TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

İSTEMCİ YÖNETİMİ REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Şubat 2020

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Şubat 2020	İlk sürüm	TÜBİTAK BİLGEM YTE

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

YÖNETİCİ ÖZETİ

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

Modeli ve **Rehberlerin** hazırlanmasına yönelik ulusal politika hedefleri, ülkemizde geliştirilen ve uygulamaya alınan Bilgi Teknolojileri (BT) rehber ve olgunluk modelleri ile 5 uluslararası kuruluş, 12 danışmanlık firması, 6 ülke tarafından geliştirilen standart, rehber ve çerçeve modelleri, uygulama örnekleri ve ilgili akademik çalışma örnekleri incelenmiştir. Farklı dijital kabiliyet alanlarında 34 bilişim uzmanından tecrübe aktarımı sağlanmıştır. Merkezi Yönetim ile yapılan anket üzerinden ilgili kapsama giren konular özelinde anket sonuçları analiz edilmiştir. Elde edilen tespitler doğrultusunda, **Dijital Olgunluk Değerlendirme Modeli**'nin taslağı oluşturulmuş ve seçilen kamu kurumlarında pilot uygulama yapılmıştır. Pilot uygulama sırasında alınan geri bildirimler doğrultusunda **Model** nihai hale getirilmiştir. **Model** ile Stratejik Yönetim, Organizasyon, Yazılım Hizmetleri, Yazılım Yaşam Döngüsü, BT Hizmetleri, İşletim ve Bakım, d-Hizmetler başlıklarında yedi yetkinlik belirlenmiştir. Bu yetkinlikler altında gruplandırılmış dijital kabiliyetler bazında seviyelendirilmiş 2745 soru belirlenmiştir.

Model'in 8 kurumda uygulaması yapılarak Dijital Olgunluk Seviyeleri belirlenmiş ve dijital kabiliyetler bazında tespit değerlendirmeleri gerekçelendirilerek Dijital Olgunluk Seviyesini geliştirmeye yönelik kısa, orta ve uzun vadede çözüm önerileri sunulmuştur.

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

seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna yönelik referans, rol, işleyiş, iş akışı ve çıktılar ile ilgili bilgiler sunulmaktadır. Aynı yıl **Model** ile belirlenen tüm dijital kabiliyetler için, yatırım planlanırken dikkate alınması gereken unsurlar ve alternatifleri ile ilgili bilgi ve yönlendirmeleri içeren 32 adet **Dijital Kabiliyet Rehberi** hazırlanmıştır. Söz konusu rehberlerin yetkinlikler altında ve tüm yaşam döngüsü dikkate alınarak genişletilmesine yönelik rehber hazırlama çalışmaları devam etmekte olup bu kapsamda 2018 yılında **BT Hizmetleri** yetkinliği altında yer alan **Veri Merkezi Rehberi**, 2019 yılında aynı yetkinlik altında **Kablosuz Ağların Yönetimi Rehberi, Aktif Dizin Yönetimi Rehberi** ve **Sunucu Yönetimi Rehberi** yayımlanmıştır. 2020 yılının hemen başında bunlara ek olarak **İstemci Yönetimi Rehberi** yayımlanmıştır.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** **www.dijitalakademi.gov.tr** platformu ile açık erişimi sağlanmakta ve **Rehberlerin** kullanımının yaygınlaşması amacıyla eğitim programları, toplantılar ve çalıştaylar düzenlenmesi ile **Rehberlik Mekanizmaları** hayata geçirilmektedir. Bu sayede d-Devlet ekosisteminde görev alan bilişim uzmanlarının yetkinliklerinin artırılması hedeflenmektedir. Yanı sıra **Dijital Olgunluk Değerlendirme Modeli** ile uyumlu olarak 2017 yılında Türkiye'ye özgü **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiş ve **Model** ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönlerinin belirlenmesi ve eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmıştır. 38 bilişim profesyonel rolü ile bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 6 kurumda yaklaşık 550 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

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

1 GİRİŞ

İstemci 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, İstemci Yönetimi Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, İstemci 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.
HA	[High Availability] Yüksek erişilebilirlik olarak adlandırılır ve sunulan servisin herhangi bir nedenle kesintiye uğramaması,

Terim / Kısaltma	Tanım
	sürekliliğinin sağlanmasıdır.
Hizmet	Kullanıcını ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (ör. Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
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.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.
LAN	[Local Area Network] Yerel alan ağı

Terim / Kısaltma	Tanım
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.
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,

Terim / Kısaltma	Tanım
	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.
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

Terim / Kısaltma	Tanım
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.
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

Terim / Kısaltma	Tanım
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.

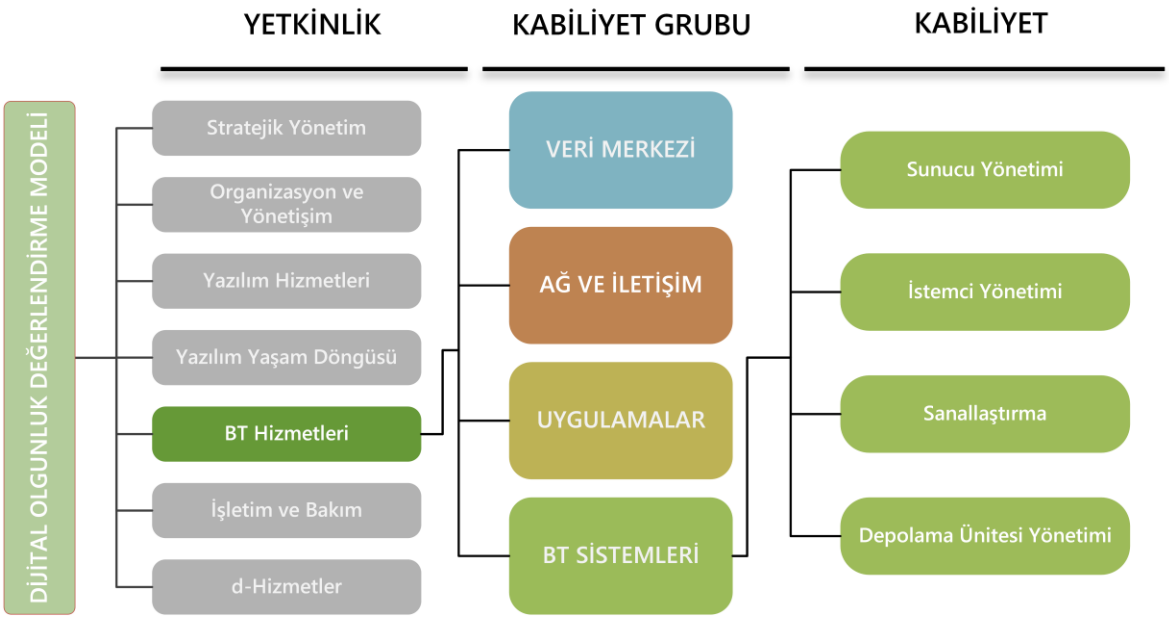
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır.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



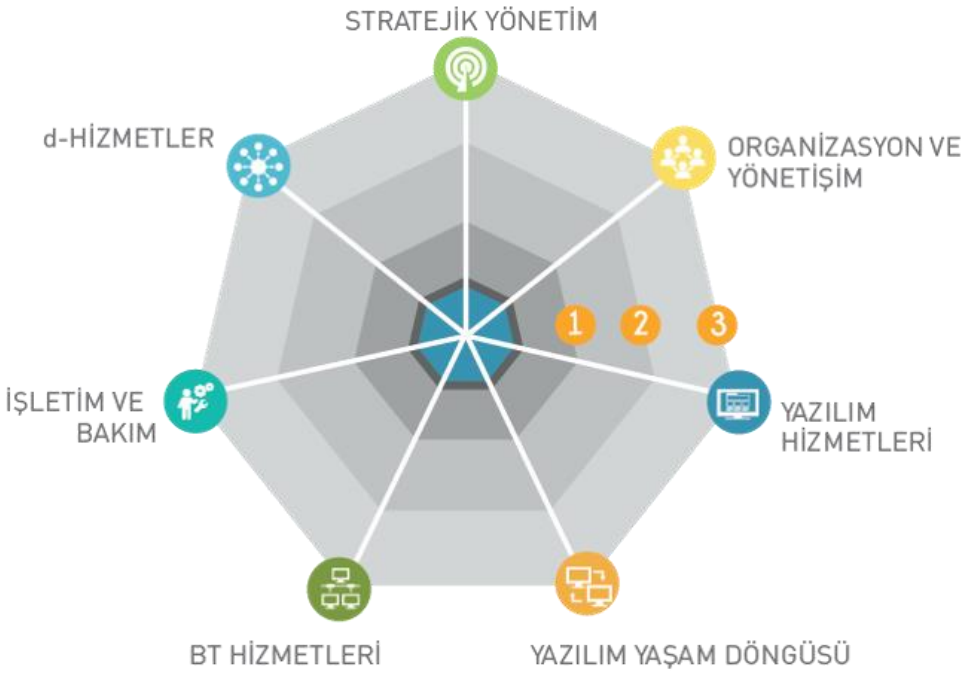
Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

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;

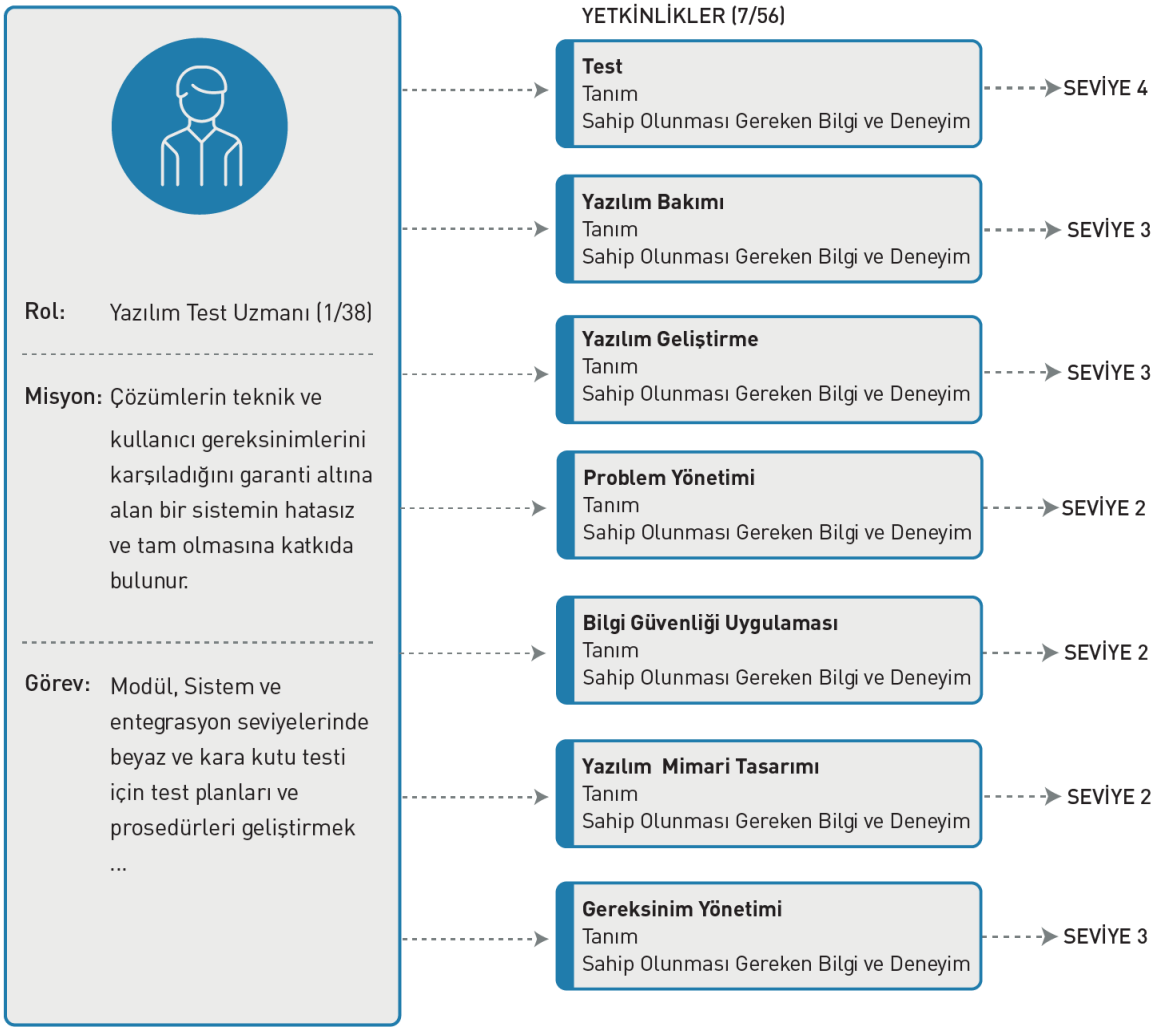
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının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

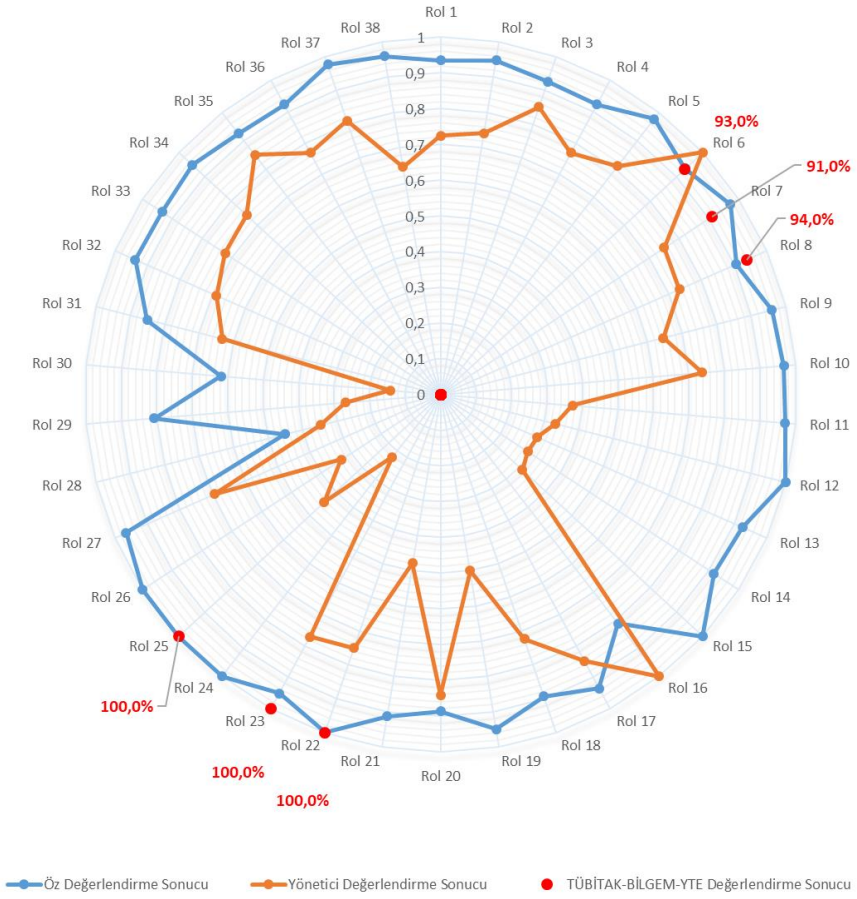
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

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:



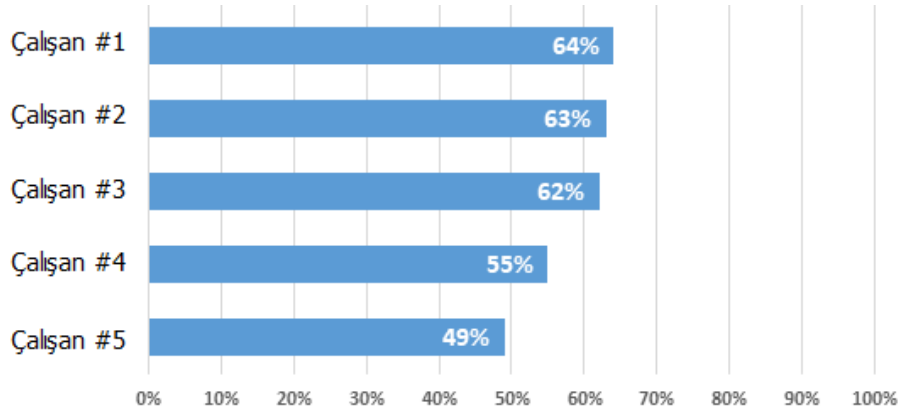
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

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:



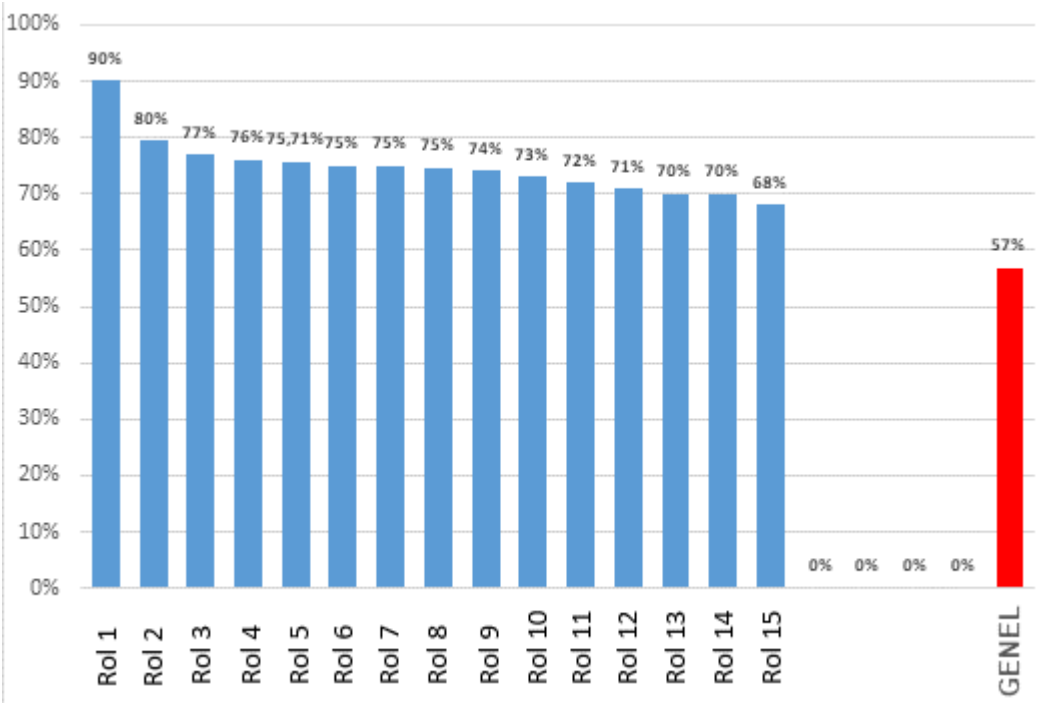
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

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 **İstemci 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.2.G1 kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

"BT Sistemleri" kabiliyet grubu için kullanılan kısaltma	**"İstemci Yönetimi" kabiliyeti için atanan numara**	**1. Gereksinim maddesi**
BTS	2	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

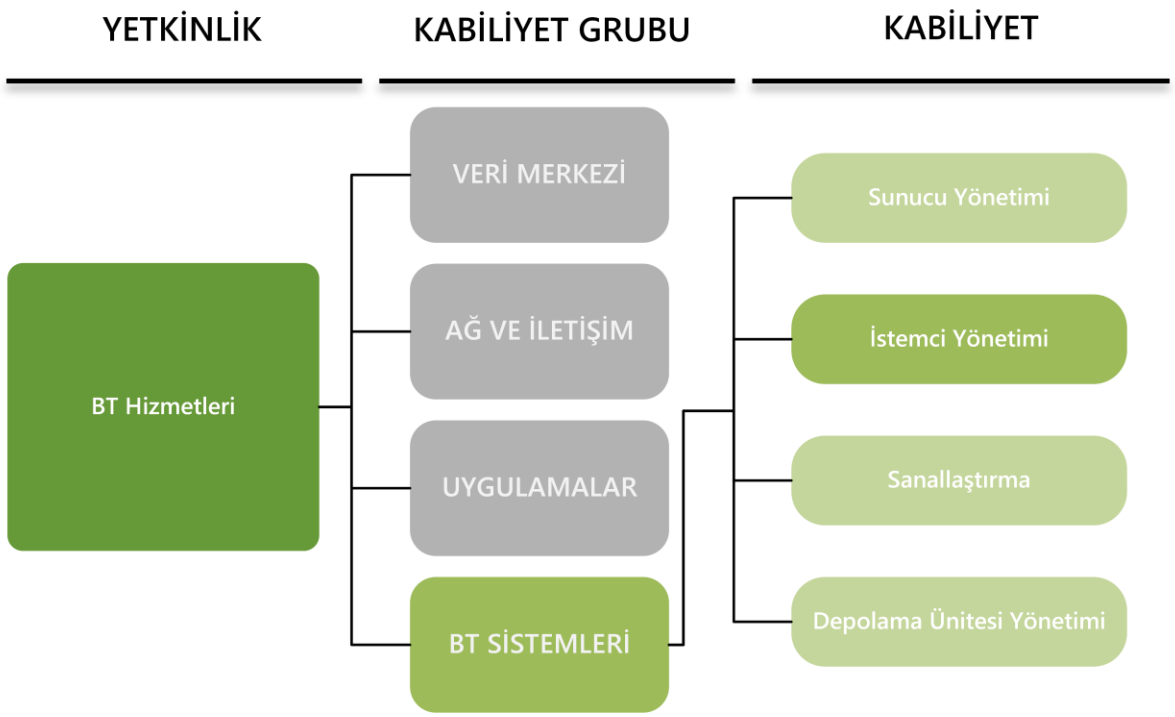
- **Veri Merkezi;** Veri merkezi kapsamında, kritik BT bileşenlerini içeren kurumun yapısal-teknik koşullarının yanında, altyapı güvenliği ile ilgili yönlerini de irdeler. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Genel Bina
    - Veri merkezi içerisinde bulunan binalar için, genel 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.2.G İSTEMCİ YÖNETİMİ

TEMEL BİLEŞEN REHBERİ

BTS.2.G İSTEMCİ YÖNETİMİ
TEMEL BİLEŞEN

1 AÇIKLAMA

1.1 TANIM

İstemci; ağ üzerindeki sunucuları veya diğer BT kaynaklarını kullanan kullanıcı bilgisayarlarıdır. Genel olarak istemciler, sunucularda çalışan uygulamalardan veya hizmetlerden talepte bulunan, veri veya sonuç isteyen bilgisayarlardır.

