sistemin de güncelleştirilmesi ve mümkünse aktif sistem üzerindeki verinin, düzenli olarak aktarılması,

- Yedek sistem ile aktif sistem arasındaki veri aktarımının, doğru yazılım çözümleri kullanılarak otomatik olarak yapılması,
- Yedekte bekleyen sistemin manuel olarak etkinleştirilmesi gerekiyorsa, aktif sistemin sürekli olarak izlenmesi ve acil durumlarda hızlıca müdahale edilmesi,
- Aktif sistemin verileri merkezi bir depolama sistemi üzerinde tutuluyorsa, yedek sistemin bu depolama sistemine erişiminin, veri bütünlüğünü sağlamak için, sadece okuma izni verilerek sağlanması,
- Yedek sistemin aktif edilmesinde, servis seviyesi sözleşmesinde belirtilen sürelere dikkat edilmesi

hususlarına dikkat edilmelidir.

Kümeleme (Clustering)

Bir sunucu kümesi, bir uygulamanın veya hizmetin erişilebilirliğini veya performansını artırmak için, paralel olarak çalışan iki veya daha fazla sunucudan oluşur. Uygulama veya hizmet, sunuculardan birinde aktif diğerlerinde yedek olacak şekilde ayarlanabileceği gibi performans amacıyla tüm kümeye de dağıtılabilir.

İşlevlerine göre kümeler ikiye ayrılır. Bunlar;

- Yük dengeleyici küme (Load Balancing Cluster)
- Yük devredici küme (Failover Cluster)

Yük dengeleyici küme (Load balancing cluster)

Bu yöntemde, sunucu kümesine gelen trafik bir yük dengeleyici ile karşılanarak, önceden belirlenmiş kurallara göre, işi yapacak olan sunuculara dağıtılır. Yük dengeleyiciler, yükü dağıttıkları sistemlerin sağlıklı olup olmadığını belirli aralıklarla kontrol ederek, sağlıklı çalışmayan sunuculara trafiği yönlendirmezler. Bu sayede, yük dengeleyiciler sistemlerin ölçeklenmesini sağladıkları gibi, yüksek erişilebilirlik için de kullanılırlar. Hizmet dışı kalan sunucuya yeni istek gönderilmez ve bu şekilde kullanıcıların problemden etkilenmemesi sağlanır.

Günümüzde, yedeklilik sağlayan yük dengeleme sistemlerine bulut sistemleri de entegre edilerek daha yüksek düzeyde erişilebilirlik değerlerine ulaşılabilmektedir.

Yük devredici küme (Failover cluster)

Bu yöntemde; sunucu kümesi içinde işleri üzerinde yürüten ana sunucuda bir sorun yaşanması halinde, yürütülen uygulamanın ya da hizmetin aktif işlemleri, otomatik olarak kümenin başka bir elemanı tarafından devralınır. Yük devretme kümesi içinde bulunan bütün sunucular aktif olarak çalışmaktadır.

Yük devretme işlemi için, küme sunucuları arasındaki iletişimi izleyip devretme özelliğini tetikleyecek bir mekanizma (heart beat) kullanılır. Bu mekanizma, otomatik devretme için gerekli tüm yazılım ve donanım bileşenlerini anlık olarak izlemektedir. Yük devretme kümesinin otomatik devretme senaryoları tasarlanırken dikkatli bir planlama yapılmalı ve bu senaryolar sık sık test edilmelidir. Mekanizma, devretme yapılacak servislere bağımlı ise, servisin ayarlarında yapılan herhangi bir değişiklikten sonra yapılandırma ayarları tekrar kontrol ve test edilmelidir.

Yük devretme kümesi kullanımında aşağıdaki hususlar dikkate alınmalıdır:

- Paylaşılan diske erişim:

Yük devretme kümelerinde, uygulama verilerini tutmak için ortak paylaşılan disk kullanmak önerilir. Bu disklere erişim, aktif olan küme sunucusuna verilir. Paylaşılan disk yerine, sürekli kopyalanan disklerin (replikasyon) kullanılması da mümkündür. Bu durumda, bu tür disk yapılarındaki karmaşıklık ve bağımlılıkların, erişilebilirlik açısından ek bir tehdit oluşturup oluşturmadığı dikkate alınmalıdır.