"İstemci Yönetimi Rehberi", istemcilerin tedariğinden başlayarak, kullanım dışına çıkarma işlemine kadar olan bütün süreçlerin güvenli bir şekilde yönetilebilmesini ele almaktadır.

1.2 HEDEF

Bu rehberin amacı; işletim sistemi ne olursa olsun, istemci üzerinde oluşturulan, okunan, düzenlenen, saklanan veya gönderilen verilerin gizliliğini, bütünlüğünü ve erişebilirliğini korumaya yönelik bilgileri sağlamaktır.

1.3 KAPSAM DIŞI

Bu rehber, istemcilerin güvenli yönetimi için bir temel oluşturur. İstemciler, çeşitli güvenlik önlemleri alınması gereken işletim sistemleriyle çalışırlar. İstemcilerde sistem yazılımı olarak kullanılan her işletim sisteminin, kendine has güvenlik gereksinimleri olabilir. Bu sebeple, bu rehberde ele alınmayan önlemler için bu rehbere ek olarak farklı rehberler de kullanılabilir. İstemci üzerinde farklı bir yapı yoksa, istemci bu rehberin gereksinimlerine göre yönetilebilir. Akıllı telefonlar veya tabletler gibi mobil cihazlara dair özel güvenlik gereksinimleri için farklı kaynaklar kullanılabilir.

İstemci üzerinde, veri alışverişi sağlayan USB, Bluetooth, LAN veya WLAN gibi ara yüzler var ise, kurumun güvenlik gereksinimlerine uygun olarak, bu ara yüzlere ait farklı rehberlerin kullanılması da tavsiye edilir.

2 RİSK KAYNAKLARI

Aşağıda belirtilen güvenlik açıkları ve tehditler, istemci yönetimine dair öncelikli olarak dikkat edilmesi gereken hususlardır.

2.1 ZARARLI (KÖTÜ AMAÇLI) YAZILIMLAR

Zararlı yazılımlar; bilgisayar ve mobil cihazların istenmeyen ve kötü amaçlı çeşitli işlevler yerine getirmesini sağlamak, cihazlar üzerindeki kritik bilgileri toplamak, özel bilgisayar sistemlerine erişmek veya reklam göstermek gibi amaçlar için kullanılan yazılımlardır. Kötü amaçlı yazılımlar kendilerini gizleyerek, bulaştığı bilgisayar sisteminden bilgi toplayabilir ve casusluk işlemleri yapabilirler. Saldırganlar bu yazılımlar ile, istemci üzerinde birçok yönetimsel ayrıcalıklara sahip olabilir, parolalara erişebilir, BT sistemlerini uzaktan kontrol edebilir, mevcut koruma yazılımını devre dışı bırakabilir veya veri çalabilirler.

Kullanıcılar, zararlı yazılım içeren bir web sayfasını ziyaret ettiklerinde, özel e-posta hesaplarına gelen zararlı yazılım barındıran içerikleri denetimsiz bir şekilde açtıklarında veya taşınabilir disklerdeki zararlı yazılımları istemcilerine kopyaladıklarında; zararlı yazılımlar kurumun ağında yayılabilirler.

Bu yazılımlar; çalıştırılabilir kod, betik, aktif içerik veya diğer farklı yazılım türleri şeklinde ortaya çıkabilirler ve zararsız görünen dosyaların içine gizlenebilirler. Zararlı yazılımlar genel olarak şunlardır:

- Virüs
- Solucan yazılımı (worm)
- Truva atı (trojan horse)
- Arka kapı açıklığı (backdoor hole)
- Spam mesajlar
- Şantaj yazılımı (ransomware)
- Kök kullanıcı takımı (rootkit)
- Telefon çevirici (dialer)
- Korunmasızlık sömürücü (exploit)
- Klavye dinleme (keylogger)
- Tarayıcı ele geçirme (browser hijacking)
- Casus yazılım (spyware)

2.2 YAPILANDIRILMAMIŞ YEREL VERİ YÖNETİMİ

Kurum güvenlik politikalarına ve yapılan uyarılara rağmen birçok kullanıcı, kritik verileri merkezi bir dosya sunucusunda değil de kendi bilgisayarında saklama eğilimindedir. Örneğin, aktif bir projeye ilişkin dosyalar veya e-posta arşivleri genellikle yerel olarak saklanır. Bu durum, aşağıdaki sorunlara yol açabilir:

- Donanım hatalarının oluşması durumunda veri kaybı yaşanması,
- Çalışanın, iş/birim değiştirmesi durumunda ilgili verilere erişimin sağlanamaması.

Merkezi depolama yöntemleri kullanıldığında dahi bazı dosyaların kopyaları istemcilerde de oluşturulur. Bu durum ise aşağıdaki sorunların yaşanmasına neden olabilir:

- Yerel depolama alanında gereksiz dosya saklanması ile yerel diskin verimsiz kullanımı,
- Dosya sürümlerinde tutarsızlık oluşması.

2.3 VERİ KAYBI

İstemciler üzerinde yer alan verilerin bir şekilde kaybolması veya zarar görmesi, iş süreçlerinde, dolayısıyla tüm kurum üzerinde ciddi olumsuz etkilere neden olabilir. Veri kaybı ya da bozulmasından dolayı işler gecikebilir veya ilgili çalışmalar tamamen durabilir. Verilerin zarar görmesi veya kaybolması, iş gücü kaybı ve verileri tekrardan elde etme maliyetine ek olarak, müşteriler veya paydaşlar arasında güven kaybının yaşanması gibi uzun vadeli olumsuzluklara da yol açabilir. Veri kayıplarının neden olduğu doğrudan ve dolaylı zararlar kurumun gelecekteki varlığı açısından tehdit oluşturabilir.

2.4 HATALI KULLANIM NEDENİYLE OLUŞAN DONANIM SORUNLARI

Sunucu gibi merkezi olarak hizmet veren BT sistemlerinden farklı olarak, istemcilerde, kullanıcılar doğrudan cihaz üzerinde çalışırlar. Kullanıcıların istemcilere fiziksel olarak direkt erişebilmesi, istemcinin kasıtlı veya kasıtsız zarar görmesine neden olabilir. Örneğin; istemcinin düşürülmesi, kablolarının zarar görmesi veya klavyesine sıvı dökülmesi gibi durumlar yaşanabilir. Donanımlarda yaşanabilecek arızaların çoğunda, donanımın değiştirilmesi tek başına yeterli olmaz. Örneğin, sabit diskte meydana gelebilecek bir hata durumunda; sabit diski değiştirmek saklanan verilerin kurtarılması anlamına gelmeyecektir. Buna ek olarak, BT sistemleri onarım tamamlanana kadar kullanılamazlar. Kurum dışında kullanımda olan taşınabilir BT cihazlarının arızalanması durumunda, çalışmalara ancak kuruma döndükten sonra devam edilebilecek durumlarla karşılaşılabilir.

2.5 YAZILIM GÜVENLİK AÇIKLARI VE HATALARI

Karmaşık mimarilere sahip yazılımlarda, programlama veya tasarım hatalarıyla karşılaşılma ihtimali yüksektir. Yazılım güvenlik açıkları; kullanıcılar tarafından henüz bilinmeyen ancak sistemde güvenlik riski oluşturan programlama hatalarıdır. Hem BT altyapısında uzun süredir kullanılan yazılımlarda, hem de yeni geliştirilen yazılımlarda neredeyse her gün yeni bir güvenlik açığı tespit edilmektedir.

İstemcilere çok çeşitli uygulamaların yükleniyor olması, sistemi olumsuz etkileyebilecek olan güvenlik açıklarının sayısını artırabilir. Ayrıca, çok sayıda istemcinin var olduğu ortamlarda, istemcilerin güvenlik açıklarına dair ilgili yamaların geçilmesi, sunucu gibi yerleşik sistemlerde bu çözümün uygulanmasına nazaran daha zordur.

Yazılım hataları derhal tespit edilmezse veya hızlı bir şekilde düzeltilmezse, bu durum ciddi sorunlara yol açabilir. Yaygın olarak kullanılan bir yazılımdaki ortaya çıkabilecek açıklık, büyük ölçekte güvenlik sorunlarına neden olabilir.

2.6 İSTEMCİNİN YETKİSİZ KULLANIMI

Bir istemcinin yetkisiz olarak kullanımı, kullanıcı kimlik doğrulaması yapılarak engellenmelidir. Her ne kadar istemciler kimlik doğrulaması yapılarak yetkisiz erişimlere karşı korunsa da, bir saldırganın erişim bilgilerini tahmin etmeyi başarması durumunda bu koruma etkisiz kalacaktır. İstemcide aktif olarak ekran kilitleri kullanılmıyorsa, kullanıcının yokluğunda istemci yetkisiz kişiler tarafından kullanılabilir.

2.7 İHTİYAÇ DUYULMAYAN İŞLETİM SİSTEMİ BİLEŞENLERİ VE UYGULAMALARI

İşletim sistemi kurulumu yapılırken isteğe bağlı eklentileri ve yazılımları yüklemek mümkündür. Bununla birlikte, istemcilerin işletimi boyunca da sık sık uygulamalar kurulup test edilirler. İstemciye kurulan her uygulamayla birlikte, istemcinin hafıza, depolama alanı gibi kaynaklarının kullanımının yanı sıra güvenlik açığı ihtimalinin de arttığı hesaba katılmalıdır. Gerek duyulmayan ancak istemciye yüklenen uygulamalar, genellikle düzenli yama yönetimine tabi tutulmazlar ve bu nedenle ilgili güvenlik açıkları zamanında kapatılamazlar. Bu durum, istemci üzerinde güvenlik açığı oluşmasına sebep olur ve saldırganlar bu açıkları kullanarak istemciye erişim sağlayabilirler.

2.8 İSTEMCİ ÜZERİNDEKİ MİKROFON VE KAMERA İLE ORTAM DİNLEME

Günümüzde istemci olarak kullanılan birçok sistem dâhili mikrofon ve kameralara sahiptir. Bu istemciler, akıllı kişisel asistan (IPA: Intelligent Personal Assistant) olarak adlandırılan ve çevreyi sürekli izleyip, dinleyerek; müzik çalma, arama yapma, aydınlatma ve iklimlendirme sistemini kontrol etme gibi işlevleri yerine getirebilen sistemlere sahip olabilirler.

Çevreyi takip edip dinleyerek kendisine iletilecek olan talebi yerine getirmeyi bekleyen bu sistemler, yeterli erişim hakkına sahip olan herkes tarafından, özellikle de dış kullanıcılar tarafından kullanılabilirler.

Bu yetkiler özenle ve dikkatli bir şekilde verilmezse, yetkisiz kişiler, internet üzerinden erişim ile ortamları dinleyebilir veya toplantılardan görüntüler kaydedebilirler.

3 GEREKSİNİMLER

İstemcilerin güvenli yönetimine ilişkin gereksinimler, bu başlıkta açıklanmaktadır. 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

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

Tablo 2. İstemci Yönetimi Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Operasyon Ekibi
Diğer Sorumlular	Bina hizmetleri, Kullanıcı

3.1 1.SEVİYE GEREKSİNİMLER

İstemcilerin işletimi için aşağıdaki gereksinimler öncelikli olarak dikkate alınmalıdır.

BTS.2.G1 Kullanıcı kimlik doğrulaması

İstemciyi kullanmak isteyen kullanıcıların mutlaka doğrulanması gerekmektedir. Kullanıcı kimlik doğrulamasında parolalar kullanılacaksa, bu parolalar, kurumun güvenlik politikasında belirtilen kriterlere uygun olmalıdır.

BTS.2.G2 Rollerin ayrıştırılması

Kullanıcılar, rutin işlemlerini yönetici rolü gibi ayrıcalıklı haklara sahip hesaplar ile gerçekleştirmemelidir. Ayrıcalıklı haklara sahip hesaplar, sadece sistem yöneticileri için tanımlanmalı ve yine sadece sistem yöneticileri sistem yapılandırmasını değiştirme, uygulamaları yükleyip kaldırma, sistem dosyalarını değiştirme veya silme yetkilerine sahip olmalıdır. Sistem dosyalarında standart kullanıcılar, yalnızca okuma yetkisi verilerek sınırlandırılmalıdır.

Yönetici görevlerinin yönetilmesi için süreçler ve gereksinimler tanımlanmalıdır. Buna ek olarak, BT sistemlerindeki farklı rollere sahip kullanıcılar için de gerekli tanımlamaların yapılması tavsiye edilmektedir.

BTS.2.G3 Otomatik güncelleme mekanizmalarının etkinleştirilmesi

Merkezi yazılım dağıtımı ile veya düzenli bir şekilde manuel güncelleme yapılmadığı durumlarda otomatik güncelleme mekanizmaları aktif edilmelidir. Otomatik güncelleme için bir zaman aralığı belirlenebiliyorsa, yeni güncellemelerin var olup olmadığının, günde en az bir defa kontrol edilecek şekilde ayarlanması tavsiye edilir.

BTS.2.G4 Düzenli yedekleme

Veri kaybını önlemek için kritik veriler düzenli olarak yedeklenmelidir. Bilgisayar sistemlerinin çoğunda otomatik yedekleme seçenekleri yer almaktadır. Yerel olarak depolanan verilerden hangilerinin, kimin tarafından ve ne zaman yedekleneceğine dair düzenlemeler yapılmalıdır. Yedeklenecek verilerin seçimiyle ilgili asgari bir tercih yapılacak olursa, tekrardan elde edilmesi mümkün olmayan veriler öncelikli olarak tercih edilmelidir. Kurumun veri yedekleme politikasına istemciler de dahil edilmelidir. Gizlilik seviyesi yüksek olan verilerin yedekleri şifreli olarak saklanmalıdır. Uygulama verilerinin yedeklemeye dahil edilip edilmeyeceğine ayrıca karar verilmelidir. Yedekten geri dönüş testleri yapılarak yedeği alınan verilerin sağlıklı bir şekilde geri döndürülebildiği düzenli aralıklarla kontrol edilmelidir. Kullanıcılar, istemcilerde hangi verilerin hangi şartlar altında yedeğinin alındığına dair düzenleme hakkında bilgilendirilmelidir.

BTS.2.G5 Ekran kilidi [kullanıcı]

İstemcilere yetkisiz erişimi önlemek için ekran kilitleri kullanılmalıdır. Hem belirli bir süre boyunca işlem yapılmadığında otomatik devreye giren hem de kullanıcılar tarafından manuel olarak aktif edilebilen ekran kilitlerinin kullanılması tavsiye edilmektedir. Ekran kilidinin, sadece başarılı bir kullanıcı kimlik doğrulamasından sonra devre dışı bırakılabilmesi sağlanmalıdır.

BTS.2.G6 Zararlı yazılımlardan koruma programlarının kullanımı

Zararlı yazılımların yol açabilecekleri istenmeyen durumların engellenmesi için zararlı yazılımlardan korunma programlarının kullanımı tavsiye edilir.

Zararlı yazılımlardan korunma programlarının veri tabanları, düzenli aralıklarla güncellenmelidir. Kullanılan programlar, bir uygulama veya bir veriye erişildiğinde devreye girerek gerçek zamanlı tarama yapabilmeli; ayrıca kullanıcının, isteğe bağlı olarak tarama yapabilmesine imkân sağlamalıdır. Sıkıştırılmış veya şifrelenmiş veriler de taranabilmelidir. İstemcilerde kurulu olan zararlı yazılımlardan korunma programlarının ayarlarının ve güvenlik seçeneklerinin, kullanıcılar tarafından yetkisiz bir şekilde değiştirilmesi veya tamamen kapatılması engellenmelidir.

BTS.2.G7 Loglama

İstemcilerde gerçekleşen hangi olay bilgilerinin loglara kaydedileceği, log kayıtlarının ne kadar süre ile saklanacağı ve hangi koşullar altında log kayıtlarının incelenebileceği önceden tanımlanmalıdır. Genel yaklaşım olarak, güvenlikle ilgili tüm sistem olayları loglara kaydedilmelidir.

BTS.2.G8 Önyükleme işleminin korunması

İstemcilerdeki önyükleme işlemi, dışarıdan yapılacak yetkisiz müdahalelere karşı korunmalıdır. Hangi ortamlardan veya aygıtlardan önyükleme yapılabileceği önceden tanımlanmalıdır. Önyükleme işleminin şifreli olarak yapılmasının gerekip gerekmediğine ve bunun nasıl sağlanabileceğine karar verilmelidir. İstemcileri, varsayılan önyükleme aygıtı veya ortamı dışında bir ortamla başlatabilme hakkı, sadece yetkili sistem yöneticilerinde olmalıdır. Buna ek olarak, sistem başlatma seçeneklerindeki değişiklikler, sadece ayrıcalıklı haklara sahip sistem yöneticileri tarafından yapılabilmelidir.

3.2 2.SEVİYE GEREKSİNİMLER

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

BTS.2.G9 İstemciler için bir güvenlik politikası oluşturulması

Kurumun genel güvenlik politikası temel alınarak, istemcilerin güvenli yönetimine dair ihtiyaçlar tanımlanmalıdır. İstemcilerin güvenli yönetim politikasının; istemcilerin tedarik edilmesinden hizmet dışı bırakılmasına kadar tüm yaşam döngüsünde görev alan personel ve kullanıcılar tarafından bilinmesi tavsiye edilir. Personelin ve kullanıcıların, çalışmalarında bu politikaları dikkate almaları tavsiye edilir. Politikanın içeriği düzenli olarak gözden geçirilmeli ve yapılan ilgili çalışmaların sonucu belgelenmelidir.

BTS.2.G10 İstemci işletiminin planlanması

İstemcilerin güvenli bir şekilde işletilebilmesi için nerede ve nasıl kullanılacağı kapsamlı bir şekilde planlanmalıdır. Planlama, istemcilerin yönetimini sadece güvenlik odaklı bir yaklaşımla ele almamalı, aynı zamanda pratikteki operasyonel faaliyetleri içerecek şekilde gerçekleştirilmelidir. İstemci türüne göre profiller oluşturularak gereksinimler tanımlanmalıdır. Buna ek olarak, sistem yöneticisi ve standart kullanıcı için gerekli istemci özelliklerinin tanımlarının da yapılması tavsiye edilir. Planlama aşamasında alınan tüm kararların belgelenmesi önerilir.

BTS.2.G11 İstemcilerin tedarik edilmesi

İstemciler tedarik edilmeden önce, piyasadaki ürünleri değerlendirebilmek için bir ihtiyaç listesi hazırlanmalıdır. İstemcilerin hedeflenen kullanım süresi boyunca gerekli olacak güvenlik güncellemeleri, üretici tarafından hızlı bir şekilde sağlanabilir olmalıdır. Tedarik edilecek olan sistemler, UEFI SecureBoot ve TPM için aygıt yazılımını (firmware) yapılandırma arayüzüne sahip olmalıdır.

BTS.2.G12 Yazılım uyumluluk kontrolü

Bir yazılım tedarik edilmeden önce, yazılımın mevcut istemcilerle uyumlu olup olmadığı kontrol edilmelidir. Yazılım üreticisi veya yazılımın dağıtımından sorumlu olan özgür yazılım toplulukları uyumluluk kontrolleri için ihtiyaç duyulan bilgileri sağlamıyorlarsa, uyumluluk kontrolü bir ortamda gerçekleştirilecek testlerle yapılmalıdır. Yaşanılabilecek bir donanım değişikliğinde veya sistem göçlerinde, değişiklikten etkilenen tüm donanımlar için sürücü yazılımlarının sağlanabiliyor olduğu garanti altına alınmalıdır.

BTS.2.G13 Kod çalıştırılabilen ortamlara erişim

Kod çalıştırılabilen disk alanlarına, sistem dosyalarının bulunduğu klasörlere veya aygıt yazılımlarının bulunduğu alanlara erişim sadece sistem yöneticisi ayrıcalıklarına sahip kullanıcı hesaplarıyla mümkün olmalıdır. İlgili kısıtlamaların ayarlanabildiği BIOS, UEFI gibi ara yüzlere erişimler ise parolalar ile korunmalıdır. Eğer bu yapılandırmalar işletim sistemi üzerinden yapılıyorsa, ayarların yapıldığı ilgili ara yüzler, sadece yetkili sistem yöneticilerinin erişebileceği şekilde kısıtlanmalıdır.

BTS.2.G14 Güncellemeler ve yamalar

Sistem yöneticileri, bilinen güvenlik açıklarına karşı sistemleri düzenli olarak kontrol etmelidir. Tespit edilen güvenlik açıkları mümkün olan en kısa zamanda kapatılmalıdır. Yamalar ve güncellemeler, sadece güvenilir kaynaklardan temin edilmelidir. Gerekli ise, ilgili uygulamalar veya işletim sistemleri güncellemeden sonra yeniden başlatılmalıdır. Tespit edilen güvenlik açıkları için henüz herhangi bir güncelleme veya yama yayınlanmamış ise, güvenlik açığının seviyesine bağlı olarak alternatif BT çözümleri değerlendirilmelidir.

BTS.2.G15 İstemcilerin güvenli kurulumu ve yapılandırması

İstemciye kurulması önerilen işletim sistemi bileşenleri, uygulamalar ve araçlar önceden tanımlanmalıdır. Kurulumlar ve yapılandırmalar, önceden tanımlanmış süreçlere göre, sadece yetki verilmiş sistem yöneticileri tarafından gerçekleştirilmelidir. Tüm kurulum ve konfigürasyon adımları belgelenmelidir (bkz. *“BTS.2.G40 İşletim belgeleri”*).

İstemcilerin temel yapılandırma ayarları, gerektiğinde güvenlik rehberlerine göre gözden geçirilmeli ve yeniden düzenlenmelidir. İstemcilerin, ancak tüm temel güvenlik yapılandırmaları tamamlandıktan sonra internete bağlanmalarına izin verilmelidir.

BTS.2.G16 Gereksiz bileşenlerin ve kullanıcı hesaplarının kaldırılması

İstemci kurulumu tamamlandıktan sonra; hangi aygıt yazılımlarının, hangi işletim sistemi bileşenlerinin, hangi uygulamaların ve araçların istemciye yüklenip etkinleştirildiği gözden geçirilmelidir. İhtiyaç duyulmayan yazılımlar, bileşenler, araçlar ve ara yüzler devre dışı bırakılmalı veya tamamen kaldırılmalıdır. Buna ek olarak, ihtiyaç duyulmayan çalıştırma ortamları ve derleyiciler istemciden kaldırılmalı, istemciye bağlanmış ancak gerekli olmayan tüm bileşenler devre dışı bırakılmalıdır. İhtiyaç duyulmadığı için devre dışı bırakılan bu bileşenlerin yetkili olmayan kullanıcılar tarafından yeniden etkinleştirilebilmesi önlenmelidir. Bütün bu yapılandırmalar belgelendirilmelidir.

BTS.2.G17 Kullanıma sunma

İstemci, kullanıma sunulmadan ve kurum canlı ağına bağlanmadan önce bir onay süreci işletilmelidir. Onay sürecinde, istemci bir test ortamında işlevsellik testlerine tabi tutulmalı, kurulum ve yapılandırma belgeleri incelenmelidir. Bu onay süreci, kurumun yetkilendirilmiş birimleri tarafından işletilmeli ve gerçekleştirilen işlemler belgelenmelidir.

BTS.2.G18 İletişim bağlantılarının şifrelenmesi [kullanıcı]

İletişim için kurulan bütün bağlantılar mümkün olduğunca şifrelenmelidir. Kullanıcılar da erişim sağladıkları web sayfaların SSL/TLS kullanmasına dikkat etmelidir.

BT birimi, istemcide desteklenen TLS'in güvenilir ve güncel bir sürüm olup olmadığını kontrol etmelidir. İstemcilerde, kurumun güvenlik politikasına uygun olan, son teknolojiye sahip şifreleme algoritmaları ve yeterli uzunlukta şifreleme anahtarları kullanılmalıdır.

Yeni sertifikalar "sertifika parmak izi" kontrol edildikten sonra etkinleştirilmelidir. Sertifikaların doğrulanması özelliği, tarayıcılar ve e-posta istemcileri gibi uygulamalarda aktif hale getirilmelidir. Oturumun yeniden oluşturulması ve TLS sıkıştırması gibi özellikler devre dışı bırakılmalıdır.

BTS.2.G19 Kısıtlayıcı hakların tahsisi

İstemcilerde, kullanıcı veya kullanıcı gruplarına, sadece sorumlu oldukları işleri yapabilecekleri kadar yetki verilmelidir. Erişim hakları mümkün olduğunca kısıtlayıcı bir şekilde tanımlanmalıdır. Özellikle sistem dizinleri ve sistem dosyalarına erişim için verilen yetkilerin kurumun güvenlik politikasına uygun olup olmadığı, düzenli aralıklarla kontrol edilmelidir. Mümkünse, sistem dosyaları yalnızca sistem yöneticileri tarafından erişilebilir

olmalıdır. Ayrıcalıklı yetki verilmiş sistem yöneticileri sayısının mümkün olduğunca az olması önerilmektedir.

BTS.2.G20 Yönetim ara yüzlerinin korunması

İstemcilerin yerel veya ağ üzerinden merkezi olarak yönetilmesine bağlı olarak, uygun güvenlik önlemleri alınmalıdır. İstemcilerin yönetiminde kullanılacak yöntem, güvenlik politikasında tanımlanmalı ve sistem yöneticilerinin güvenlik politikasındaki tanımlamalara uygun olarak çalışmaları sağlanmalıdır. Ağ üzerinden gerçekleştirilen yönetim amaçlı erişimlerde güvenli protokoller kullanılmalıdır.

BTS.2.G21 İstemci mikrofon ve kameralarının yetkisiz kullanımının önlenmesi

İstemci üzerinde bulunan mikrofon ve kameraya erişim, kullanıcının istemciye sadece yerel olarak bağlandığı müddetçe mümkün olmalıdır. İstemci üzerinde bulunan mikrofon ve kamera hiç kullanılmayacaksa veya istenmeyen şekilde kullanımının önüne geçilmek isteniyorsa; bunlar kapatılmalı, devre dışı bırakılmalı veya cihazdan fiziksel olarak tamamen ayrılmalıdır. Kameraların ve mikrofonların nasıl kullanılacağı ve bu aygıtlara erişim haklarının nasıl düzenleneceği tanımlanmalıdır.

BTS.2.G22 Oturumun kapatılması [kullanıcı]

Özellikle birden fazla kullanıcının aynı istemciyi kullandığı durumlarda; kullanıcılar, görevlerini tamamlandıktan sonra istemciden veya uygulamadan çıkmaya zorlanmalıdır. Bir kullanıcı, çalışmasına kısa bir ara verecekse oturum kapatma yerine ekran kilidini etkinleştirebilir. İstemcinin uzun bir süre kullanılmadığı durumlarda, ekran kilitleri otomatik olarak devreye girmeli veya kullanıcı oturumu otomatik olarak sonlandırılmalıdır.

BTS.2.G23 İstemci-sunucu hizmetlerinin kullanımı

Veri aktarımları gerçekleştirilirken, mümkün olduğu müddetçe, sadece bu iş için özelleştirilmiş sunucu hizmetlerinin kullanılması önerilir. İstemcilerin bu amaçla birbirleriyle doğrudan bağlantıları kurmaları tavsiye edilmemektedir. Eğer istemciden istemciye bir bağlantı yapılacaksa, hangi servislerin kullanılacağı ve hangi verilerin transfer edileceği belirlenmelidir. Kullanıcılar, bu hizmetleri nasıl kullanacakları konusunda eğitilmelidir. İstemciler arasındaki doğrudan bağlantılar, sadece LAN ile sınırlı olmalıdır. Otomatik keşif protokolleri mümkün olduğunca kısıtlanmalıdır.

BTS.2.G24 Çıkarılabilir medyanın kullanımı

İstemciler üzerinde bulunan CD, DVD sürücü veya USB portları gibi arabirimler kullanılarak istenmeyen yazılımların yüklenebilmesi veya verilerin izinsiz olarak bu

ortamlara kopyalanabilmesi engellenmelidir. Bu ara yüzlerin kullanımı, mümkün olduğunca kısıtlı tutulmalıdır. Genel olarak istemcilerin, güvenilmeyen kaynaklardan elde edilen çıkarılabilir medyalara ve verilere erişmesi engellenmelidir.

BTS.2.G25 BT güvenli kullanım politikası [kullanıcı]

Tüm çalışanlara yönelik olarak; BT sistemlerini kullanırken hangi çalışma çerçevesine bağlı kalacaklarını ve hangi güvenlik önlemlerini almaları gerektiğini açık bir şekilde anlatan BT güvenli kullanım politikası hazırlanmalıdır. Bu politika, aşağıdaki hususları içermelidir:

- Kurumun güvenlik hedefleri,
- Önemli koşullar,
- Bilgi güvenliği ile ilgili görevler ve roller,
- Bilgi güvenliği ihlal olayları için iletişim noktaları,
- Çalışanlar tarafından uygulanacak ve takip edilecek güvenlik önlemleri.

Güvenlik politikası, tüm çalışanlar tarafından bilinmelidir. Her yeni çalışan, BT sistemlerini kullanmadan önce politikadan haberdar olduğunu ve kurumun BT güvenli kullanım politikasına sadık kalacağını kabul etmelidir. Politikada yapılan önemli değişikliklerden sonra veya en geç iki yılda bir çalışanlara güvenli kullanım politikası tekrar aktarılmalı ve çalışanların onayı yeniden alınmalıdır.

BTS.2.G26 Uygulamaların korunması

Uygulamalardaki güvenlik açıklarının zafiyete sebep vermesini zorlaştırmak için, ASLR ve DEP/NX koruması etkinleştirilmeli ve uygulamalar tarafından kullanılmalıdır. Sistem çekirdeği seviyesindeki varsayılan güvenlik özellikleri ve kütüphaneleri devre dışı bırakılmamalıdır.

BTS.2.G27 İstemcinin kontrollü olarak hizmet dışı bırakılması

Bir istemci hizmet dışı bırakılırken, disklerinde önemli ve hassas verilerin bırakılmadığından emin olunmalıdır. İstemcilerde hangi verilerin depolandığına dair genel bir bilgi oluşturulmuş olmalıdır. İstemci hizmet dışı bırakılır iken kullanılmak üzere, bir kontrol listesi oluşturulmalıdır. Bu kontrol listesinde, hassas ve önemli verilerin yedeklendiğini ve yedekleme işlemi yapıldıktan sonra güvenli olarak silindiğini teyit eden maddeler yer almalıdır.

3.3 3.SEVİYE GEREKSİNİMLER

1. ve 2. seviye gereksinimler sonrasında, istemcilerin yönetimi için artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların

kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilmektedir. Gereksinim tarafından öncelikli koruma sağlanan prensip, parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

BTS.2.G28 İstemcilerin şifrelenmesi (G)

Gizliliği yüksek verilerin istemcilerde barındırıldığı durumlarda; ilgili dosyaların, belirli klasörlerin veya yerel diskin tamamının şifrelenmesi önerilmektedir. Bu doğrultuda disk şifreleme ile ilgili ayrı bir politika oluşturulmalıdır. Herhangi bir hata durumunda, şifrelenmiş verilerin tamamının kaybolma riski olduğu için, bu politika içinde şifrelemeye dair yapılandırma detayları özellikle ele alınmalıdır. Bu kapsamda, aşağıda belirtilen hususlar düzenlenmelidir:

- Kimlik doğrulama yöntemi (parola, PIN, token),
- Kurtarma bilgilerinin saklanması,
- Şifrelenecek sürücülerin ve disklerin belirlenmesi,
- Şifrelenmemiş ortamlara erişim yetkilerinin düzenlenmesi,
- Kurtarma bilgilerinin yalnızca yetkili kişiler tarafından erişilebilir olmasının sağlanması.

Şifreli dosyalar, bölümler veya depolama birimleri de düzenli yedeklemeye dâhil edilmelidir. Kullanılan güvenlik anahtarı açık metin olarak saklanmamalıdır. Şifrelenmiş verilerin çözümlenmesi için kullanılan aygıt veya ortam kaybedildiğinde takip edilmesi gereken adımlar konusunda kullanıcılar eğitilmelidir.

BTS.2.G29 Sistem izleme (E)

İstemciler; sistem sağlık durumunu ve işlevselliğini sürekli olarak takip eden, arıza veya takip edilen parametrelerin tanımlanmış eşik değerleri dışına çıktığı durumlarda ilgili personele bildirim sağlayan bir izleme sistemi aracılığı ile izlenmelidir.

BTS.2.G30 Referans sistem kurulumu (GBE)

İstemciler için, temel yapılandırma ayarlarını içeren referans bir kurulum oluşturulmalıdır. İstemci yapılandırma ayarlarında yapılacak herhangi bir değişiklik, güncelleme ve yama istemciye uygulanmadan önce referans ortamında test edilmelidir. Böyle bir referans ortamının, istemcilerin çoklu sayıda kurulumunu kolaylaştırmak amacıyla da kullanılması önerilir.

Tipik ve sık tekrarlanan testlerde kullanılmak üzere kontrol listeleri oluşturulmalıdır. Yapılan testler belgelenmelidir.

BTS.2.G31 Yerel güvenlik duvarı kullanımı (GBE)

Merkezi güvenlik duvarına ek olarak, istemcilerde yerel güvenlik duvarlarının kullanımı önerilmektedir. Güvenlik duvarında beyaz liste stratejisinin uygulanması tavsiye edilir.

BTS.2.G32 Açıklara karşı ek koruma tedbirleri (GBE)

İstemcileri açıklara karşı koruyacak ek tedbirler alınmalıdır. Kurumda mevcut kullanılan sistemler, yazılımlar veya araçlarla bu güvenlik tedbirleri alınamıyorsa, uygun ek güvenlik ürünleriyle bu gereksinim karşılanmalıdır. Ek güvenlik ürünleriyle dahi bu önlemler alınamıyorsa, idari açıdan tedbirler alınabilir.

BTS.2.G33 Uygulama beyaz listesi (GBE)

Yalnızca izin verilen uygulamaların ve betiklerin çalıştırılabilmesini sağlamak; bunlar dışında uygulamaların çalışmasını engellemek için yazılım beyaz listesi kullanılmalıdır. Beyaz liste olabildiğince sınırlı/dar tutulmalıdır. Uygulamalara dair dosya yolu ve özetleme adresinin açıkça saptanamadığı durumlarda, beyaz liste kuralları oluşturulurken sertifika tabanlı ve uygulama dizin adresini içeren tanımlar kullanılmalıdır.

BTS.2.G34 Uygulama izolasyonu (GBE)

Harici verileri işleyen uygulamalar, işletim sisteminden izole edilmiş ortamlarda çalıştırılmalıdır.

BTS.2.G35 Kök sertifikaların aktif yönetimi (BE)

İstemcinin tedarik edilmesi ve kurulumu esnasında, istemci kullanımında hangi kök sertifikalarının gerekli olduğu belgelenmelidir. İstemcide yalnızca, gerekli olan ve daha önce belgelenmiş olan kök sertifikaları kullanılmalıdır. Mevcut kök sertifikalarının, kurumun güvenlik gereksinimlerini karşılayıp karşılamadığı düzenli olarak kontrol edilmelidir. İstemcideki, tüm sertifika alanları denetime tabi tutulmalıdır (UEFI sertifika alanı, web tarayıcılarının sertifika alanı, vb.).

BTS.2.G36 Güvenli önyükleme ve TPM yongası kullanımı (BE)

UEFI uyumlu sistemlerde, önyükleyici, sistem çekirdeği ve gerekli tüm aygıt yazılım bileşenleri, öz kontrol mekanizmasına sahip anahtarlar tarafından imzalanmalı ve gereksiz anahtarlar devreden çıkarılmalıdır. TPM yongası, gerekli olmadığı durumda devre dışı bırakılmalıdır.

BTS.2.G37 Yetkisiz oturum açma olaylarına karşı korunma (GBE)

Ele geçirilmiş kimlik bilgileriyle, bir saldırganın istemciye erişimini engellemek için çok faktörlü kimlik doğrulaması kullanılmalıdır.

BTS.2.G38 Acil durum eylem planlaması (E)

İstemciler, acil durum yönetim sürecine dahil edilmelidir. Kurtarma planları, sistem önyükleme ortamının oluşturulması, şifrelerin ve şifreleme anahtarlarının güvenli bir şekilde saklanması gibi acil durum prosedürleri oluşturulmalıdır.

BTS.2.G39 Kesintisiz güç kaynakları [bina hizmetleri] (E)

İstemciler için erişilebilirliğin yüksek seviyede bir gereksinim olduğu durumlarda, istemcilerin kesintisiz güç kaynağına (UPS) bağlanmaları gerekir. Güç ve destek süresi dikkate alınarak UPS'ler yeterli ve doğru bir şekilde ölçeklendirilmelidir. UPS'e bağlı donanımlarda adet ve güç tüketimi açısından değişim yaşandı ise, UPS güç destek süresinin yeterli olup olmadığı tekrar kontrol edilmelidir. Hem UPS'ler hem de istemciler aşırı gerilime karşı korunmalıdır. Akülerin gerçek kapasitesi ve dolayısıyla UPS'in sağladığı destek süresi düzenli olarak test edilmelidir.