- Uygulama taşınabilirliği:

Bir uygulamayı, paralel olarak iki veya daha fazla sunucuya yüklemek ve dağıtmak, çoğu zaman ek lisansların kullanımını gerektirir. Ayrıca, uygulamanın yük devretme özelliğinin olup olmadığı kontrol edilmelidir.

- Tek hata noktası (SPoF – Single Point of Failure):

Kümenin yük devretme özelliği, tek bir bileşenin bozulmasıyla kullanılamaz duruma geliyorsa bu durum, sunucu kümesi mimarisinin gerçek amacına uygun olarak çalışmadığını gösterir. Tek hata noktalarından kaçınmak için sistem genel olarak analiz edilmeli ve bileşenlerden (güç kaynakları, sistem belleği, ağ kartları, anahtarlar, hub'lar vb.) kaynaklanacak hatalar ise tek tek kontrol edilmelidir.

- İşletim sistemi ve küme sunucularının yapılandırılması:

Küme sunucuları; aynı işletim sistemi sürümleri, yamalar, kütüphaneler ve uygulama sürümleriyle donatılmış olmalıdır. Donanım ve yazılımlar ne kadar benzer yapılandırılırsa, yük devretme işlemi esnasında yükü devralan sistemin, yükü devreden sistemle o kadar çok aynı davranışı sergileyeceği ve işlemin başarılı olacağı varsayılabilir. Dahası, aynı sistemler söz konusu olduğunda, tüm sistemin karmaşıklığı daha da azalacaktır (ör. aynı yük devretme yazılımının kullanımı, ağ ara yüzleri, paylaşılan depolama sisteminin uyumluluğu, yönetim vb.).

- Sunucular arasında yedekli bağlantı:

Küme sunucuları arasındaki bağlantı mümkün olduğunca hızlı ve diğer ağ yüklerinden bağımsız olmalıdır. Böylece, yük devretme işlemi mümkün olduğunca hızlı ve sorunsuz gerçekleşebilir. Yüksek erişilebilirlik gereksinimleri isteniyorsa, bu bağlantıların yedekli olması da gerekmektedir.

- Yük devretme yönetimi için uygun yazılım çözümlerini kullanma:

Bir kümenin aktif sunucusunun başarısız olup olmadığına karar verme işlemi bazı durumlarda karmaşık olabilir. Bu işlemin, yeni veya yeterliliği ispatlanmamış yazılımlar ile yapılması, hatalı sonuçlar verebilir ve sunucu kümesi fonksiyonunun düzgün çalışmamasına neden olabilir.

- Yük devretme işleminin kapsamlı test edilmesi:

Son olarak, herhangi bir tek hata noktası (single point of failure) olmadığını belirlemek için kapsamlı testler yapılması gerekmektedir. Özellikle sunucu izleme ve yük devretme yönetimi, tüm olası hatalar için test edilmelidir.

Yük devretme kümesinin yararları:

- Otomatik devralma, erişilebilirliği önemli ölçüde artırabilir.
- Manuel müdahale gerekmez.

Yük devretme kümesinin dezavantajları

- Uygulamaya bağlı olarak çözüm oldukça karmaşık olabilir.
- Yük devretme kümeleri iyi ölçeklenebilir değildir.
- Kaynakların sadece bir kısmı kullanılır.
- Ek donanım ve yazılım nedeniyle yüksek maliyetler gerekebilir.

Avantajları ve dezavantajları göz önünde bulundurulduğunda sunucu kümelerinin kullanımı özellikle bir ya da daha fazla uygulamanın yüksek erişilebilirlik ihtiyacı olduğunda daha anlamlıdır. Yüksek maliyetine ilaveten bu yöntemlerin etkin kullanılabilmesi için, ilgili sistem yöneticilerinin işletim sistemleri, ilgili uygulamalar ve yük devretme özellikleri konusunda iyi düzeyde bilgiye sahip olmaları gereklidir. Sunucu tarafında kümeleme yapısı kullanılırken, ağ ve hizmet edinen istemcilerin de yedekli olma durumu değerlendirilmelidir.

Sunucu küme sistemlerinin genel kullanım sahaları şu şekildedir;

- Veri tabanı uygulamaları,
- Dosya sunucusu hizmetleri,
- Dinamik içeriğe sahip uygulamalar,
- E-posta sunucuları.

İş süreçleri, uygulamalar veya hizmetler yüksek erişilebilirlik gereksinimlerine sahip olduğunda, bu gereksinimlerin nasıl karşılanabileceğini dikkate almak önemlidir. BT yöneticileri ve güvenlik yönetimi, ilgili sunucular için bir planlama oluşturmalı ve uygun mimarileri seçmelidir.

BTS.1.U29 Test ortamının oluşturulması (GBE)

Yüksek güvenlik gereksinimine sahip sunucularda yapılacak herhangi bir değişiklik, canlı ortamda uygulanmadan önce mutlaka test edilmelidir. Bu testlerin sağlıklı bir şekilde yapılabilmesi için canlı ortamdan fiziksel veya mantıksal olarak ayrılmış bir test ağ alt yapısının oluşturulması önerilmektedir. Ayrıca, bu test ortamında canlı sistemler ile aynı konfigürasyonlara sahip test sunucuları kullanılmalıdır. Oluşturulan bu test ortamında, uygulanması planlanan güvenlik yamaları, güncellemeler, yapılandırma değişiklikleri, sunucu üzerindeki servis ve uygulamalarda yapılacak değişiklikler mutlaka test edilmelidir.

Test ortamı; donanım ve yazılım bakımından canlı ortam ile işlevsel olarak eşdeğer kurulumlara imkân verecek şekilde tasarlanmalıdır. Bu tasarımı yaparken pahalı bir sunucu için, aynı şekilde yapılandırılmış ikinci bir sistemin tedarik edilmesine gerek yoktur. Yapılandırma değişikliklerini, güncellemeleri, uygulamaları ve servisleri test etmek için ekonomik sistemleri kullanmak yeterli olacaktır.

Tipik ve sık yapılan testlerde kullanılmak üzere verimliliği artıracak ve hatalardan kaçınılmasını sağlayacak kontrol listelerinin oluşturulması tavsiye edilmektedir. Yapılan tüm testler açık ve sade bir şekilde belgelenmelidir.

BTS.1.U30 Sunucu üzerinde tek hizmet sunulması (GBE)

Kritik bir hizmet sunan veya bilgi taşıyan bir sunucunun gizlilik, bütünlük ve erişilebilirliğinin sağlanması için, söz konusu sunucu üzerinde sadece tek bir hizmet sunulması, önem arz eden bir noktadır. Böylece, sistemin saldırı yapılabilecek yüzey alanı azaltılmış olur. BT sistemlerindeki çoğu güvenlik açığı, saldırganlar tarafından tekil olarak değil; kümülatif olarak kullanılırlar. Çoğu zaman bir sunucuya ancak, sunucu üzerindeki mevcut birçok güvenlik açığı birlikte istismar edilerek yapılan saldırılar başarılı olur. Özellikle internete erişimi olan veya diğer yabancı ağlar üzerinde hizmet veren kritik sunucularda tek bir hizmetin sunulması, sunucuya yapılacak siber saldırıların başarılı olma oranını büyük ölçüde azaltacaktır.

Örneğin, e-posta hizmetinin verildiği bir sunucu aynı zamanda web sunucusu olarak da kullanılırsa, web sunucusuna yapılan bir saldırı sonucunda, saldırgan web sitesinde yapacağı değişiklikler ile itibar kaybına neden olabileceği gibi tüm e-posta trafiğini okuyarak kişisel ve gizli bilgilere de erişim sağlayabilir.

Ayrıca sunucu güvenliğini daha ileri düzeyde sağlamak için, aynı hizmetin farklı görevleri de farklı sunucular üzerine dağıtılabilir. Örneğin, internet üzerinden gelen e-postaları iç ağa ileten bir "A" e-posta sunucusu; iç ağdan e-postaları internete ileten "B" e-posta sunucusu olsun. "A" sunucusunun bir siber saldırı sonucunda hizmet veremez olması durumunda sadece dışardan gelen e-postalar okunamaz; ancak "B" sunucusu çalışmaya devam ettiği için, iç ağdan e-postalar dışarıya gönderilebilir ve böylece hizmet, topyekûn kesintiye uğramamış olur.

Farklı sunucular üzerinden farklı servislerin verilmesi, aşağıdaki avantajları sağlayacaktır:

- Sunucular daha kolay yapılandırılabilir.
- Sunucunun güvenlik duvarı kuralları daha güvenli ve rahat oluşturulur.
- Sunucunun siber saldırılara karşı direnci artar.
- Sunulan servislerin güvenilirliği artar.
- Sunulan servislerin bakımı daha kolay yapılır.