BTS.2.G40 İşletim belgeleri (EB)

İstemciler ile ilgili yapılan bütün işlemler, kapsamlı bir şekilde belgelendirilmelidir (ör. kim, ne zaman, hangi çalışmayı yaptı?). Özellikle, yapılandırma ayarlarında yapılan değişiklikler kayıt altına alınan belgeler üzerinden geriye dönük olarak izlenebilir olmalıdır. Otomatik olarak belgelendirilebilecek her şey otomatikleştirilmelidir. Belgeler yetkisiz erişim ve veri kayıplarına karşı korunmalıdır.

BTS.2.G41 Depolama alanlarını kapasite aşımından koruma (E)

Kullanıcıların, yerel fiziksel depolama alanlarında aşırı disk kullanımını önlemek için kota uygulanmalıdır. Kota kullanımı lle birlikte disk doluluğu belli bir seviyeye ulaştığında kullanıcıları uyaracak bir sistem de kullanılabilir.

BTS: BT SİSTEMLERİ

BTS.2.U İSTEMCİ YÖNETİMİ

UYGULAMA REHBERİ

BTS.2.U İSTEMCİ YÖNETİMİ

UYGULAMA

1 AÇIKLAMA

1.1 TANIM

İstemci; ağ üzerindeki sunucuları veya diğer BT kaynaklarını kullanan kullanıcı bilgisayarlarıdır. Genel olarak istemciler, sunucularda çalışan uygulamalardan veya hizmetlerden talepte bulunan, veri veya sonuç isteyen bilgisayarlardır.

"İstemci Yönetimi Rehberi", istemcilerin tedariğinden başlayarak, kullanım dışına çıkarma işlemine kadar olan bütün süreçlerin güvenli bir şekilde yönetilebilmesini ele almaktadır.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

İstemcilerin güvenli yönetimi için temel koşullar kapsamlı bir şekilde tanımlanmalıdır. Bu tanımlara, mevcut BT sistemleri ve planlanan işletim senaryoları için güvenlik gereksinimleri en baştan dâhil edilmelidir (bkz. *"BTS.2.U10 İstemci işletiminin planlanması"*). İstemciler ve yazılımlar tedarik edilmeden önce güvenlik politikası oluşturulmalıdır (bkz. *"BTS.2.U9 İstemciler için güvenlik politikasının oluşturulması"*).

Tedarik

İstemciler tedarik edilmeden önce, istemcilerin genellikle yüksek adette satın alındıkları da göz önünde bulundurularak, uygun ürünlerin seçimine yönelik kıstaslar kullanım senaryoları dikkate alınarak belirlenmelidir (bkz. *"BTS.2.U11 İstemcilerin tedarik edilmesi"*). Sonradan yapılan tekil satın almalarda, alınacak istemcilerin mevcut yapıya uyumlu olmasına dikkat edilmelidir. Böylece, sonradan tedarik edilen az sayıda da olsa istemcinin uyumsuzluk sorunundan dolayı oluşacak entegrasyon ve işletim ek maliyeti engellenebilir.

Donanım veya yazılım, önceden tanımlanmış güvenlik gereksinimlerini karşılamazsa ilave tedbirlere ihtiyaç duyulur. Bunlar, idare tarafından alınacak yönetimsel önlemler olabileceği gibi ek donanım/yazılımların tedarik edilmesi gibi maliyet içerek önlemler de olabilir.

Özellikle istemcilerin erişilebilirlik oranının yüksek olmasının beklendiği durumlarda, kesintisiz güç kaynağı (UPS) kullanımı önerilir (bkz. *"BTS.2.U39 Kesintisiz güç kaynağı"*). Bunun için istemciye özel, tekil UPS donanımları kullanılabileceği gibi, merkezi UPS sistemleri de tercih edilebilir.

Uygulama

İstemcilerin, kasıtlı veya kasıtsız yanlış kullanım riskini ortadan kaldırmak için; işletim sistemi ve yazılımların doğru seçimi, güvenli kurulumu ve yapılandırılması önemlidir. Alınacak önlemler büyük ölçüde, tercih edilen işletim sistemine bağımlıdır.

Güvenliğin temeli, aslında kuruluma hazırlık aşamasında atılmaktadır. Kuruluma başlamadan önce, hangi işletim sistemi bileşenlerinin, uygulamaların ve araçlarının kurulacağı belirlenmelidir. İhtiyaç duyulduğunda; istemcinin nasıl yapılandırıldığının ve istemci üzerine hangi yazılımların kurulduğunun anlaşılabilmesi için alınan kararlar belgelenmelidir (bkz. *"BTS.2.U15 İstemcilerin güvenli kurulumu ve yapılandırılması"*).

İşletim

Güncel bir zararlı yazılımlardan korunma programının kullanımı, günümüzde istemcileri korumak için tercih edilen en önemli ve etkin güvenlik önlemlerinden biridir (bkz. *"BTS.2.U6 Zararlı yazılımlardan korunma programlarının kullanımı"*). Ayrıca, verileri düzenli olarak yedeklemek; donanım, yazılım veya kullanıcı hataları sonucuyla yaşanabilecek veri kayıplarının önüne geçmek için en temel ön koşuldur (bkz. *"BTS.2.U4 Düzenli yedekleme"*).

Kullanım Dışı Bırakma

Bir istemciyi hizmet dışı bırakmadan önce, tüm kullanıcı verilerinin bir depolama sistemine aktarılması sağlanmalıdır. Daha sonra, istemcinin sabit disklerinde hiçbir şekilde hassas verinin kalmadığından emin olunmalıdır. Diskteki verileri tamamen ortadan kaldırmak için diskleri biçimlendirmek tek başına yeterli değildir. Sabit disk üzerindeki hassas verinin tamamen ortadan kaldırılması için güvenli biçimlendirme uygulamaları kullanılmalı veya diskin tamamının üzerine en az bir kez başka bir veri yazılmalıdır. İstemci hizmet dışı bırakıldıktan sonra, envanter bilgileri ve ağ kayıtları güncellenmelidir.

Acil Durum Hazırlık Planı

İstemcinin acil durum hazırlığının ne seviyede yapılması gerektiği, istemcinin kullanım amacına göre değişiklik gösterebilir. Genel bir önlem olarak; istemcide bulunan kurumsal hassas verilerin düzenli olarak yedeklenmesi ve acil durumlar için ön yüklenebilir bir veri ortamının oluşturulması yeterli olacaktır (bkz. *"BTS.2.U38 Acil durum eylem planlaması"*). Özel erişilebilirlik gereksinimi olan istemciler için, yedek bir sistemin hazırda bekletilmesi gibi ek önlemlerin alınması planlanabilir.

2 UYGULAMALAR

İstemcilerin güvenli yönetimi için gerekli uygulamalar aşağıda verilmiştir.

2.1 1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların tüm sunucularda öncelikli olarak ele alınması önerilmektedir.

BTS.2.U1 Kullanıcı kimlik doğrulaması

İstemcilere veya uygulamalara erişim için kullanılan kimlik saptama ve doğrulama mekanizmaları, kullanıcıların benzersiz bir şekilde tanımlanmasını ve doğrulanmasını sağlayacak şekilde tasarlanmalıdır. Kimlik saptama ve doğrulama işlemi, kullanıcının istemci üzerinde herhangi bir işlem yapmasından önce gerçekleşmelidir. Kullanıcıların istemci üzerinde herhangi bir işlem yapabilmeleri, kimlikleri doğrulandıktan sonra mümkün olabilmelidir. Kimlik doğrulama bilgileri, sadece yetkili kullanıcıların erişebileceği bir yerde tutulmalıdır.

Bir kullanıcı kimliğini doğrulayabilmek için kullanılan çeşitli yöntemler vardır. En çok bilinen yöntemlerden bazıları şunlardır:

- PIN'ler (Personal Identification Number : Kişisel Kimlik Numaraları),
- Parolalar,
- Akıllı Kartlar, vb.,
- Biyometrik özellikler.

Kritik uygulamalarda güvenliği artırmak için parolalara ek olarak, yapılan işleme özel üretilmiş işlem numarası ile birlikte tek seferlik parolalar veya akıllı kart gibi iki veya daha fazla kimlik doğrulama tekniğini birleştiren güçlü kimlik doğrulama yöntemleri kullanılmalıdır. Bu tip koruma yöntemleri, iki faktörlü kimlik doğrulama veya çok faktörlü kimlik doğrulama (Multi-Factor Authentication-MFA) olarak adlandırılır. Kullanılan kimlik doğrulama yöntemlerinin güncel teknolojiye sahip olması önerilmektedir.

Parolalar

İstemcilerde kimlik doğrulaması amacıyla sadece parolalar kullanılırsa, güvenlik büyük ölçüde doğru parola kullanımına bağımlı kalır. Bu sebeple, doğru parola seçimi ve kullanımıyla ilgili bir talimat hazırlanıp yayımlanmalıdır. Ayrıca kullanıcılar düzenli aralıklarla bu konu hakkında bilgilendirilmelidir.

Kimlik doğrulaması olarak parola kullanımı tercih edildiğinde, aşağıdaki hususların sağlanması gerekir:

- Her bir kullanıcı bireysel parola kullanmalı ve bunu kendi oluşturabilmelidir.

- Parolalar güvenlik politikasında tanımlı özellikleri sağlayabilmelidir (ör. asgari uzunluk, basit kelimelerin engellenmesi vb.). Parolanın kalitesi her kıstas için ayrı ayrı kontrol edilebilmelidir. Örnek olarak; kurum tarafından oluşturulmuş parola politikasındaki herhangi bir özelliğe uymayan parolalar kabul edilmemelidir.
- BT sistemleri tanımlanan özellikleri sağlayan parolaları otomatik olarak üretip kullanıcıya önerebilmelidir.
- Parola değişimi, BT sistemleri tarafından belirlenmiş süre sonunda otomatik olarak zorlanmalıdır. Bir parolanın ömrü ayarlanabilir olmalıdır.
- Parola değiştirilirken eski parolaların tekrar kullanılması engellenmelidir.
- Parola girilirken ekranda gizlenmelidir.
- Kullanıcı yeni oluşturulmuşsa, kullanıcı ilk kez oturum açma esnasında parola değişikliğine zorlanmalıdır.

BTS.2.U2 Rollerin ayrıştırılması

Temel olarak, standart kullanıcılar ve sistem yöneticileri arasında rol ayrımı yapılabilir. Sadece yönetici yetkilerine sahip olan kullanıcı hesaplarının BT sistemlerini yönetebilmesi sağlanırken, standart kullanıcıların ise sadece görevleri çerçevesinde yetkiler tanımlanmalıdır. Kasıtlı veya kasıtsız olarak işletim sistemi ve istemci ayarlarının değiştirilmesinin önüne geçmek için, standart kullanıcılar yönetici haklarına sahip olmamalıdır.

Eğer bir kullanıcının sadece belirli yönetici görevlerini yerine getirmesi gerekiyorsa, o kullanıcıya, yönetimle ilgili tüm yetkilerin tanımlanmasına gerek yoktur. Özellikle, geçici olarak görevlendirilmiş bir personele veya dışardan belirli bir süre destek veren kullanıcıya, sadece görevli olduğu işi yerine getirecek kadar yetki tanımlanmalıdır. Belli bir görev için verilen yönetici yetkileri, kullanıcının o işle ilgili görevi sona erdiğinde mutlaka geri alınmalı, hatta kullanıcı hesabı devre dışı bırakılmalıdır.

Mümkünse, kullanıcılara sınırlı bir kullanıcı ortamı sağlanmalıdır. Örneğin, Unix altında kısıtlanmış bir kabuk (rsh) sağlamak veya “chroot” Unix komutu ile erişim yollarının kısıtlanması gibi. Bu yaklaşıma dair bir diğer örnek ise; web tarayıcısı gibi uygulamaların kiosk modunda, yani sadece sınırlı erişim yetkilerine sahip bir şekilde çalıştırılması olabilir.

Kullanıcılara ayrıcalıklı hakların mutlak surette atanması gerekiyorsa ayrıcalıklı haklar mümkün olduğunca kısıtlı tutulmalıdır. Bir yandan ayrıcalıklı haklara sahip kullanıcı hesapları olabildiğince kısıtlı tutulmalı, diğer yandan kullanıcılara sadece tanımlanmış görevlerini yerine getirebilecekleri kadar yetki tanımlanmalıdır. Ayrıcalıklı haklara gerek

duyulmadan yapılacak tüm diğer işlerde, standart haklara sahip olan hesaplar kullanılmalıdır.

BTS.2.U3 Otomatik güncelleme mekanizmalarının etkinleştirilmesi

Birçok üründe, yamalar veya güncellemeler olduğunda kullanıcıları bilgilendiren otomatik güncelleme mekanizmaları bulunur. Bu ürünler genellikle, güncellemeleri internet üzerinden anında indirip yükleme seçeneği de sunarlar. Güncellemeler için düzenli manuel işletim yapılmıyor veya merkezi yazılım dağıtım sistemi gibi mekanizmalar kullanılmıyorsa, otomatik güncelleme mekanizmaları etkinleştirilmelidir. Otomatik güncelleme mekanizmasının işlevselliği üreticiye, kullanılan yazılım sürümüne ve kurulum tercihlerine göre değişkenlik gösterebilir.

Yazılım güncelleme mekanizmaları aşağıdaki şartları sağlamalıdır:

- Güncelleme sunucusunun doğruluğu kontrol edilmelidir.
- Güncelleme paketlerinin yanı sıra güncelleme bilgileri de şifreli olarak taşınmalıdır.
- Güncelleme yapmadan önce güncelleme sunucusundan alınan verilerin bütünlüğü kontrol edilmelidir.
- Kritik öneme sahip eylemlerin izlenebilmesi için güncelleme işlemleri loglara kaydedilmelidir. Loglar merkezi olarak tutulmalı ve işlenebilmelidir.
- Genel prensip olarak, yapılan güncellemeler ilgili yazılımın yapılandırma ayarlarını değiştirmemelidir. Eğer bu durum güvenlik açısından zorunlu ise, özel hassasiyet gösterilmeli ve kayıt altına alınmalıdır.
- Güncellemeler, uyumluluk sorunları yaşanması durumunda geri alınabilir olmalıdır.
- İnternet bağlantısı olmasa bile güncellemeler yapılabilir olmalıdır.
- Yerel ağda bir güncelleme sunucusu kurarak, güncellenecek istemcileri merkezi olarak yönetmek ve güncellemeleri merkezi olarak dağıtmak mümkün olmalıdır.
- Her bir güncelleme, istemcilerde en az ayrıcalıklı haklar ile yüklenebilir olmalıdır.
- İstemciler, yeni güncellemelerin olup olmadığını otomatik olarak denetleyebilmelidir.
- İstemcilerin güncelleme seçenekleri yapılandırılabilir olmalıdır (güncellemeleri kontrol etme sıklığı ve yükleme zamanları gibi).

Otomatik güncelleme özelliğine sahip BT sistemleri, önceden ayarlanmış aralıklarla veya her yeni başlatıldıklarında bir güncelleme sunucusuna bağlanarak yeni güncellemelerin olup olmadığını denetlerler. BT sistemleri otomatik güncelleme için birkaç farklı seçenek sunabilir. Yeni BT bileşenleri devreye alındığında hangi güncelleme mekanizmasına sahip olduğu ve bunların nasıl ayarlanacağı kontrol edilmelidir. Ayrıca, otomatik

güncelleme esnasında üreticiye hangi bilgilerin aktarıldığına da dikkat edilmelidir. Öncelikli olarak, otomatik güncelleme mekanizmasının nasıl çalıştığı net olarak bilinmelidir. Ardından, bu mekanizmanın nasıl yapılandırıldığı öğrenilmelidir. BT sistemlerinin dış dünya ile kontrolsüz bir şekilde bilgi alışverişi yapmasının engellenmesi isteniyorsa, güvenlik duvarları veya paket filtreleme uygulamaları kullanılmalıdır. Eğer güncelleme için istemcinin dış dünya ile bağlantı kurması istenmiyorsa; çoğu yazılım için istemciler, üreticinin internet adresi yerine iç ağda bulunan bir güncelleme sunucusuna yönlendirilebilir.

Bazı üreticiler, güncelleme servisinin yerel olarak kurulabildiği bir güncelleme sunucusu veya ayna sunucusu çözümü sunabilirler (ör. Windows Server Update Services WSUS). Bu güncelleme sunucuları, doğrudan üreticinin internetteki sunucusuyla iletişim kurar ve istenen güncellemeleri indirir. Bu tür bir çözüm sayesinde, kurumun BT sistemlerinin her birinin güncelleme için üreticinin güncelleme sunucusu ile iletişim kurmasına ihtiyaç kalmamaktadır. Aynı zamanda bu çözüm, kurumun güncelleme için oluşturacağı internet trafiğinin en aza indirilmesini sağlar. Güncelleme sunucuları ayarları, grafik kullanıcı ara yüzü (GUI) ile kolayca yapılabilir.

Güncelleme metodu olarak, üreticinin internete açık güncelleme sunucuları kullanılacaksa, öncelikli olarak sunucunun doğruluğu kontrol edilmelidir. Daha sonra, yeni güncellemelerin var olup olmadığının denetlenmesi işleminin, tanımlanmış zaman aralıklarında mı yoksa bir olayla mı tetikleneceği belirlenmelidir. Bu ayarlar kurumun politikalarına uygun olarak yapılmalıdır.

Güncelleme sunucularıyla yapılacak veri alışverişinin mümkün olduğunca asgari düzeyde olması sağlanmalıdır. Ayrıca, üreticinin güncelleme sunucularına yapılan bağlantının tek alternatif olarak mı kullanılacağına yoksa iç ağdaki bir güncelleme sunucusunun da var olduğu diğer yöntemin mi kullanılacağına karar verilmelidir.

Otomatik güncelleme konfigürasyonuyla ilgili olarak; güncellemelerin dâhili bir BT sistemine indirilip indirilmeyeceği, güncelleme tercihinin kullanıcıya bırakılıp bırakılmayacağı veya indirildikten hemen sonra kullanıcıya sormadan otomatik olarak yüklenip yüklenmeyeceği gibi tercihler karara bağlanmalıdır.

İstemcinin, bir güncelleme sonunda yeniden başlatılması gerekirse bunun nasıl yapılacağı belirlenmelidir. İstemci güncellemeler yüklendikten hemen sonra yeniden başlatılabilir veya yeniden başlatma işlemi daha sonraya bırakılabilir. Yeniden başlatma işlemi sonraya bırakılırsa bazı güncellemelerin tam olarak etkin olmayabileceği bilinmelidir.

BTS.2.U4 Düzenli yedekleme

Veri kaybını önlemek için kritik veriler düzenli olarak yedeklenmelidir. BT sistemlerinin çoğunda otomatik yedekleme seçenekleri vardır. Yerel olarak depolanan verilerden hangilerinin, kim tarafından ve ne zaman yedekleneceğine dair düzenlemeler yapılmalıdır

Yedeklenecek verilerin seçimiyle ilgili asgari bir tercihin yapılması gerektiği durumda, tekrardan elde edilmesi mümkün olmayan veriler öncelikli olarak yedeklenmelidir. Kurumun güvenlik gereksinimleri göz önünde bulundurarak istemciler için bir veri koruma konseptinin oluşturulması tavsiye edilir.

Not: Kurumsal politika gereği kullanıcıların tüm çalışmalarını merkezi sunucularda saklıyor olmaları beklense dahi, iş ile ilgili bir takım veriler istemcilerde bulunabilir. Bu nedenle, istemciler de kurumun veri yedekleme politikasına dâhil edilmelidir.