Her servisin farklı bir sunucu üzerinden veriliyor olması daha fazla sunucu gerektireceği için ek yönetim maliyeti getirecektir. Ancak sunucuların merkezi bir yönetim yazılımı ile yönetilmesi ortaya çıkacak bu maliyeti azaltacaktır.

Sanallaştırma

Kritik güvenlik gereksinimlerinin gerektiği durumlarda, fiziksel sunucularda olduğu gibi, sanal sunucularda da bir sunucu üzerinde yalnızca bir hizmet verilmelidir. Ancak sanallaştırma hizmetinin verildiği fiziksel sunucu üzerinde birden fazla sanal sunucu çalıştırılabilir. Kullanılan sanallaştırma ürünün güvenlik ile ilgili hangi hizmetleri sağladığının kontrol edilmesi gereklidir. Sanallaştırma sunucusu üzerinde hizmet veren sanal sunucular birbirlerinden yalıtılarak, sanallaştırma ürünü aracılığı ile farklı servisler sunma olasılığı artırılır.

Ayrıca, sanallaştırma hizmetinin sunulduğu fiziksel sunucuda, sanallaştırma yazılımının ve bu yazılıma doğrudan bağlı hizmetlerin dışında hiçbir servis çalıştırılmamalıdır.

BTS.1.U31 Uygulama beyaz listesi (GB)

Uygulama beyaz listesi oluşturularak, sunucu üzerinde yalnızca izin verilen uygulamaların çalıştırılması sağlanmalıdır. Bunun için izin verilen uygulamaların bulunduğu paylaşım adresleri tanımlanmalıdır. Uygulama beyaz liste yöntemini uygulamak için kullanılabilecek özel mekanizmalar ve üçüncü taraf çözümler vardır.

Bu konuda uygulanabilecek basit bir yaklaşım, dizin yolu tanımlayarak beyaz liste uygulamaktır. Örneğin, bu yöntemle, program ile ilgili dizinlere veya işletim sistemi

dosyalarının dizinlerine çalıştırma izni verilir. Bu, kötü amaçlı bir programın tarayıcı önbelleğinden veya geçici bir klasörden yürütülmesini engelleyebilir.

Alternatif olarak uygulanabilecek diğer bir yöntem, her bir uygulama için açık bir şekilde çalıştırma izni tanımlamaktır. Bu yaklaşım, yalnızca önceden tanımlanmış uygulamalar için güvenlik sağlar. Ancak bu yöntemde, iş yükü artacaktır. Örneğin, gerekli olan tüm işletim sistemi bileşenlerinin çalıştırılabilir olduğundan emin olunmalıdır. Buna ek olarak, beyaz listedeki değişen uygulamaları güncellemek de ek işletim maliyeti oluşturacaktır.

Beyaz liste uygulaması devreye alındığında, komut dosyaları gibi betiklerin çalıştırılamayabileceği unutulmamalıdır.

BTS.1.U32 Ayrıcalıklı hesapların korunması (GB)

Yönetimsel hesapların parolaları, birden fazla parçaya ayrılarak her bir parçanın farklı kişiler tarafından bilinmesi sağlanmalıdır. Kritik operasyonel çalışmaların birden fazla sistem yöneticisinin katılımı ile gerçekleştirilmesine dikkat edilmelidir. Ayrıca yönetimsel hesapların birden fazla hatalı giriş denemesi sonucunda kilitlenerek kullanılamaz hale getirilmesi prensibi uygulanmalıdır.

BTS.1.U33 Kök sertifikaların yönetimi (GB)

Sunucunun hizmet sunabilmesi için hangi kök sertifikalarına sahip olması gerektiği belirlenmeli, belgelenmeli ve düzenli olarak kontrol edilmelidir.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

- Using the GNU Privacy Guard Agent Configuration,[Çevirimiçi]. Erişim: https://www.gnupg.org/documentation/manuals/gnupg/Agent-Configuration.html [Erişim tarihi: 06 Eylül 2019].

- Configure Trusted Roots and Disallowed Certificates Microsoft, 2017. [Çevirimiçi]. Erişim: https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx [Erişim tarihi: 17 Eylül 2019].

- Beginning your General Data Protection Regulation journey for Windows Server Microsoft, 2017. [Çevirimiçi]. Erişim: https://docs.microsoft.com/en-us/windows-server/security/gdpr/gdpr-winserver-whitepaper [Erişim tarihi: 12 Ekim 2019].

- Guide to General Server Security NIST Special Publication 800-123, 2008.[Çevirimiçi]. Erişim: https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf [Erişim tarihi: 05 Ekim 2019].

- The Transport Layer Security (TLS) Protocol RFC 5246, Internet Engineering Task Force (IETF), 2008. [Çevirimiçi]. Erişim: , https://tools.ietf.org/html/rfc5246 [Erişim tarihi: 11 Ekim 2019].

- Transport Layer Security (TLS) Renegotiation Indication Extension RFC 5746, Internet Engineering Task Force (IETF), 2010. [Çevirimiçi]. Erişim: https://tools.ietf.org/html/rfc5746 [Erişim tarihi: 12 Ekim 2019].

- Transport Layer Security Registry Settings Microsoft, 2019. [Çevirimiçi]. Erişim: https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings [Erişim tarihi: 18 Eylül 2019].

- Protection Attack Analytics and Rapid Response Microsoft, 2018. [Çevirimiçi]. Erişim: https://azure.microsoft.com/tr-tr/blog/ddos-protection-attack-analytics-rapid-response/ [Erişim tarihi: 12 Ekim 2019]

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
BTS.1.U1	Uygun kurulum	Sunucu, bir sistem odasında veya kilitli bir sunucu kabininde mi kuruldu? Bu alanlara kimlerin erişim yetkisi var?
		Sunucuda, çıkarılabilir bir medyadan ön yükleme yapılabiliyor mu?
		Sunucuda kullanılan diskler şifrelenmiş mi?
BTS.1.U2	Kullanıcı kimlik doğrulaması	Kullanıcıların parola kullanımını düzenleyen bir politika var mı?
		Kullanıcılar için yeterli karmaşıklıkta parola oluşturmalarını sağlayacak bir talimat mevcut mu?
		Parolanın politikada belirtilen sayıda yanlış girilmesi sonucunda, ilgili hesap kilitleniyor mu?
		Kullanıcılar parolalarını düzenli aralıklar ile değiştirmeye zorlanıyor mu?
		Kullanıcılar, parolalarının çalınması şüphesi olduğu anda, parolalarını değiştiriyorlar mı?
		Oturum açmanın başarısız olduğu durumda: Kullanıcı adı veya parolanın hangisinin yanlış olduğu bilgisi kullanıcı ile paylaşılıyor mu?
		Kullanıcıya, görevlerini yerine getirmesi için, sistemde erişmesi gerekli yerlere yetki tanımlaması yapıldı mı?
		Kullanıcıya görevini yerine getirmesi için gerekli yetkiden daha fazlası tanımlandı ise, bu yetkilerin kaldırılması için bu durumun takibi yapılıyor mu?
		Geçici kullanıcı hesaplarının erişim yetkileri ile ilgili bir politika mevcut mu?
BTS.1.U3	Kısıtlayıcı hakların tahsisi	Sunucularda erişim yetkisi kısıtlaması yapılıyor mu?
		Yetkili kullanıcı hesaplarının gerekli uygulamalara ve BT sistemlerine erişebilmeleri sağlandı mı?
		Sistem dosyalarına erişim, sadece yetkili sistem yöneticileri ile sınırlandırıldı mı?
		Sunucular, yalnızca yetkili kullanıcılara gerekli ayrıcalıkları sağlayacak şekilde yapılandırıldı mı?
		Kullanıcılara erişim haklarının verilmesi sırasında kurumun güvenlik politikaları dikkate alınıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Sistem dosyalarına, hangi uygulamaların ve kullanıcıların, ne zaman erişim yaptığı kayıt altına alınıyor mu?
BTS.1.U4	Rollerin ayrıştırılması	Sistem yöneticileri ile standart kullanıcı rolleri için farklı yetkilendirmeler yapıldı mı?
		Sistem yöneticilerine, sadece sorumlu olduğu alana dair yetkiler tanımlandı mı?
BTS.1.U5	Yönetim arayüzlerinin korunması	Sunucuların Yönetim için kullanılan yöntemler güvenlik politikasında tanımlandı mı?
		Yönetim amaçlı yapılan bağlantılarda kullanılan protokoller ve yöntemler güncel teknolojiye uygun mu?
		Merkezi kimlik doğrulama hizmetinin kurulumu, işletimi ve bakımı için mevcut bir plan var mı?