Verilerin miktarına, önemine, bu verilerin kaybolması durumunda oluşabilecek olası hasarın boyutuna bağlı olarak, aşağıdaki hususlar tanımlanmalıdır:

- Hangi sıklıkla yedek alınacağı (ör. Günlük, haftalık, aylık, vb.),
- Ne zaman yedek alınacağı (ör. Geceleri, cumartesi 02:00, vb.),
- Korunacak yedek noktası sayısı (ör. Son alınan 3 yedek),
- Yedeği alınacak verilerin kapsamı (ör. Proje dosyaları, değişiklik yapılan kurumsal dokümanlar, yapılandırma dosyaları, vb.),
- Alınan yedeklerin nerede tutulacağı (ör. Kasetler, DVD'ler, taşınabilir disk, yedekleme sistemi),
- Yedeklerin saklanacağı medyanın yeniden kullanımdan önce silinip silinmeyeceği,
- Yedekleme sorumlusu (ör. Sistem yöneticisi, kullanıcı),
- Yedekleme izleme sorumlusu (ör. Hata mesajlarının takip edilmesi, depolama ortamındaki kalan alanın izlenmesi, vb.),
- Belgeleme (ör. Tarih, yedekleme türü, yedeklenen veriler, vb.).

İstemciye fazla yük getireceği için tam yedeklemeler genellikle günde en fazla bir kez yapılabilir. Son yedeklemeden bu yana yapılan değişikliklerin kurtarılamayacağı bilinmelidir. Bu nedenle riskleri azaltmak için, tam yedeklemeler arasında düzenli veya artırımlı yedekleme noktaları oluşturulmalıdır. Veri yedeklemeyle ilgili daha kapsamlı bilgi için konuyla ilgili yazılmış özel kaynakların incelenmesi tavsiye edilmektedir.

Önemli veriler oluşturulduktan sonra artırımlı yedekler veya fark yedekleri daha sık alınabilir. Böylece, tam yedeklemeden sonra yapılan değişiklikler ve bu aradaki oluşturulan hassas veriler de korunmuş olur.

Yüklenen uygulamaların yedeklemeye dâhil edilip edilmeyeceğine karar verilmelidir. Buna karar vermek için; uygulamaların tekrar yüklenmesi, güncellemelerin ve yamaların uygulanması için gerekli süre ve operasyonel maliyet göz önünde bulundurulabilir.

Yedeklenen verilere dair; problemsiz bir şekilde yedekten dönüşün yapılıp yapılamadığı, yedekten dönüş sonrası sistemin beklenen şekilde çalışıp çalışmadığı, düzenli aralıklarla kontrol edilmelidir.

Kullanıcılar, yedekleme politikaları ve kuralları hakkında bilgilendirilmelidir. Bilgilendirme sayesinde kullanıcılar; hangi verilerin yedeklendiği, hangilerinin yedeklenmediği, ne sıklıkla yedek alındığı, en son kaç noktaya kadar yedeklerin saklandığı konularında bilgi sahibi olurlar.

Ağa bağlı istemcilerde eğer sadece ağ üzerinden paylaşılan veriler yedekleniyorsa, istemcinin yerel diskinde depolanan verilerin otomatik olarak ağ paylaşımına aktarımı takip edilmelidir. Verilerin her zaman ağda bulunan depolama alanlarına kaydedilmesi önerilir. BT sistemlerinde veya ağda büyük çapta bir değişiklik yapılırsa, yedekleme sistemi ve süreci bu değişikliğe göre güncellenmelidir.

Gizli veriler, mümkün oldukça yedeklenmeden önce şifrelenmelidir. Ancak, şifrelenerek saklanan yedeklerin parolalarının uzun süre sonunda dahi korunacağı garanti altına alınmalıdır.

BTS.2.U5 Ekran kilidi [kullanıcı]

Ekran kilidi, ekranda o an açık olan bilgileri gizleme ve bilgisayarı yetkisiz erişime karşı korumak için kullanılır. Bu sebeple bir ekran kilidi, örneğin parola ile korunarak sadece başarılı bir kullanıcı kimlik doğrulaması ile açılabilmelidir.

Ekran kilidi, kullanıcı tarafından manuel olarak etkinleştirilebileceği gibi, istemcide belirli bir süre işlem yapılmadığında otomatik olarak da devreye girmelidir. Tüm kullanıcılar, istemcilerinin başından ayrıldıklarında ekranı kilitli tutmaları gerektiği konusunda bilgilendirilmelidir. İstemci uzun süre kullanılmayacaksa kullanıcı oturumu kapatılmalıdır.

Ekran kilidinin otomatik olarak devreye girmesi için ayarlanacak süre, analiz edilerek belirlenmelidir. Bu süre, ne kullanıcının çalışmasını engelleyecek kadar kısa olmalı ne de istemcilerin kötü niyetli kişiler tarafından istismar edilebilmesine müsaade edecek kadar uzun tutulmalıdır. BT sistemlerinin sistem özelindeki güvenlik gereksinimlerine göre bekleme süresi değiştirilebilir.

BTS.2.U6 Zararlı yazılımlardan koruma programlarının kullanımı

Zararlı yazılımlara karşı korunmak için farklı yöntemler kullanılabilir. Bilinen tüm zararlı yazılımları BT sistemlerinde tarayabilen programların, zararlı yazılımlara karşı sistemi koruyan potansiyel bir araç olduğu geçmişteki tecrübelerle kanıtlanmıştır. Bu nedenle, güvenlik gereksinimleri de dikkate alınarak zararlı yazılımlardan korunma programlarının kullanımı önerilmektedir.

Tüm dosyaların periyodik olarak taranması

Zararlı yazılımlardan korunma programları, kötü amaçlı yazılımları dosyalara her erişildiğinde denetlese bile, istemciler ve dosya sunucularındaki tüm dosyaların, belli aralıklarla otomatik olarak taratılması tavsiye edilmektedir. Böylece, kötü amaçlı yazılımların tespit edilmesinde proaktif bir yol izlenmiş olacaktır. Kötü amaçlı bir yazılım tespit edildiğinde; hassas verilerin daha önce sızdırılıp sızdırılmadığı, diğer güvenlik ayarlarının ve koruma işlevlerinin gizlice devre dışı bırakılıp bırakılmadığı gibi durumlar kontrol edilmelidir.

BT sistemlerinde performans kaybı yaşanmaması için tam tarama işleminin, sistemlerin yoğun bir şekilde kullanılmadığı zaman aralığında yapılması tavsiye edilmektedir. Yazılımın kullanıcı etkinliği takip edilerek, tarama işleminin sistem kullanımının en aza indiği aralarda devreye girmesi en ideal yöntemdir. İstemcilerde bu işlem, ekran koruyucuların devreye girmesiyle eşleştirilebilir. Ancak bazı kullanıcıların örneğin yazılım derleme gibi uzun soluklu işlemleri çalıştırdıktan sonra istemcilerinin başından ayrılabilecekleri ve ekran koruyucuların bu sebeple devreye girebileceği göz önünde bulundurulmalıdır. İstemci kaynakları yoğun olarak kullanılıyor olsa dahi periyodik taramaların yapılması tavsiye edilir.

Veri alışverişi ve veri iletimi

Ortamlar arasında veri aktarımı yapılmadan hemen önce, aktarılacak veriler kötü amaçlı yazılımlara karşı kontrol edilmelidir. Benzer şekilde, başka kaynaktan alınan veriler, transfer sonrası hemen taranmalıdır. Bu kontroller, hem veri kaynaklarına ilk erişimde hem de ağ üzerinden veri aktarılırken yapılmalıdır. Taramalar mümkün olduğunca otomatikleştirilmelidir.

Şifrelenmiş veya sıkıştırılmış dosyalarda zararlı yazılımların tespit edilmesi

Şifreleme teknikleri kullanılırken, zararlı yazılımlardan korunma programları üzerindeki potansiyel etkisi dikkate alınmalıdır. Veriler şifrelenirse, sistem bileşenleri veya uygulamaları uygun anahtar olmadıkça bu verilere erişemez. Bu durum, zararlı yazılımlardan korunma programının kullanıcı bağlamında çalıştırılması veya kötü amaçlı

yazılım için şifrelenmiş bir dosyayı kontrol etmek için uygun şifreleme anahtarının kullanıcı tarafından girilmesi anlamına gelir. Zararlı yazılımlardan koruma programının çalıştığı kullanıcı kimliğine şifreleme anahtarı girildiğinde; bu durumun daha farklı güvenlik riskleri ortaya çıkarabileceği unutulmamalıdır. Bu nedenle, şifreleme anahtarının başka bir sistemle paylaşmadığına emin olunan yerleşik bir zararlı yazılımlardan koruma programının kullanılması önerilir.

Zararlı yazılımlardan korunma programları; popüler sıkıştırma teknikleriyle sıkıştırılmış dosyaları, arşivlenmiş dosyaları ve iç içe arşivlenmiş dosyaları da tarayabilmelidir.

Yetkisiz değişiklik veya devre dışı bırakmaya karşı koruma

Kullanıcılar, istemcilerinde kurulu olan zararlı yazılımlardan korunma programlarının ayarlarında herhangi bir değişiklik yapamayacak şekilde kısıtlanmalıdır. Kullanıcıların özellikle, zararlı yazılımlardan korunma programlarını devre dışı bırakabilmeleri engellenmelidir.

BTS.2.U7 Loglama

İstemcilerde log tutma özellikleri makul bir seviyede etkinleştirilmelidir. İstemciden toplanan log kayıtları düzenli olarak kontrol edilmelidir. Güvenlikle ilgili tüm olaylar loglara kaydedilmelidir. Aşağıdaki olayların log olarak tutulması önerilir;

- Kullanıcı hesabının kilitlenmesine neden olacak sayıda hatalı parola denemeleri,
- Yetkisiz erişim girişimleri,
- Ağ kapasitesinin yüksek kullanımına neden olabilecek girişimler.

İstemcinin koruma gereksinimlerine bağlı olarak, kaydedilecek olay türleri değişkenlik gösterebilir. Koruma gereksinimi ne kadar yüksek olursa, kaydedilecek parametreler o kadar artacaktır.

Log dosyalarında kaydedilen veriler zamanla artacağı için logları değerlendirme aralıkları, anlamlı sonuçlar çıkartılabilecek şekilde kısa tutulmalıdır. Log dosyalarında yapılacak çalışmalarda anlamlı sonuçlar çıkarabilmek ve doğru tespitler yapılabilmek için; kullanıcı kimliği, işlem numarası, istemci kimliği, tarih ve zaman gibi bilgiler log dosyalarına kaydedilmelidir.

Log dosyalarının saklama süresi belirlenirken; yasalar, mevzuatlar ve sözleşmeler dikkate alınmalıdır. Log dosyalarının saklanması amacıyla asgari sürenin belirlenmesi gerekecektir. Bunun yanı sıra kayıtlarda yer alan verilerin mahremiyeti ve gizliliği göz önünde bulundurularak, kayıtların ne şekilde ve ne zamana kadar saklanacağını da belirlemek gerekebilir. Kayıtların saklanması için belirlenen azami sürenin sonunda log dosyalarının silinmesi için de bir mevzuat ya da yasal zorunluluk olabileceği bilinmelidir.

Özellikle çok sayıda istemcinin olduğu durumlarda, log kayıtları merkezi olarak birleştirilmeli ve merkezi olarak değerlendirilmelidir.

BTS.2.U8 Önyükleme işleminin korunması

Çıkarılabilir medyadan önyükleme yaparken veya üçüncü taraf yazılımı yüklerken, yalnızca güvenlik ayarları atlanmakla kalmaz, aynı zamanda istemciye zararlı yazılımlar da bulaşabilir. Ayrıca, zararlı yazılımlar önyükleme işlemine müdahale de edebilir. Bu durumun önüne geçmek için, uygun idari önlemlere ve teknik güvenlik önlemlerine ihtiyaç duyulur. Bu amaçla, aşağıdaki hususlar dikkate alınmalıdır:

- Sürücülerin çıkarılması,
- Sürücülerin fiziksel olarak kullanıma kapatılması,
- Sürücülerin, BIOS veya işletim sistemi ayarlarıyla devre dışı bırakılması,
- Ara yüz kullanım kontrolü yapılması,
- Şifreleme (şifreli veri taşıyıcılarına özel erişim),
- Kullanım talimatları.

Kurumun hangi yaklaşımı tercih ettiğine bakılmaksızın, taşınabilir bir ortamdan gelen içeriğin istemciye bağlandığında otomatik olarak yürütülmesini önlemek önemlidir. Bunu yapmak için, işletim sisteminin ilgili otomatik çalıştırma ve otomatik oynatma işlevleri devre dışı bırakılmalıdır.

Önyükleme işlemini şifreli olarak güvence altına almak için UEFI arayüzüne sahip sistemlerde SecureBoot seçeneği etkinleştirilmeli ve anahtar veritabanları kurumun gereksinimlerine göre yapılandırılmalıdır. En azından hangi anahtarların güvenilir olduğu kontrol edilmeli ve belgelenmelidir. Bu yapılandırma ayarları yetkisiz kişiler tarafından kapatılamayacak şekilde ayarlanmalıdır. Aygıt yazılımının yapılandırma arayüzüne erişim en azından parola korumalı olmalıdır.

Güvenlik önlemlerinin kullanıcı tarafından kabul görmesi için, kullanıcılar konunun hassasiyeti ve oluşabilecek zararlar hakkında bilgilendirilmelidir.

2.2 2. SEVİYE UYGULAMALAR

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

BTS.2.U9 İstemciler için bir güvenlik politikası oluşturulması

İstemciler için güvenlik gereksinimleri, kurumun güvenlik politikasının bir sonucu olarak ortaya çıkar. Bu sebeple, kurumun güvenlik politikası temel alınarak, istemciler için

güvenlik gereksinimleri belirlenmelidir. Bu bağlamda, kurum çapında uygulanan genel güvenlik politikasına ek olarak parola belirleme ve güvenli internet kullanım kılavuzu gibi daha özel BT kılavuzlarına gerek olup olmadığı değerlendirilmelidir.

Güvenlik politikası; istemcilerin tedarik edilmesinden hizmet dışı bırakılmasına kadar geçen yaşam döngüsünde görev alan çalışanlar ve istemciyi kullanan kullanıcılar tarafından bilinmeli ve uygulanmalıdır. Politikanın, içeriği ve uygulaması düzenli olarak gözden geçirilmelidir.

Güvenlik politikası, elde edilmesi planlanan güvenlik hedeflerini ve temel tanımları içermelidir. Anlaşılabilirliği artırmak için, farklı uygulama alanlarına yönelik farklı güvenlik kılavuzlarının hazırlanması faydalı olabilir.

Hazırlanacak kılavuzda öncelikle, genel yapılandırma ve yönetim stratejisi üzerinde durulmalıdır. Bu bağlamda, güvenlik önlemleri ele alınırken daha özgürlükçü mü yoksa daha kısıtlayıcı bir yaklaşıma mı sahip olunacağı en başta belirlenmelidir. Bundan sonra alınacak diğer kararlar, bu stratejiyi temel alacaktır.

Normal koruma gereksinimi olan istemciler için, nispeten daha özgür bir strateji seçilebilir. Bu tercih, çoğu durumda yapılandırmayı ve yönetimi basitleştirir. Aslında stratejiyi sadece "gerektiği kadar özgür" olarak belirlemek tavsiye edilmektedir.

Yüksek koruma gereksinimi olan istemciler için genellikle kısıtlayıcı bir strateji önerilir. Bilgi güvenliğinin üç temel değerinden (Gizlilik, Bütünlük, Erişilebilirlik) herhangi biriyle ilgili daha fazla koruma gereksinimi olan istemciler için kısıtlayıcı bir yapılandırma ve yönetim stratejisi uygulanmalıdır.

Bu kapsamda dikkate alınması gereken bazı hususlar aşağıdaki gibidir;

İstemciyi kullanan kullanıcılar için düzenlemeler:

- Bir istemci aynı anda sadece tek kullanıcı tarafından mı kullanılacak yoksa birkaç farklı kullanıcı tarafından mı kullanılacak?
- İstemcilerin belirli yapılandırma ayarlarının kullanıcılar tarafından değiştirilmesine izin verilecek mi (ör. Ekran arka planı, ekran koruyucu vb.) yoksa tüm ayarlar merkezi olarak mı yönetilecek?
- Kullanıcıların, istemcilerin belirli alanlarına erişmesine izin verilecek mi? Bu özellik istemcinin kurulumu ve temel yapılandırmasını etkileyeceği gibi istemcinin kendisine hakların atanmasını da etkileyecektir.
- Kullanıcılar istemcilerde yerel olarak hangi verileri depolayabilecekler? Genel olarak, kurumsal tüm bilgiler, düzenli olarak yedeği alınan bir sunucuda merkezi olarak

depolanmalıdır. Aksi halde, istemcide yerel olarak depolanan bilgilerin korunması, yedekleme işlemlerinde ayrıca değerlendirilmelidir.

- Kullanıcılar istemcileri akşam kapatacak mı yoksa çalışır halde mi bırakacaklar? Yangına karşı güvenlik tedbirleri ve enerji tasarrufu gerekçesiyle istemcilerin kapatılması yönünde kullanıcıların bilgilendirilmesi gerekir. Ayrıca istemcilerde kullanılan sabit diskler genellikle sürekli çalışmaya uygun olmayabilir. Buna rağmen otomatik yedeklemeler, güncellemeler, anti-virüs taramaları gece çalışabileceği için istemcilerin sürekli açık kalması da gerekebilir.

BT ekibinin ve denetçilerinin çalışmaları için düzenlemeler:

- Yöneticilere hangi düzenlemelere göre haklar verilecek? Hangi yöneticinin hangi yetkilere sahip olmasına izin verilecek ve bu yetkiler nasıl belirlenecek?
- Yöneticilerin ve denetçilerin hangi yolla istemcilere erişimlerine izin verilecek?
- Hangi süreçler ve olaylar belgelenecek? Belgeler hangi biçimde oluşturulacak ve korunacak?
- Belli değişikliklerin gerçekleştirilmesinde birden fazla sistem yöneticisinin aynı anda rol alması ilkesi uygulanacak mı?

Kurulum ve temel konfigürasyon için özellikler:

- Kurulum için hangi kurulum medyaları kullanılacak?
- Merkezi kimlik doğrulama ve kullanıcı yönetimi mi yapılacak; yoksa sadece yerel kimlik doğrulama mı kullanılacak?

Kullanıcı, rol yönetimi ve yetkilendirme yapısı:

Yönetim için bir rol model geliştirilmelidir. Farklı kullanıcılar tarafından aynı kullanıcı hesabı kullanılmamalıdır.

- Eğer istemcide dosya sistemi bölümlerinin şifrelenmesine karar verildi ise, bunun nasıl yapılması gerektiği belirlenmelidir (ayrıca bkz. *"BTS.2.U28 İstemcilerin şifrelenmesi"*).
- Şifrelenmiş dosya yapısı kullanıldığında, bunun için ayrı bir politika oluşturulmalıdır. Yapılandırma ayarları detaylı bir şekilde belgelenmelidir aksi takdirde bir problem yaşanması durumunda şifrelenmiş veriler tamamen kaybedilebilir.
- Doküman oluşturma ve güncellenmesine yönelik kurallar belirlenmelidir.

Güvenli işletim için gereksinimler:

- Hangi kullanıcı grubunun istemcide oturum açmasına izin verilecek?

- İstemciye erişmek isteyen kullanıcılar nasıl doğrulanacak? Aktif bir kimlik doğrulama olmaksızın, kullanıcıların istemcilerde otomatik oturum açması engellenmelidir.
- Kullanıcılar bir veya daha fazla yerel ağa veya internete erişebiliyor mu? Hangi protokoller kullanılacak? İstemciler kurumda bir iş istasyonu olarak kullanılıyorsa genelde normal bir kullanıcının yerel ağ üzerinden başka bir iş istasyonuna erişimi istenmez.
- İstemciler, hangi kaynaklara erişebilecek?
- Parola kullanımıyla ilgili gereksinimler nelerdir?.
- İstemci önyüklemesi kötü amaçlı saldırılara karşı nasıl korunacak? Yalnızca yetkili sistem yöneticileri sürücülerden veya harici depolama ortamlarından önyükleme yapabilmelidir. Bu nedenle istemcilerde, CD-ROM, DVD veya USB depolama aracı gibi harici ortamlardan önyükleme yapılmasını engelleyen bir önyükleme kilidi kullanılmalıdır (bkz. *"BTS.2.U12 Yazılımın uyumluluk kontrolü"*). Sorun giderme esnasında kullanılabilmesi için, kilidi çözme yetkisi sadece ilgili BT ekiplerinde olmalıdır.
- BT sistemi önyükleme işlemi şifrelenecek mi (ör. Örneğin UEFI Secure Boot)?