		Yönetim arayüzlerine yapılan bağlantıların politikalara uygunluğu düzenli olarak kontrol ediliyor mu?
BTS.1.U6	Gereksiz servislerin ve hesapların devre dışı bırakılması	Kullanıcı hesapları oluşturulurken bu hesapların yetkileri gereksinimlere göre tanımlandı mı?
		Kullanımı sona eren hesapların yetkileri alınıyor ve bu hesaplar devre dışı bırakılıyor mu?
		Kullanılmayan kullanıcı hesapları, servisler ve arayüzler devre dışı bırakılmış veya kaldırılmış mı?
		Kullanıcı hesaplarına tanımlanan yetkiler kayıt altına alındı mı?
BTS.1.U7	Ürün yazılımı, işletim sistemi ve uygulamaları için güncellemeler ve yamalar	Tüm organizasyon genelinde yama ve değişiklik yönetiminden sorumlu kişiler belirlendi mi?
		Etki alanı yüksek olan değişiklerde Bilgi Güvenliği Yönetimi sürece dahil edildi mi?
		Yama yönetimi için kurum politikası mevcut mu?
		Yazılım güncellemeleri ve yamaları sadece güvenilir kaynaklardan mı indiriliyor?
		Yazılım güncellemeleri ve yamaları, uygulanmadan önce test ediliyor mu?
		Başarısız bir güncelleme durumunda, güncelleme öncesindeki versiyona geri dönüş yapılabiliyor mu?
		Yamadaki sorunlardan dolayı yamanın yüklenmemesi kararı alındı ise bu karar kayıt altına alındı mı? Bilgi Güvenliği Yönetimi sürece dahil edildi mi?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
BTS.1.U8	Düzenli yedekleme	Yedeklerin depolandığı alanlar yetkisiz erişime karşı korunuyor mu?
		Yedeklerin saklandığı alanlar canlı sistemlerden ayrı mı tutuluyor?
		Yedekleme kartuşlarını ya da disklerini uzun süre sakladığınız alanlarda gerekli iklimlendirme şartları sağlanıyor mu?
		Gizli verilerin yedekleri şifreli olarak saklanıyor mu?
		Kritik veriler düzenli olarak yedekleniyor mu?
		Yedekleme politikası kurum erişilebilirlik gereksinimlerini karşılıyor mu?
		Kullanıcılar, yedekleme politikası hakkında bilgilendiriliyor mu?
		Yedekten dönüş testleri düzenli olarak yapılıyor mu?
BTS.1.U9	Zararlı yazılımlardan koruma programlarının kullanımı	Güvenlik politikasına uygun olarak, tüm BT sistemlerinde zararlı yazılımlardan koruma programları yüklü mü?
		Zararlı yazılımlardan koruma programının ve imzalarının, güncel olması sağlanıyor mu?
		Kullanıcılara 'isteğe bağlı tarama' seçeneği ile bilgi verildi mi?
		e-Posta sunucuları, zararlı yazılımlardan koruma programları ile korunuyor mu?
		İnternet üzerinden bulaşabilecek zararlı yazılımlara karşı yeterli koruma sağlanıyor mu?
		Bir zararlı yazılım tespit edildiğinde, tüm veri tabanı kontrol edilir mi?
		Zararlı yazılım tespit edilirse: zararlı yazılımın sunucuda mevcut gizli verilere erişip erişmediği, koruma yazılımlarının işlevselliklerini devre dışı bırakıp bırakmadığı kontrol edilir mi?
		Veri alışverişi esnasında zararlı yazılımlardan koruma sağlanıyor mu?
		Şifrelenmiş verilerin zararlı yazılımlardan korunduğu garanti ediliyor mu?
		Kullanıcıların, zararlı yazılımlardan koruma programlarının ayarlarında herhangi bir değişiklik yapabilmeleri engellendi mi?
BTS.1.U10	Loglama	Sunucularda gerçekleştirilen işlemlerin logları tutuluyor mu?
		Loglar düzenli olarak değerlendiriliyor mu?
		Yapılan değerlendirmelerin sonucu kayıt altına alınıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Logların saklama süreleri için yasa ve mevzuatlar dikkate alındı mı?
BTS.1.U11	Sunucular için bir güvenlik politikasının oluşturulması	Sunucular için mevcut bir güvenlik politikası var mı?
		Sunucunun güvenlik politikası, istenen güvenlik seviyesine ulaşmak için gerekli olan tüm stratejileri, gereksinimleri ve düzenlemeleri dikkate alıyor mu?
		Güvenlik politikasının içeriği düzenli olarak güncelleniyor ve uygulamalarının kontrolü periyodik olarak denetleniyor mu?
BTS.1.U12	Sunucu kurulumunun planlanması	Yukarıdan aşağıya tasarım prensibine dayanan bir sunucu dağıtımı planı yapıldı mı?
		Servisler için; IT güvenlik hedefleri, görevler ve fonksiyonlar gibi tüm gereksinimler planma öncesinde dikkate alındı mı?
BTS.1.U13	Sunucuların tedarik edilmesi	Sunucu alımı öncesinde sunucuda bulunması gerekli tüm özelliklerin mevcut olduğu bir talep listesi var mı?
BTS.1.U14	Kullanıcı ve yönetici kavramının oluşturulması	Sunucularda kullanıcılar ve yöneticiler için farklı roller oluşturuldu mu?
BTS.1.U15	Kesintisiz güç kaynağı	UPS'in gücü ve açık kalma süresi ile ilgili gereksinimleri sağlayıp sağlamadığının kontrolü yapıldı mı?
BTS.1.U16	Sunucuların güvenli kurulumu ve temel yapılandırması	Kritik sunucular, konfigürasyon ve log dosyaları gibi yerlere erişim parola ile korunuyor mu?
		Mevcut sürümde bir sunucu servisi çalıştırmak için gereken tüm kaynaklar var mı?
		Networke sadece izin verilen arayüzler ve uygulamalardan erişim sağlanıyor mu?
		Sunucu hizmetlerine erişim için parola ile kimlik doğrulama her seferinde yapılıyor mu?
		Sunucu hizmetlerinin güvenlik ile ilgili logları düzenli olarak tutuluyor mu?
		IT sistemlerin güvenli kurulumu için fonksiyonel gereksinimleri ve güvenlikle ilgili özellikleri dikkate alan bir kurulum konsepti mevcut mu?
		Kurulum konsepti,kurulum için yapılması gerekli konfigürasyonları içeren adım adım açıklamaların bulunduğu bir doküman içeriyor mu?
		Kurulum konsepti içerisinde, çevirimdışı kurulum yapılırken gerekli güvenlik tedbilrleri ile ilgili bir politika mevcut mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
BTS.1.U17	Uygulama kurulumu	BT bileşenlerinde, yazılımında veya yapılandırma verilerinde değişiklik yapmak için herhangi bir yönerge var mı?
		Değişiklikler yapılırken güvenlik yönlerinin dikkate alınması zorunlu mudur?
		Tüm değişiklikler planlanmış, test edilmiş, onaylanmış ve belgelendirilmiş midir?
		Değişiklikler yapılmadan önce geri dönüş çözümlerinin testi yapılmış mı?
		Bilgi güvenliği yönetimi önemli değişiklikler yapılacağı zamanlarda sürece dahil oluyor mu?
BTS.1.U18	İletişim bağlantılarının şifrelenmesi	Sunucular arası ve sunucuya yapılan bütün bağlantılar mümkünse TLS protokolü ile şifreleniyor mu?
		Sunucular, TLS'in güvenli versiyonununu destekliyor mu?
		Güvenilir bir sertifika otoritesi seçimi yapıldı mı?
		SSL/TSL sertifikaları canlı ortamda kullanılmadan önce sertifikada hata olup olmadığı kontrol edilip, sertifikanın durumu periyodik aralıklarda doğrulanıyor mu?
BTS.1.U19	Güvenlik duvarı yapılandırması	Güvenlik duvarı kullanım politikası oluşturuldu mu?
		Güvenlik duvarında kısıtlayıcı strateji uygulanıyor mu?
		Güvenlik duvarının yapılandırılması için temel bir konfigürasyon mevcut mu?
		ICMP filtremelesi yapılıyor mu?
		Güvenlik duvarı kuralları düzenli olarak kontrol ediliyor mu?
BTS.1.U20	Ağ üzerinden erişimin kısıtlanması	Ağ mimarisinin tasarlanması aşamasında, Kurum güvenlik gereksinimlerine uygun olarak farklı alt ağların kulllanım dikkate alındı mı?
		Farklı alt ağlar oluşturulurken hangi ağ cihazlarının kullanılacağı belirlendi mi?