Ağ iletişimi ve hizmetleri:

- İstemcilere yerel bir güvenlik duvarı kurulmalı mı?
- İstemciden hangi dış ağ servislerine erişilebilmelidir?
- Kullanıcı verileri şifrelenmeden transfer edilecek mi? Bu durum sadece yerel ağ için bir istisna olarak yapılmalıdır. Eğer veriler güvenli olmayan bir ağ üzerinden aktarılacaksa veri transferi başka önlemler alınarak güvenli hale getirilmelidir (Ör. vpn kullanımı veya tünelleme).

Log tutma:

- Hangi bilgiler log olarak kaydedilecek? Log kayıtları nasıl ve hangi aralıklarla değerlendirilecek? Değerlendirmeyi kim yapacak?

Yukarıda verilen bilgilere dayanarak, denetimlerde veya gözden geçirmelerde yardımcı olabilecek bir kontrol listesi oluşturulabilir.

Güvenlik politikasının sorumluluğu, bilgi güvenliği yönetimine aittir. Politikada yapılacak değişiklikler bilgi güvenliği yönetimiyle koordineli olarak gerçekleştirilmelidir.

Bir güvenlik politikası oluşturulurken, ilk olarak BT sistemlerinin güvenliği için maksimum gereksinim ve en olumsuz şartlar belirlenmelidir. Bunlar daha sonra gerçek koşullara uyarlanabilir. Bu şekilde hareket edilmesi, gerekli tüm hususların dikkate alınmasını

sağlayacaktır. İkinci adım olarak, oluşan her güvenlik zafiyeti ve zayıflık için, hesaba katılmayan durumlar gerekçeleri ile birlikte belgelenmelidir.

Kullanıcılar için yapılan düzenlemeler, günlük çalışmalara ne kadar uygulanabilir olursa o kadar verimli olacaktır. Bu düzenlemelerin kullanıcılar için nasıl zorunlu kılınacağı ve nasıl takip edileceği belirlenmelidir. Örneğin, sadece güvenlik politikasında yasaklayarak, kullanıcıların belirli dizinlere erişmesini kısıtlamak yeterli olmaz. Bu durum ancak, kullanıcılara uygun erişim hakları tanımlayarak sağlanabilir. Bu nedenle güvenlik politikasında tanımlanan erişim hakları, kurulum ve yapılandırma ayarlarının izin verdiği düzeyde uygulanabilir olmaktadır.

İstemciler için bir güvenlik politikasının oluşturulması önemlidir ancak alınan güvenlik önlemleri ile kullanım kolaylığı arasında bir denge kurmak gerekir. Kullanıcılar, içeriği ve sınırları net olmayan, aşırı sayılabilecek düzenlemelerle kısıtlanırlarsa, güvenlik için yapılan bu düzenlemeleri ve sınırlandırmaları atlatmaya çalışacaklardır.

BTS.2.U10 İstemci işletiminin planlanması

İstemcilerin güvenli bir şekilde işletilebilmesi için en temel gereksinim, kapsamlı bir planlamanın yapılmasıdır. İstemcilerin güvenli kullanımı için yukarıdan aşağıya planlama prensibiyle kapsamlı bir planlama yapılmalıdır. Tüm sistemleri içine alan genel bir konsept temel alınarak daha alt bileşenler ve özel konuları ele alan somut ve sağlam güvenlik planları tanımlanmalıdır. Planlama, yalnızca güvenlik yaklaşımı ile değil aynı zamanda günlük işlemlere dair süreçleri de ele almalıdır.

Genel konsepte örnek olarak aşağıdaki konular ele alınmalıdır;

- İstemciler hangi görevleri yerine getirmeli? İstemciler ile hangi hizmetlere erişilebilmelidir? İstemcilerin kullanılabilirliği, verilerin gizliliği veya bütünlüğü için özel şartlar var mıdır?
- İstemcilerde hangi donanım bileşenleri kullanılmalı? Bu durum, işletim sisteminin seçimi için önemli olabilir.
- Donanım için temel gereksinimler ne olmalıdır (CPU, RAM, sabit disklerin kapasitesi, ağ kapasitesi, vb.)?
- İstemciler yalnızca kendileri gibi benzer görevleri yapan sistemlerin bulunduğu bir ağı mı yoksa farklı görevleri yapan farklı sistemlerin bulunduğu bir ağı mı kullanacaklar?
- İstemciler mevcut bir sistemin yerini aldıklarında eski sistemdeki veriler yeni istemciye aktarılacak mı?
- İstemcilerde çoklu önyükleme seçeneği aktif edilerek, çoklu işletim sistemi kurulumuna izin verilecek mi?

İyi bir planlamanın temeli olarak istemciler için bir veya daha fazla gereksinim profili oluşturulması önerilir (ör. "Genel Ofis PC", "Geliştirici Bilgisayarı" veya "Yönetici Bilgisayarı" gibi).

Aşağıdaki alt başlıklar detaylı planlama esnasında dikkate alınmalıdır:

- Kimlik doğrulama ve kullanıcı yönetimi: Ne tür kullanıcı yönetimi ve kullanıcı kimlik doğrulama yöntemi kullanılmalıdır? İstemciler sadece yerel olarak mı yoksa merkezi olarak mı yönetilecek? İstemciler merkezi bir kimlik doğrulama hizmetinden mi faydalanacak yoksa sadece yerel bir kimlik doğrulama mı kullanacak?
- Kullanıcı ve grup kavramı: Kurum çapında belirlenen kullanıcı, yetki ve rolleri temel alınarak, kullanıcılar için uygun kurallar oluşturulmalıdır.
- Yönetim: İstemciler nasıl yönetilmelidir? Tüm ayarlar ve yönetim yerel olarak mı yoksa merkezi olarak mı yapılacak?
- Disk bölümleme ve dosya sistemi düzeni: Planlama aşamasında, gerekli sabit disk alanı boyutunun ilk tahmini yapılmalıdır. Yönetim ve bakım kolaylığı için, işletim sistemi (sistem programları ve yapılandırma), uygulama programları, uygulamaya ilişkin verilerin ve kullanıcı verilerinin disk üzerinde barındırılacakları alanların ayrılması önerilir. Bu amaçla, farklı işletim sistemleri farklı mekanizmalar sunar (Windows ve Linux dosya sisteminin farklı olması gibi). Çoğu zaman sabit diskte kayıtlı olsa dahi bazı verileri farklı bir yerde saklamak faydalı olabilir. Bu durum genellikle yeni bir kurulumda veya istemcinin güncellenmesi gibi durumlarda gerekli olabilir. Planlama aşamasında, barındırma alanları için planlanan bölümlemeler ve büyüklükleri belgelenmelidir.
- İstemcilerde gizli veriler tutulacak ise şifrelenmiş dosya sistemlerinin kullanılması kesinlikle önerilir (ayrıca bkz. *"BTS.2.U28 İstemcilerin şifrelenmesi"*). Tüm dosya sistemlerinin şifrelenmesi gerekmeyebilir bunun yerine verilerin saklanacağı belirli alanların, örneğin verilerin önbelleğe alınabileceği kısımların şifrelenmesi genellikle yeterli olacaktır. Şifreleme için kullanılan anahtarlar gibi güvenlik parametreleri düz metin formatında kaydedilerek saklanmamalıdır. Böyle bir durum güvenlik seviyesini düşürür. Uygun bir disk bölümleme ve dosya sistemi planı hazırlanarak bu önlemlerin alınması kolaylaştırılabilir.
- İstemcilerde saklanan verilerin gizliliği için daha yüksek güvenlik gereksinimine ihtiyaç duyulduğunda, istemcinin tüm sabit diskini şifreleyen ve işletim sistemini başlatmadan önce kimlik doğrulaması yapan bir şifreleme programının kullanılması gerekebilir.
- Ağ hizmetleri ve ağ bağlantısı: İstemciler tarafından erişilmesi gereken verilerin güvenlik gereksinimlerine bağlı olarak, bir ağ erişim planı oluşturulmalıdır.

- İstemciler, kullanım amacına bağlı olarak, ağdaki farklı hizmetlere erişim ihtiyacı duyabilirler. Bu durum, planlama esnasında göz önünde bulundurulmalıdır. Böylece, gelecekte oluşabilecek yetersiz ağ kapasitesi veya hizmetlere ağ üzerinden ulaşamama gibi sorunların en başta önüne geçilmiş olur.
- İzleme: İstemcilerin erişilebilirliğiyle ilgili özel gereksinimlere ihtiyaç varsa, istemcileri izlemek için bir izleme aracı kullanılmalıdır. Bunu yapmak için, merkezi bir sunucu üzerine bir izleme aracı yüklenir, istemcilerde yerel olarak yüklenen bir ajan ise, sistem yükü, işlemci, bellek kullanımı, âtıl kapasite gibi izlenmesi gereken parametreleri takip eder ve belirlenen bilgileri sunucuya gönderir. Sorun yaşandığı durumlarda da otomatik olarak bir alarm üretilebilir (ayrıca bkz. *"BTS.2.U29 Sistem izleme"*).
- Log tutma: Loglar, arızaların veya saldırıların teşhis edilmesinde önemli rol oynar. Log tutma planlanırken asgari olarak hangi bilgilerin kaydedilmesi gerektiğine ve log kayıtlarının ne kadar süre ile saklanacağına karar verilmelidir. Ayrıca, log kayıtlarının yerel olarak istemci üzerinde mi yoksa ağdaki merkezi bir sunucuda mı saklanacağı belirlenmelidir.
- Log kayıtlarının nasıl ve ne zaman değerlendirilmesi gerektiği de planlama aşamasında belirlenmelidir.
- Yüksek Erişilebilirlik: İstemcilerin erişilebilirliğine yönelik özel gereksinimlere ihtiyaç varsa, planlama aşamasında bu gereksinimlerin nasıl karşılanacağı planlanmalıdır.

Daha sonraki bir zamanda ihtiyaç duyulması halinde incelenebilmesi için, planlama aşamasında alınan tüm kararlar belgelenmelidir. Belgeler farklı kişiler tarafından erişilebileceği için açık ve net olmalıdır.

BTS.2.U11 İstemcilerin tedarik edilmesi

İstemcilerin tedarik sürecinde, tedarik sırasında genellikle yüksek sayıda istemcinin tedarikinin gerçekleştiği düşünülecek olursa, uygulama senaryoları göz önünde tutularak, uygun ürünlerin seçimine yönelik gereksinimler belirlenmelidir. Tedarik edilecek yeni istemcilerin, mevcut kullanılan BT alt yapısına uyumlu olması önemlidir. Bu sayede, istemcilerin entegrasyonu, yönetimi ve işletimi gibi operasyonlar için oluşacak ek maliyetlerin önüne geçilebilir.

BTS.2.U12 Yazılımın uyumluluk kontrolü

Herhangi bir yazılım tedarikinden önce, yazılımın mevcut istemcilerle uyumlu olup olmadığı kontrol edilmelidir. Uyumluluk kontrolü, yazılımın istemcilere yüklenmesinden önce uygulanacak prosedürlere dâhil edilmelidir. Yazılımın üreticisi veya bilgi

alınabilecek uzman gruplar, yazılımın uyumluluğu hakkında güvenilir bilgi sağlamazsa, uyumluluk kontrolü bir test ortamında gerçekleştirilecek testlerle yapılmalıdır. Bir donanım değişikliği veya işletim sistemi göçü planlanıyorsa, değişiklikten etkilenen tüm donanımlar için sürücü yazılımlarının sağlanabiliyor olduğu garanti altına alınmalıdır.

BTS.2.U13 Kod çalıştırılabilen ortamlara erişim

Kötü amaçlı yazılımların tanımlama ve yok edilmesiyle uğraşmak yerine, kodlar ve veriler için özel bellek alanı oluşturarak koruma sağlayan Intel SGX gibi çözümlerin kullanılması tavsiye edilir. Bu ayar genellikle istemcilerin UEFI arayüzünde güvenlik bölümünde yer alır.

Bazı durumlarda, yürütme ortamlarında istenmeyen kodların çalıştırılmasının devre dışı bırakılamayacağı dikkate alınmalıdır. Bu gibi durumlarda güvenlik, mevcut güvenlik açıklarının hızlı bir şekilde kapatılmasıyla sağlanmalı ve kod çalıştırılabilen ortama tam erişim sadece BT yönetimi ve ilgili üreticilerle sınırlandırılmalıdır.

BTS.2.U14 Güncellemeler ve yamalar

BT sistemlerindeki yazılım hataları ve güvenlik açıkları, kurumun bilgi ağı ve BT alt yapısı için bir risk oluşturur. Bu durum; donanımları, ürün yazılımlarını, işletim sistemlerini ve uygulamaları olumsuz etkiler. Güvenlik açıkları mümkün olduğunca hızlı giderilmelidir. Böylece, saldırganların bu açıkları kullanarak istemcilere yetkisiz erişim sağlamalarının önüne geçilir. Bu durum, söz konusu BT sistemlerinin özellikle internet erişimlerinin olduğu hallerde önem kazanır. İşletim sistemi veya yazılım üreticileri genellikle periyodik olarak güvenlik açıklarını düzeltmek için gerekli güvenlik yamalarını ve güncellemeleri yayınlarlar. Sistem yöneticileri yayınlanan güvenlik güncellemeleri ile ilgili kendilerini sürekli güncel tutmalıdırlar.

Yamaların ve güncellemelerin güvenilir kaynaklardan elde edilmesi önemlidir. Kullanılan her bir BT ürünü veya yazılım için güvenlik güncellemelerin ve yamaların hangi kaynaktan yayınlandığı bilinmelidir. Güncellemeyi veya yamayı uygulamadan önce hem mevcutta yüklü olan hem de yüklenecek olan güncellemelerin bütünlük ve doğruluk kontrolleri yapılmalıdır. Ayrıca, zararlı yazılımlardan korunma programları kullanılarak söz konusu bileşenlerin kötü amaçlı yazılımlara karşı taranması önerilir. Tarama işlemi, bütünlüğü ve gerçekliği doğrulanmış olan bileşenler için de uygulanmalıdır.

Güvenlik güncellemeleri veya yamalar hızlı bir şekilde uygulanmalı ancak uygulanmadan önce test edilmelidir. İstemciler üzerinde yer alan diğer kritik bileşenlerle veya programlarla bir çakışma yaşanması durumunda, BT sistemi çalışamaz hale gelebilir. Gerekirse ilgili BT sistemi, testler tamamlanana kadar farklı önlemlerle korunmalıdır.

Bir güncelleme veya yama yüklenmeden önce veriler, başka bir BT sistemine yedeklenmelidir. Böylece, bir sorun yaşanması durumunda geri yükleme yapılabilir. Zaman kısıtı veya uygun test ortamı olmaması nedeniyle test yapılmadan yüklenen güncellemeler için yedekleme işlemi, ayrıca önem kazanır.

Her türlü durumda güncellemelerin; kim tarafından, ne zaman ve hangi sebeple yapıldığı kayıt altına alınmalıdır. Böylece, güvenlik açıkları yayınlandığında, bu kayıtlar aracılığıyla istemcilerin mevcut yama düzeylerini kontrol ederek, BT sistemlerinin risk altında olup olmadığı hızlı bir şekilde tespit edilebilir.

Bir güvenlik güncellemesinin veya yamanın başka bir önemli bileşenle veya programla uyumsuz olduğu ve sorunlara neden olduğu belirlenirse sürece nasıl devam edileceği hususu önceden planlanmalıdır. Karşılaşılan sorunlardan dolayı bir yamanın kurulmayacağına karar verilirse, bu karar mutlaka kayıt altına alınmalıdır. Bu durumda, açıklığın zafiyete dönüşmesini önlemek için hangi önlemlerin alındığı açıkça belirtilmelidir.

Güvenilir yükleme medyasının kullanımı

Dikkatsiz bir şekilde, "güvensiz" kaynaklardan yüklenen programları çalıştırmak büyük zararlara neden olabilir. Kötü niyetli yazılımlar bir istemcide önemli verileri ve şifreleri, truva atı veya arka kapı casusluk yöntemlerini kullanarak ele geçirebilir veya önemli verilere zarar verebilir ya da bu verileri tamamen silebilir.

Bu tür kötü amaçlı yazılımlar, genel olarak ekran koruyucular, virüsten koruma yazılımları veya diğer yardımcı programlar gibi yazılımların içine gizlenebilir. Ayrıca bu zararlı yazılımlar, sahte gönderen adreslerini kullanarak e-posta ile çok sayıda istemciye yayılabilir. Dikkatsiz kullanıcılar, çoğu zaman bu tür uygulamaları internet üzerinde yer alan güvenli olmayan kaynaklardan indirip kontrol etmeden istemcilerine kurabilirler.

Prensip olarak, yazılımlar özellikle iyi bilinen kaynaklardan kurulmalıdır. Kurulum dosyaları, yerel bir veri saklama ortamından değil de internetten indirilmişse bu duruma özellikle dikkat edilmelidir. Günümüzde güncellemeler veya yamalar için artık taşınabilir medyalar ile (disk, usb bellek vb.) dağıtımı yapılmamakta olduğu için, söz konusu durum daha sık yaşanabilmektedir. Çoğu üretici veya dağıtıcı, indirilen bir paketin bütünlüğünün kontrol edilmesini sağlayan kontrol anahtarları sağlamaktadır. Kontrol anahtarları (ör. sağlama toplamı), genellikle üreticinin web sayfalarında yayınlanır veya imzalanmış bir e-posta ile gönderilir. İndirilen bir uygulamanın veya veri dosyasının bütünlüğünü doğrulamak için, üretici tarafından verilen sağlama toplamı değeri, ilgili program tarafından yerel olarak oluşturulan sağlama toplamı değeriyle karşılaştırılmalıdır. Bir

yazılım paketi için sağlama toplamı değeri mevcutsa, bunlar paket kurulmadan önce mutlaka kontrol edilmelidir.

Sağlama toplamı değeri ile özgünlük kontrolü yapılamaz. Bu nedenle, birçok durumda, programlar veya paketler için dijital imzalar sunulur. Buna karşılık, imzayı doğrulamak için gereken genel anahtarlar genellikle üreticinin web sayfalarında veya genel anahtar sunucularında bulunur. Çoğunlukla doğrulama anahtarları, PGP (Pretty Good Privacy) veya GnuPG programlarından biriyle üretilir.

Üreticinin dijital imza ile yayınladığı veri paketleri, sağlama toplamı ile yayınlanan veri paketlerinden daha güvenilirdir. Linux dağıtımları için yaygın olarak kullanılan paket yönetim sistemi RPM (Redhat Package Manager) veya Debian tabanlı dağıtımlar için kullanılan Apt/DPKG paket yönetim sistemi entegre bir doğrulama işlevselliği sağlamaktadır.

Bazen, ilgili işletim sisteminin veya uygulamaların yerleşik yazılım güncelleme mekanizmaları bile, şifrelenmiş bir sağlama toplamı doğrulaması gerçekleştirmeyebilir. Bu güvenlik kontrolleri yapılmadan yazılım kullanılmamalıdır. Mümkün olduğunca her bir yazılım paketi yüklenmeden önce sağlama toplamı ile doğrulama yapılmalıdır.

Ayrıca sağlama toplam değerleri, imzalar veya sertifikalar aksine üreticiler tarafından tutarlı bir şekilde sunulmadıkları için, genellikle otomatik olarak karşılaştırılamazlar. Bu nedenle, genellikle üretici sayfalarından sağlama toplamları kullanılarak veya yama ve düzeltme yazılımındaki URL'ler özelleştirerek karşılaştırılmaları gerekebilir.

Bir yazılım paketi için dijital imzalar mevcutsa, paket kurulmadan önce mutlaka kontrol edilmelidir.

Dijital imzaların kullanımı ile ilgili temel bir sorun, anahtarın kendisinin gerçekliğinin doğrulanamamasıdır. Yazılım paketinin dijital olarak imzalanması sırasında kullanılan anahtarın, bilinen, güvenilir bir otorite tarafından oluşturulmamış olması, yazılım paketinin doğruluğu konusunda tam bir garanti vermez. Bu durumda, tercihen yazılım paketinin temin edildiği kaynak harici, farklı bir kaynaktan, örneğin üreticinin sağladığı bir DVD’den, paketin indirilebileceği başka bir sunucudan veya tescilli bir otoriteden genel anahtar temin edilmelidir.

Sağlama toplamı değerlerini ve dijital imzaları kontrol etmek için gerekli programlar yerel olarak mevcut olmalıdır. Sistem yöneticileri, sağlama toplamı ve dijital imzaların anlam ve önemi hakkında bilgilendirilmelidir. Buna ek olarak, sistem yöneticileri uygun yazılımları günlük çalışmalarında kullanmaları için yeterli zamana sahip olmalı ve bu tür yazılımları kullanmaya aşinalık kazanmalıdırlar.

Yamalar ve güncellemeler, sebebi her ne olursa olsun e-posta ile gönderilmemelidir. E-posta iletilerinde gönderen adresinin doğruluğunu, ek güvenlik mekanizmaları kullanmadan belirlemek zordur. Kurumlardaki bireysel alıcı ve dağıtım gruplarının e-posta adreslerinin tahmin edilmesi genellikle kolaydır. Bu durum sahte bir göndericiden zararlı yazılım alma riskini artırır. Ayrıca, yamalar ve güncellemelerin dosya boyutları büyük olabilir. Birçok şirket ve kurum, e-posta eklerinin boyutunu sınırlamakta ve bazı durumlarda çalıştırılabilir dosyaların e-posta ekleri ile dağıtılmasını yasaklamaktadır. Ayrıca, büyük boyutlara sahip veriler e-posta sunucularında gereksiz yük oluşturmaktadır. Bu nedenle, özellikle güvenlik yamaları ve kritik güncellemelerin dağıtımı e-posta ile yapılmamalıdır.

BTS.2.U15 İstemcilerin güvenli kurulumu ve yapılandırılması

Planlamalar yapıldıktan ve bir güvenlik politikası oluşturulduktan sonra istemci kurulumuna başlanabilir.

BT sisteminin kurulumu ve yapılandırması, yalnızca yetkili kişiler (sistem yöneticileri veya sözleşmeli teknik personeller) tarafından yapılmalıdır. Sistem yöneticileri ve sözleşmeli destek personelleri özenli bir şekilde seçilmelidir. Sistem yöneticileri, kendilerine sağlanan yetkilerin sadece gerekli yönetimsel görevler için kullanılması gerektiği konusunda bilgilendirilmelidir. Yetki verilmiş teknik personelin, donanım ve yazılımların işleyişinde önemli bir rolü bulunmaktadır. insan hatası durumunda dahi BT faaliyetlerinin devamlılığının sağlanabilmesi için, yetkilendirilmiş teknik personelin, sistem yapılandırma ayarlarına, gerekli parolalara ve anahtarlara erişebilmesi gerekir.

Planlamanın işlevsellik ve güvenlik gereksinimlerine bağlı kalınarak, kısa bir kurulum talimatı oluşturulmalıdır. Kurulumun iki aşama şeklinde gerçekleştirilmesi önerilir. İlk olarak, temel bir sistem kurulumu yapılır ve yapılandırılır. Daha sonra diğer gerekli uygulamalar yüklenir. Çoğu işletim sistemi bu yaklaşımı desteklemektedir.

Tanımlanmış adımların, her istemci için mutlaka tekrar tekrar yapılması gerekmez. Aynı adımları sürekli tekrar etmek, gerek zaman alması, gerekse hata riskini artırması açısından verimsiz olabilir. Bu nedenle, bir referans sistemin kurulması önerilmektedir. Kurulum konseptinde tanımlanan adımların, bir referans sistem üzerinde büyük bir dikkatle uygulanması, gerekli yapılandırma ayarlarının kayıt altına alınması ve daha sonra ilgili işletim sistemi için daha özel bir kurulumun elde edilmesi ile referans sistem oluşturulabilir (bkz. *"BTS.2.U30 Referans sistem kurulumu"*). İşletim sisteminin tamamen yeni bir sürüm içermeyen değişikliklerinde (güncellemeler, yamalar, servis paketleri, vb.), oluşturulan bu referans sistemin tekrar kontrol edilmesi ve gerekirse değişikliklere göre yeniden uyarlanması gerekeceği dikkate alınmalıdır.

Kurulum

Kurulum ve daha sonraki yapılandırma ayarları sürecinde, en azından önemli adımlar kayıt altına alınmalıdır. Böylece, gerektiğinde bu adımlar gözden geçirilebilir. Örneğin, yapılan bütün işlemlerin takibini kolaylaştıracak bir kurulum kontrol listesi oluşturulabilir ve yapılan ayarlar not edilebilir. Böyle bir belgenin oluşturulması, bir hata analizi yapılması gerektiği durumlarda veya sonraki kurulumlarda faydalı olabilir. Teknik personelin yanı sıra, uzmanlık alanı dışındaki başka idari görevlilerin bu belgeleri incelemesi gerekebileceğinden, işlemler kayıt altına alınırken sade ve açık bir anlatım kullanılmalıdır.

Kurulum, DVD veya diğer depolama ortamlarından yapılıyorsa, yükleme ve temel yapılandırmanın çevrimdışı veya en azından güvenli bir ağda gerçekleştirilmesi önerilir. Kurulum esnasında, diğer BT sistemlerinin kurulumu yapılan istemciye erişebilmeleri engellenmelidir. Çünkü kurulum esnasında genellikle herhangi bir parola atanmaz, koruma mekanizmaları henüz aktif değildir ve istemci kurulum süresince kontrolsüz erişime açıktır. Bazı istemcilerin kurulumu esnasında ağa bağlanması gerekirse (ör. paketlerin yüklenmesi, vb.), ayrıştırılmış bir ağda bu amaçla oluşturulan bir sunucunun kullanılması önerilir.

Özellikle, işletim sisteminin yüklü sürümünün güvenilir bir kaynaktan temin edilmiş olması önemlidir. Bu durum, kurulum dosyalarının internetten indirildiği durumlarda ayrıca önem kazanmaktadır. Bunun için, paketlerin bütünlüğünü ve orijinalliğini doğrulamak üzere kullanılabilecek dijital imzaların olup olmadığı kontrol edilmelidir. Mümkünse, dijital imzaları olmayan veya en azından sağlama toplamı değerleri bulunmayan paketler kullanılmamalıdır.

Sabit disk bölümlerini oluştururken, planlama aşamasında hazırlanan konsept uygulanmalıdır. Şifrelenmiş bir dosya sistemi kullanılacaksa, veriler kopyalanmadan önce dosya sisteminin şifrelenmesi sağlanmalıdır, çünkü genellikle dosya sistemleri daha sonra şifrelenememektedir.

Log kayıtlarının tutulması otomatik olarak aktif edilmediyse, kurulum tamamlandıktan hemen sonra log tutma özelliği etkinleştirilmelidir. Log kayıtları, kurulum ve yapılandırma esnasında sorunların çıkması durumunda faydalı bilgiler sağlayabilir.

Yapılandırma

Bir işletim sisteminin üreticisi veya dağıtıcısı tarafından yapılan temel ayarlar genellikle tam bir güvenlik sağlamaz. Üreticinin kurulum için yaptığı temel ayarlar genellikle, kolay kurulum ve kolay devreye almanın yanı sıra kullanıcıların birçok özelliğe mümkün olduğu kadar kolay erişebilmesine yöneliktir. Bu sebeple istemcinin, üreticinin yaptığı ilk yapılandırma ile kullanılmaması tavsiye edilmektedir.

İlk yapılandırmalar sonrası ilk adım, temel ayarları kontrol edip gerekirse güvenlik politikalarına göre söz konusu ayarları yeniden uyarlamak olmalıdır. Temel yapılandırma ayarları, büyük ölçüde kullanılan işletim sistemine göre değişiklik göstermektedir.

Güvenli temel yapılandırmanın amaçları şunlar olmalıdır:

- İstemciler ağ üzerinden gerçekleştirilebilecek "basit" saldırılara karşı korunmalı,
- Standart kullanıcılar, yetkisi bulunmayan ve kullanıcının kullanımı için tasarlanmış olmayan hassas verilere kasıtlı veya kasıtsız olarak erişememeli,
- Standart kullanıcılar, BT sistemlerine veya başka kullanıcı verilerine dikkatsizlik ya da başka bir nedenle zarar verememeli,
- Sistem yöneticilerinin yaptığı küçük hataların etkileri olabildiğince sınırlandırılmalıdır.

Temel yapılandırmanın bir parçası olarak kontrol edilmesi ve yapılandırılması gereken ayarlar özellikle aşağıdaki gibidir:

Sistem yöneticileri için ayarlar

Sistem yöneticilerinin kullanıldığı hesapların güvenliği daha hassas bir şekilde sağlanmalıdır.

Bu ayarlar gerektiğinde kontrol edilmeli ve ayarlanmalıdır. Ayrıca, sistem yöneticilerine ait dizinlere normal kullanıcıların erişmesi engellenmelidir.

Sistem dizini ve dosya ayarları

Temel yapılandırma ayarları sayesinde, sistem dizinlerine ve sistem dosyalarına ilişkin izinlerin kurum güvenlik politikasıyla uyumluluğu sağlanmalıdır.

Kullanıcı kimlikleri ve kullanıcı dizin ayarları

Temel yapılandırmanın bir parçası olarak, kullanıcı kimlikleri ve kullanıcı dizinleri için hangi ayarların varsayılan olarak uygulanacağı kontrol edilmelidir. Ayarların güvenlik politikasına göre yapılması gerekebilir.

Ağa erişim ayarları

Temel yapılandırma kapsamında, ağa ve önemli dış BT hizmetlerine erişim için yapılan ayarlar da dikkate alınmalı ve belgelenmelidir.

- IP adresinin atanması, temel ağ ayarlarının yapılandırılması veya ağ ayarlarını otomatik olarak dağıtan bir sunucuya erişim için yapılan ayarlar gibi. Ör. Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP).
- DNS sunucusuna erişim ayarları.
- Dağıtık dosya sistemlerine, veri tabanlarına veya diğer harici servislere erişim için yapılan ayarlar.

Yerel paket filtresi ile ek koruma

Yüksek koruma gereksinimi olan istemciler; kurum genelinde çalışan güvenlik ağ geçitlerine, güvenlik duvarlarına veya ağın bölümlere ayrılmasıyla sağlanan güvenlik tedbirlerine ek olarak, istemci üzerinde kurulu yerel paket filtresi veya yerel güvenlik duvarıyla korunmalıdır.

Destek özelliklerini devre dışı bırak

Bazı işletim sistemleri ve uygulamalar, çalışma esnasında oluşan hataları, uyarıları bir rapor halinde doğrudan üreticiye gönderebilir. Bu amaçla, internet üzerinden üreticinin sunucusuna bir bağlantı kurulur. Böyle bir veri aktarımı, özellikle kullanıcılar veri aktarım sıklığı ve içeriği hakkında bilgilendirilmediği durumlarda, güvenlik için risk oluşturabilir. Genel bir kural olarak, istemcilerin dışarıdaki bir sunucuya bağlantı yapması ve bilinmeyen/istenmeyen her tür bilgi alışverişi önlenmelidir. Genellikle, kullanılan yazılımın kullanıcı sözleşmesinde, hangi verilerin üreticiyle paylaşıldığı hakkında bilgiler yer alır. Birçok uygulama bu otomatik çağrı oluşturma ve hata raporu gönderme sistemini devre dışı bırakmayı da bir seçenek olarak sunabilir. Bu durum detaylı bir şekilde incelenmelidir. Üreticiyle bağlantı kurup bilgi transferi yapmaya olanak tanıyan bu özellik, sadece gerekli durumlarda aktif edilmelidir. Eğer bu özellik devre dışı bırakılacaksa, gerekli ayarlar yapıldıktan sonra, ilgili fonksiyonunun tamamen devre dışı olup olmadığı kontrol edilmelidir. Gerekli durumlarda, yerel paket filtreleri veya merkezi güvenlik ağ geçidi (güvenlik duvarı) üretici ile bağlantı kurulmasını önlemek için de kullanılabilir. Örnek olarak, hedef adreslere veya port numaralarına doğru yapılacak bağlantılar yerel güvenlik duvarları kullanılarak reddedilebilir. Fakat tüm uygulamaların ayarlarının kontrol edilmesi iş gücü anlamında verimsiz olabilir. Bu sebeple her bir uygulamanın ayarlarının özel olarak tek tek kontrol edilmesi yerine, üretici sunucularına yapılan bağlantıları yerel güvenlik duvarından tamamen engellemek daha kullanışlı olabilir.

Gereksiz ara yüzlerin(portların) devre dışı bırakılması

İstemcilerin temel yapılandırılmasında, kullanılması muhtemel bütün ara yüzler etkin olarak ayarlanabilirler. Ancak genellikle, bu ara yüzlerin çoğu kullanılmaz. Kullanılmayan ara yüzlerden bazıları, potansiyel güvenlik riskleri oluşturabilir. Bu nedenle, söz konusu kullanılmayan ara yüzler ya tamamen kaldırılmalı ya da devre dışı bırakılmalıdır. Kullanımı kontrol edilmesi gereken ara yüzler arasında Bluetooth, WLAN, Firewire, eSATA (harici SATA HDD bağlantısı) ve Thunderbolt öncelikli olarak yer almaktadır.

Dizin Tabanlı Yürütme Denetimi

Günümüzde kullanılan işletim sistemlerinin çoğunda, uygulama çalıştırma yetkileri dizin veya disk bölümleri bazında yönetilebilmektedir. Bu özellik sayesinde, tüm dosyaların ve tüm alt dizinlerin yürütme hakları kapatılabilir. Örneğin, Windows tabanlı işletim sistemlerinde Grup Politikası aracılığıyla (“Yazılım Kısıtlama İlkeleri” kullanılarak) bu tür bir kontrol gerçekleştirilebilir. Linux sistemlerde ise, sabit disk veya istenilen kısımlar "ro" (salt okunur) veya "noexec" (çalıştırılamaz) olarak ayarlanabilir. Ayrıca, yüksek koruma gereksinimlerinde kullanılmak üzere, işletim sistemlerinde dosya bazlı yetkilerin yönetimini sağlayan araçlar da bulunmaktadır. Kullanıcılar için:

- Yazma yetkilerine sahip oldukları dizinlerde program yürütme
- Program yürütme yetkilerine sahip oldukları dizinlerde dosya yazma

Yetkileri özel olarak yapılandırılabilir. Böylelikle, kullanıcıların internetten indirdikleri veya bir USB bellek sürücüden kopyaladıkları dosyaları çalıştırmaları zorlaştırılabilir.

İzleme

İstemci üzerinde ne olup bittiğini gözlemlemek; kritik sistem olaylarında, gerektiğinde hızlı aksiyon alabilmek için bir uygulama yardımı ile sistem olayları izlenebilir. Bu amaçla, istemcinin anlık durum bilgisi genellikle olayların değerlendirildiği merkezi bir uygulamadan (servis) elde edilir. Bununla birlikte, doğru bir biçimde yapılandırılmamış bu tür izleme uygulamaları, işletim sisteminin sistem ayarlarını değiştirebilir (Ör. SNMP - Basit Ağ Yönetimi Protokolü ile). Böyle bir değişiklik gerçekleştirilmesi istenmiyorsa, bu değişikliklere fırsat verecek özellikler devre dışı bırakılmalıdır.

Bellek

İşletim sistemini ve uygulamayı olası tampon taşmalarına karşı korumak için, donanım ve CPU desteklediği müddetçe uygun hafıza koruma mekanizmaları aktifleştirilmelidir. Örneğin, Yürütülebilir Alan Koruması (ESP), programların yetkisiz bellek alanlarında çalıştırılmasını engelleyebilir.

Bütünlük veri tabanı oluşturma

Temel yapılandırma ayarları tamamlandıktan sonra, uygun bir araç kullanarak bir bütünlük veri tabanı oluşturulması önerilir. Bazı işletim sistemlerinin standart kurulumları bu tür araçları içermektedir. Bütünlük veri tabanı farklı bir BT alt yapısında saklanmalıdır. Veri tabanının depolandığı sistemin istismar edildiğine ilişkin herhangi bir şüphe oluşursa, veri tabanı önceden oluşturulmuş bir sağlama toplamı değeri ile kontrol edilebilir. Düzenli olarak yapılacak bütünlük testlerinde, bu veri tabanı istemcinin güvenliği için bir referans olacaktır.

İstemcinin temel yapılandırılması esnasında hangi ayarların gözden geçirildiği, hangi ayarların değiştirildiği, sebepleriyle birlikte kayıt altına alınmalıdır. İlgili BT sisteminde acil bir durum olması durumunda, hangi ayarların bulunduğu ve ne tür değişikliklerin yapıldığını anlamak için bu kayıtlar önem arz etmektedir. Bu sebeple kayıt tutulurken, açık ve sade bir dil kullanılmalıdır. İdeal olarak, bu kayıtlar kullanılarak bir BT sistemini yeniden kurtarmak mümkün olmalıdır.

BTS.2.U16 Gereksiz bileşenlerin ve kullanıcı hesaplarının kaldırılması

İşletim sistemlerinin standart kurulumlarında, kullanım esnasında gerek olmayacak birçok kullanıcı kimliği, uygulama, hizmet ve bileşen de kurulabilmektedir. Standart kurulum ile birlikte gelen kullanıcı kimliklerine gerçekten ihtiyaç olup olmadığı istemcinin temel yapılandırması sonrasında gözden geçirilmelidir. Gereksiz kullanıcı kimlikleri tamamen silinmeli ya da devre dışı bırakılmalıdır.

Bir işletim sisteminin standart kurulumu çoğunlukla, normalde gerekli olmayan ve bu sebeple bir güvenlik açığına neden olabilen bir dizi program ve hizmet içerebilir. Bu durum özellikle ağ hizmetlerinde ortaya çıkabilmektedir. Kurulumdan sonra, BT sistemlerinde hangi servislerin ve uygulamaların kurulduğu ve aktif olduğu kontrol edilmelidir. İhtiyaç duyulmayan hizmetler devre dışı bırakılmalı veya tamamen kaldırılmalıdır. Ayrıca kullanılmayan çalıştırma ortamları, yorumlayıcı dilleri ve derleyiciler de istemciden kaldırılmalıdır.

İşletim sisteminde çalışan servislerin kontrolü işletim sisteminin kendi kaynakları ve araçlarıyla yapılabileceği gibi, ek araçlar kullanılarak da - örneğin dışarıdan port taraması ile - yapılabilir. Her iki yöntem birlikte kullanılarak BT sistemlerinde kullanılmayan hizmetlerin tespiti daha kapsamlı olarak gerçekleştirilebilir.

BTS.2.U17 Kullanıma sunma

İstemciler kullanıma sunulmadan ve kurumun canlı ağına bağlanmadan önce, üzerinde çalışacak uygulamaların kurulumu yapılmalı ve bunlar kayıt altına alınmalıdır. İstemcinin

kullanıma sunulmadan önce gerçekleştirilen uygunluk onay sürecinde, kurulum ve yapılandırma kayıtlarının incelenmesi ve istemci işlevsellik testlerinin baz alınması tavsiye edilir. Bu kontroller, kurumda bu işi yapmakla yetkilendirilmiş bir birim tarafından yapılabilir.

Bir güvenlik güncellemesinin veya yamanın bir başka ana bileşenle veya uygulama ile uyumsuz olduğu tespit edilirse, nasıl bir yol izleneceği önceden belirlenmelidir. Oluşabilecek sorunlar nedeniyle bir yamanın kurulmaması gerektiğine karar verilirse bu karar mutlaka kayıt altına alınmalıdır. Böyle bir durumda, güvenlik güncellemeleriyle giderilmesi planlanan güvenlik açığının hangi alternatif yöntemlerle üstesinden gelineceği belirlenmelidir. Bu kararlar alınırken sadece teknik sistem yöneticileri ile değil, konuyla ilişkili idari yöneticiler ve bilgi güvenliği birimi ile birlikte çalışılmalıdır.