		Ağ bağlantıları kurulurken merkezi bir kimlik doğrulama hizmetinin kullanımı için bir mimari oluşturulmuş mu?
		Gizlilik gereksinimlerinin yüksek olduğu durumlarda; iletişimi korumak için IPSEC kullanılıyor mu?
BTS.1.U21	İşletimin belgelenmesi	Sunucu işletiminin sağlıklı bir şekilde gerçekleştirilebilmesi için sunucu mimarisinin genel bir özeti belgelendirildi mi?
BTS.1.U22	Acil durum eylem planlaması	Sunucularda meydana gelebilecek bir arıza için acil durum planı var mı?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Acil durumlarda sunucuyu kontrollü bir şekilde başlatmak için mevcut bir ön yükleme ortamı var mı?
		Arızalanması durumunda sunucunun çalışmasını etkileyecek sistemler için de bir acil durum planı mevcut mu?
		Arızalan sistemlerdeki verilerin korunmasına yönelik bir planlama mevcut mu?
		Acil durum eylem planları düzenli olarak test ediliyor mu?
BTS.1.U23	Sistem izleme	Sunucuların izlenmesine yönelik bir politika mevcut mu?
		Sunucular, merkezi bir izleme aracı ile izleniyor mu?
		Sunucuların izlenmesi sürecinde; hangi bildirimlerin kime, ne zaman ve hangi iletişim kanalı ile yönlendirileceği netleştirilmiş mi?
BTS.1.U24	Güvenlik Kontrolleri	Güvenlik kontrolleri düzenli olarak gerçekleştiriliyor mu?
		Güvenlik kontrollerinin uygulanması ve sonuçları belgelendi mi?
		Güvenlik kontrollerinde tespit edilen açıklıklar için gerekli önlemler alındı mı?
BTS.1.U25	Sunucunun denetimli hizmet dışı bırakılması	Sunucu hizmet dışı bırakılmadan önce, sunucunun verdiği hizmetler, bağımlılıklar ve sunucudaki mevcut bilgilerin kullanılabilirliği dikkate alınıyor mu?
		Sunucular kapatılmadan önce, sunucunun kapatılması ile ilgili detaylı bir planlama yapılıyor mu?
BTS.1.U26	Çok faktörlü kimlik doğrulama	Sunucu veya uygulamalara erişim öncesinde kimlik doğrulaması yapılıyor mu?
		Kurum tarafından belirlenen kritik sunucular için çok faktörlü kimlik doğrulama yöntemi kullanılıyor mu?
BTS.1.U27	Sunucu tabanlı saldırı tespit sistemleri	Sunucu tabanlı saldırı tespit sistemlerinin kullanımı değerlendirildi mi?
BTS.1.U28	Yedeklilik	Sunucu yedeklilik mimarisi, sunucu tarafından sağlanan hizmetin kritikliğine ve erişilebilirlik gereksinimlerine uygun olarak tasarlandı mı?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
BTS.1.U29	Test ortamının oluşturulması	Yüksek koruma gereksinimi bulunan sunuculara dair, yapılandırma işlemleri, güncelleme ve yamaların yüklenmesi gibi değişikliklerin canlı ortamda gerçekleştirilmeden önce test edilebileceği bir test ortamı mevcut mu?
		Sunucuların test ortamı, 'işlevsel olarak eşdeğer' bir donanım ve yazılım kurulumuna olanak sağlıyor mu?
		Tipik ve sıklıkla yinelenen testler için kontrol listeleri kullanılıyor mu?
BTS.1.U30	Sunucu üzerinde tek hizmet sunulması	Güvenlik gereksinimleri sebebi ile sunucuda tek bir hizmet sunulması değerlendirildi mi?
BTS.1.U31	Uygulama beyaz listesi	Sunucu üzerinde yalnızca izin verilen uygulamaların çalıştırılmasına yönelik bir planlama yapıldı mı?
BTS.1.U32	Ayrıcalıklı hesapların korunması	Ayrıcalıklı hesapların korunmasına yönelik bir politika mevcut mu?
BTS.1.U33	Kök sertifikaların yönetimi	Sunucunun hizmet sunabilmesi için hangi kök sertifikalarına sahip olması gerektiği belirlendi mi?

TÜBİTAK BİLGEM
Yazılım Teknolojileri Araştırma Enstitüsü

İşçi Blokları Mahallesi Muhsin Yazıcıoğlu Caddesi
No:51/C 06530 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