BTS.2.U18 İletişim bağlantılarının şifrelenmesi [kullanıcı]

Web sayfası ziyaretlerinde en sık kullanılan güvenlik yöntemi SSL/TLS (Güvenli Yuva Katmanı/Aktarım Katmanı Güvenliği) protokolüdür. SSL/TLS tüm yeni tarayıcılar tarafından desteklenmektedir. SSL/TLS bağlantıları ile aşağıdaki konular güvence altına alınır:

- Bağlantı içeriğinin şifrelenmesi,
- İletilen verilerin eksiksizliğinin ve doğruluğunun kontrol edilmesi,
- Sunucu kimliğinin kontrol edilmesi,
- İsteğe bağlı olarak, istemci kimliğinin kontrol edilmesi

SSL/TLS ile korunan bir bağlantının en başında, istemci ve sunucu arasında bir el sıkışma gerçekleşir. İstemci ve sunucu; anahtar takası, şifreleme ve bütünlük güvencesi amacı için kullanılacak şifreleme algoritmalarına karar verirler. Ayrıca istemci ve sunucu, kullanılacak SSL sürümü üzerinde anlaşırlar. Daha sonra sunucu X.509 sertifikasını istemciye gönderir. Sunucu tarafından talep edilmesi hainde, istemci de X.509 sertifikasını sunucu ile paylaşır. Asimetrik bir şifreleme yöntemi kullanılarak, simetrik bir anahtarın güvenli bir şekilde alış verişi gerçekleştirilir. Gerçek veri aktarımının şifrelenmesi için simetrik bir yöntem kullanılmaktadır çünkü bu yöntem, büyük miktarda verinin daha hızlı şifrelenmesini sağlar. Her işlem için farklı bir simetrik anahtar, oturum anahtarı olarak tayin edilir ve bağlantı şifrelenir.

Örnek olarak web sayfalarına SSL/TLS ile yapılan güvenli bağlantılar, adres çubuğundaki “https” uzantısı veya internet tarayıcısı tarafından yine adres çubuğuna yerleştirilen renkli bir uyarıyla ve kilit simgesiyle gösterilebilir.

SSL/TLS kullanımı, HTTP istemcileri ve sunucuları ile sınırlı değildir. SMTP, FTP, IMAP veya LDAP gibi protokoller de SSL/TLS kullanılarak şifrelenebilir. Ancak ilgili istemcilerin ve sunucuların bu güvenlik işlevlerini desteklemeleri gerekir.

SSL/TLS işlemi iki katmanda gerçekleşir. SSL/TLS el sıkışma protokolü üst katmanda gerçekleşir. Bu el sıkışma, istemci ve sunucunun birbirlerinin kimliğini doğrulamalarını, sonra gerçekleşecek trafik için anahtar ve şifreleme algoritmasında anlaşmalarını sağlar. Alt katman olan SSL/TLS kayıt protokolü, TCP katmanına arabirim oluşturan gerçek trafiği şifreler ve şifrelenmiş trafiğin şifresini çözer.

Sürümler

SSL/TLS protokolünün birkaç tane sürümü bulunmaktadır. Bunlar; SSL v2, SSL v3, TLS v1.0, TLS v1.1 ve TLS v1.2 dir. Bu protokolün SSL v1 sürümü hiç yayınlanmamıştır. İstemci ve sunucu arasında güvenli bir bağlantı sağlamak için kullanılan protokolün versiyonu en az TLS 1.2 olmalıdır.

TLS 1.1 yeterli düzeyde güvenlik sağlamaktadır, ancak TLS 1.2 ile karşılaştırıldığında bazı zayıf yönleri bulunur. Örnek vermek gerekirse, TLS 1.1'de yer alan IDEA (International Data Encryption Algorithm) ve DES (Data Encryption Standard)'e dayalı şifre takımları artık TLS 1.2'de mevcut değildir.

TLS 1.1 veya TLS 1.2 sürümlerinin kullanımı hızlı bir şekilde sağlanamayacaksa, TLS 1.0 sürümü geçici olarak kullanılabilir. Ancak TLS 1.0 sürümünün bazı saldırılara karşı tam koruma sağlamadığı unutulmamalıdır. Bu sebeple, TLS 1.2 sürümüne mümkün olduğunca hızlı bir şekilde geçilmelidir. SSL v2 ve SSL v3 protokol sürümlerinin kullanımı artık tercih edilmeyebilir.

Algoritmalar ve anahtar uzunlukları

SSL/TLS protokolü ile farklı anahtar uzunluklarına sahip farklı şifreleme algoritmaları kullanılabilir. İstemci ve sunucu arasında bir bağlantı oluşturulurken, kullanılacak anahtar uzunluğu ve algoritma türü üzerinde bir anlaşma sağlanır.

Kurumda uygun ürünler (tarayıcı, web sunucusu, eklenti, vb.) seçilerek ve uygun yapılandırma ayarları yapılarak, SSL/TLS korumalı bağlantıların kullandığı algoritmaların ve anahtar uzunluklarının, güncel teknoloji ve kurum güvenlik politikası gereksinimlerini sağladığından emin olunmalıdır. Ayrıca, kullanılan şifre takımları Perfect Forward Secrecy (PFS) özelliğini desteklemelidir.

Sertifikalar

Dışarıya açık ağlar üzerinden yapılan veri haberleşmesinde, iletişimi gerçekleştiren uçların kimliklerini doğrulamak zordur. Çünkü uçların isim bilgilerinin doğruluğu kesin değildir. SSL/TLS kullanımında, tarafların kimlikleri sertifikalar ile kontrol edilir. Sertifikalar, ortak anahtarın sahibine doğru bir şekilde atanmasını sağladığı gibi ortak anahtar bilgilerini de içerir. Sertifikanın doğruluğu onay otoritesinin genel anahtarı ile kontrol edilir.

Yaygın olarak kullanılan işletim sistemleri ve uygulamalar (ör. web tarayıcıları), kurulum sırasında bazı sertifika otoritelerinin (CA: Certification Authority) SSL / TLS sertifikalarını yüklerler. Bu sertifika otoriteleri, çok farklı güvenlik politikalarına ve sertifika yayınlama koşullarına sahiptirler. Bu nedenle, güvenlik açısından kritik bilgiler SSL / TLS korumalı bir bağlantı üzerinden iletilmeden önce, ilgili sertifika yetkilisinin güvenlik politikası kontrol edilmelidir.

Yeni bir sertifika eklerken, sertifikayı aktif etmeden önce "parmak izi" kontrol edilmelidir. Parmak izi, sertifika ile birlikte gönderilen, sertifika doğrulamak için kullanılan onaltılık bir sayıdır. Sertifikanın doğrulaması parmak izi ile yapılacağı için, parmak izi farklı bir yol ile iletilmeli ve kontrol edilmelidir.

Geçmişte; çevrim içi bilgi servisleri, çevrim içi portaller ve anonimleştirme servisleri de dâhil olmak üzere sertifika otoriteleri yüzlerce sahte sertifikaya maruz kalarak istismar edilmiştir. İptal listeleri ve OCSP (Çevrimiçi Sertifika Durum Protokolü) gibi doğrulama protokolleri, sahte, manipüle edilmiş veya süresi geçmiş sertifikaları zamanında geçersiz kılabilirler. Bu nedenle, tarayıcılar ve e-posta istemcileri gibi uygulamalarda sertifika doğrulama işlevi etkinleştirilmelidir. OCSP kullanımı, Sertifika İptal Listeleri (CRL) kullanımına göre tercih edilebilir. Çünkü OCSP internet üzerinden zamanında güncellenebilmektedir.

OSCP sunucusuna veya iptal listelerine (CRL) erişim sağlanamadığı için sertifika doğrulamasının yapılamadığı durumda genelde iki seçenek bulunur. Bağlantı sonlandırabilir veya muhtemelen değiştirilmiş veya geçersiz olan sertifika kabul edilir. Bu gibi durumlarda kurum güvenlik politikası dikkate alınarak karar verilmelidir.

Oturum yeniden müzakeresi ve TLS sıkıştırma

Oturum yeniden müzakeresi (renegotiation) kullanılarak hem istemci hem de sunucu, mevcut bir HTTPS oturumunun parametrelerini yeniden müzakere edebilir. TLS protokolündeki bir hata nedeniyle, ortadaki adam saldırısını gerçekleştiren bir saldırgan, oturum yeniden müzakeresini kötüye kullanarak mevcut bir HTTPS oturumuna bir içerik

ekleyebilir. Bu arada, TLS protokolü güncellenerek bu tasarım hatası düzeltilmiştir. Ancak yine de, istemci tarafında oturum yeniden müzakere edilme işlevinin devre dışı bırakılması tavsiye edilir.

TLS, iletilen verilerin şifrelenmeden önce sıkıştırabilmesini mümkün kılar. Bu durum saldırı amacıyla da kullanılabilir. Bunu önlemek için TLS sıkıştırmasının devre dışı bırakılması önerilir.

BTS.2.U19 Kısıtlayıcı hakların tahsisi

Temel olarak, kullanıcı yetkileri her zaman kısıtlayıcı olmalıdır. Böylece kullanıcılar tam olarak görevleri için ihtiyaç duydukları hizmetlere ve verilere erişebilirler. Bu, sistem dosyaları veya sistem dizinleri için ayrıca önemlidir.

Sistem dosyaları ve sistem dizinleri, BT biriminin sorumlu olduğu dosya ve dizinlerdir. Sistem dosyalarına yalnızca yetkili BT ekibi erişebilmelidir. Editör uygulamaları ve derleyiciler, gerekli olmadıkça kullanılmamalıdır. Yetki verilmiş sistem yöneticileri mümkün olduğunca az olmalıdır. Ayrıca, kullanıcıların dizinlere erişimi yalnızca ihtiyacı karşılayacak kadar olmalıdır. Sistem dosyalarına erişim her zaman kurum güvenlik politikalarına uygun ve kısıtlayıcı olmalıdır.

Sistem dosyaları, uygulama ve kullanıcı verilerinden ayrı bir alanda olmalıdır. Böylece yedeklemelerin oluşturulması ve erişim haklarının düzenlenmesi kolaylaşır.

Sistem dosyalarına yapılan erişimler, her zaman kaydedilmelidir. Gereksiz sistem dosyaları, BT sisteminden kaldırılmalı veya bütünlük için sürekli izlenmelidir. Böylece saldırılar için kötüye kullanımın önüne geçilmiş olur.

Erişim hakları kısıtlanırken, sadece bir yazılıma ait hakları kısıtlamak yeterli değildir. Ek olarak, bu program ile beraber kullanılan tüm programların hakları da göz önünde bulundurulmalıdır.

Tüm sistem dosyalarının ve dizinlerin bütünlüğünün yanı sıra erişim haklarının doğruluğu, mümkünse düzenli olarak kontrol edilmelidir. Bu işlemi hızlı ve güvenilir bir şekilde yapabilmek için işletim sistemlerinde yer alan farklı araçlardan yararlanılabilir.

BTS.2.U20 Yönetim ara yüzlerinin korunması

İstemcileri yönetmek için farklı yöntemler bulunur. Kullanılan erişim türüne bağlı olarak bazı güvenlik önlemlerin alınması gereklidir. Büyük ağlar için, istemcilerin merkezi bir yönetim sistemine entegre edilmesi önerilir. Hatta çoğu durumda bunu yapmak bir zorunluluk olabilir. Aksi takdirde, istemcilerin güvenli ve verimli bir biçimde yönetimi tam

olarak sağlanamayabilir. Yönetim için kullanılan yöntemler güvenlik politikasında tanımlanmalı ve istemci yönetimi yalnızca güvenlik politikasına uygun olarak yapılmalıdır.

Çeşitli yönetimsel işlemler için hangi çalışmaların hangi yöntemlerle yapılacağına yönelik genel anlatımlar hazırlanmalıdır.

Yerel yönetim

İstemcilerin yerel olarak doğrudan yönetimi az sayıda istemci olduğu durumlarda düşünülebilir. Genellikle çok sayıda istemcinin bulunduğu ortamlarda bu yönetim şekli sadece bir istisna olarak tercih edilir. İstisnai olarak yönetimsel BT işlemlerinin bir istemci üzerinde yerel olarak yapılması gerekiyorsa; bağlantı yapan sistem yöneticisinin, kimlik doğrulama sırasında kullandığı şifrenin gizlenemeyeceği bilinmelidir. Gerekirse, bu çalışma yöntemi için tek seferlik şifreler veya benzer teknikler kullanılmalıdır.

Bir önyükleme ortamıyla yönetim

Bir istemcide yerel olarak gerçekleştirilecek yönetimsel bir çalışma için, istemciyi bir önyükleme medyası ile başlatmak avantaj sağlayabilir (Ayrıca bkz. *"BTS.2.U4 Düzenli yedekleme"*). Böylelikle, sistem yöneticisi istemciyi "temiz" bir şekilde başlattığından emin olabilir. Bu yöntem maliyet açısından ve hataların doğru bir şekilde izlenememesinden dolayı bazı dezavantajlara sahiptir.

Uzaktan yönetim

İstemciler genellikle yönetim bilgisayarları kullanılarak ağ üzerinden yönetilirler. Yöneticilerin kimlik doğrulama bilgilerinin bir saldırgan tarafından ele geçirilmesini veya manipüle edilmesini önlemek için yönetim yalnızca güvenli protokoller üzerinden (ör. Telnet üzerinden değil, SSH aracılığıyla) gerçekleştirilmelidir. Dış (güvenli olmayan) ağlar üzerinden güvenli olmayan uzaktan yönetim, güvenlik politikasının tanımında göz önünde bulundurulmalıdır. İç ağda mümkün olduğu kadar güvenli olmayan protokoller kullanılmamalıdır.

Merkezi Yönetim Sistemiyle Yönetim

Yönetim için merkezi bir yönetim sistemi kullanılması durumunda, uzaktan yönetim için geçerli hususlar dikkate alınmalıdır. Ayrıca, merkezi yönetim sisteminin kendisinin uygun güvenlik yöntemleriyle yapılandırılmış olması ve uygun güvenlik ilkelerinin uygulanması önemlidir.

Rutin yönetimsel faaliyetler

Güvenlik politikasına göre olağan rutin BT işlemleri için yönetim talimatlarının oluşturulması tavsiye edilir. Bu talimatlarda aşağıda sunulan konular yer almalıdır.

- Kullanıcı oluşturulması ve silinmesi,
- Programların kurulumu ve kaldırılması,
- Güvenlik güncellemeleri ve yamaların uygulanması,
- Diğer güncellemelerin ve yamaların uygulanması,
- Uygun programlar ile düzenli bütünlük kontrollerinin yapılması.

BTS.2.U21 İstemci mikrofon ve kameralarının yetkisiz kullanımının önlenmesi

Günümüzde birçok istemci, mikrofonlar ve kameralarla donatılmıştır. Ağa bağlı istemciler üzerinde bulunan mikrofonlar ve kameralar, erişim yetkisi bulunan uygulamalar ve hizmetler tarafından kullanılabilir. Bu donanımlara verilen erişim hakları dikkatli bir şekilde yapılandırılmalıdır. Mevcut mikrofonlar veya kameralara ihtiyaç yoksa yanlış kullanımın önüne geçmek için bu aygıtlar devre dışı bırakılmalı veya fiziksel olarak istemciden ayrılmalıdır.

Mikrofon veya kamera istemciye kalıcı olarak takıldıysa ve yalnızca yazılım tarafından açılıp kapatılabilecekse, yetkisiz bir kişinin bunları kullanamaması için erişim hakları doğru bir şekilde yapılandırılmalıdır. Böylece, normal kullanıcıların mikrofon veya kamerayı kullanması engellenebilir. Ayrıca kameralar, uygun bir etiketle kaplanarak kolayca kapatılabilir.

Mikrofon ve kameraya sahip istemcilerde aygıt dosyalarına erişirken, erişim haklarının ve sahipliklerinin değişip değişmediği kontrol edilmelidir. Bir kullanıcının, mikrofon veya kamerayı kullanabilmesi isteniyorsa aşağıdaki hususlar sağlanmalıdır:

- Aygıtlar, istemcide bir kullanıcı oturumu açıldığında aktif edilmelidir,
- Sadece oturumu açan kullanıcı tarafından etkinleştirilebilir olmalıdır,
- Oturum kapatıldıktan sonra kullanıcının erişim yetkileri de iptal edilmelidir.

Mikrofona veya kameraya erişim güvenli bir şekilde kontrol edilmediği müddetçe, aygıtlar istemciden fiziksel olarak çıkartılmalı veya istemcinin ağ ile bağlantısı kesilmelidir.

Dâhili mikrofon veya kameralı istemciler gizli bir toplantı esnasında odadan çıkartılmalı veya en azından kapalı tutulmalıdır. Gerekli olmadığı veya kullanılmadığı durumlarda dizüstü bilgisayarların ağ ile bağlantısı kesilmelidir. Çoğu durumda, ağ bağlantısını sağlayan kabloyu istemciden çıkarmak en kolay yoldur.

BTS.2.U22 Oturumun kapatılması [kullanıcı]

Bir BT sistemi veya uygulaması, birkaç kullanıcı tarafından kullanılacaksa ve kullanıcılar bu istemci üzerinde farklı erişim haklarına sahip olacaksa, erişim kontrolü ile sağlanabilecek güvenlik ancak her bir kullanıcının veya uygulamanın oturumu güvenli bir

şekilde sonlandırması ile sağlanabilir. Üçüncü bir taraf, bir BT sistemi veya uygulamasında başka bir kimlik altında çalışmayı sürdürebilirse, anlamlı bir erişim kontrolü sağlamak mümkün olmayacaktır. Bu nedenle tüm kullanıcılar, işlemlerini tamamladıktan sonra uygulamalardan ve BT sisteminden oturumlarını kapatarak çıkmaya zorlanmalıdır.

BT sistemi üzerinde devam eden çalışmaya kısa bir ara verilecekse, güvenli çıkış yapmak yerine ekran kilidi manuel olarak etkinleştirilebilir (Ayrıca bkz. *"BTS.2.U5 Ekran kilidi"*). Kullanıcının daha uzun bir süre istemciden uzak kaldığı durumlar için ekran kilidi otomatik olarak etkinleştirilmelidir.

Bazı BT sistemleri ve uygulamalar, kullanıcının belli bir süre aktif olmadığı durumlarda oturumunun otomatik olarak kapatılması için bir zaman aralığı tanımlanmasını mümkün kılar. Veri kaybına yol açabileceğinden dolayı bu özelliğin uygulanıp uygulanmayacağı dikkatli bir şekilde analiz edilmelidir.

BTS.2.U23 İstemci – sunucu hizmetlerinin kullanımı

Benzer BT sistemleri arasında yapılan bilgi alışverişi genellikle "istemciden-istemciye" veya "eşler arası (peer to peer)" olarak adlandırılır. Her bir BT sistemi hizmet sunabilir veya kullanabilir. Bu amaç için kurulan iletişim bağlantısı, birçok BT sisteminin, merkezi olmayan bir şekilde kaynakları birbiriyle paylaşmasını sağlar. Bu durum, bir sunucu ve bir istemcinin işlevlerini bir BT sistemi üzerinde birleştirmesini sağlar.

Genellikle, bu uygulamalar diğer BT sistemlerine aşağıdaki hizmetleri sağlamak için kullanılır:

- Bir BT sistemine yerel olarak bağlı olan yazıcının diğer BT sistemleri tarafından kullanılması,
- BT sisteminde bağlı olan diskler ve depolama alanlarına başka sistemler tarafından erişilmesi,
- Metin mesajları ile doğrudan iletişim,
- IP telefon hizmeti.

İstemciden – istemciye hizmetlerin avantajları

Sunucu tabanlı mimariden farklı olarak, istemciden istemciye hizmetlerin birçok avantajı vardır:

- Özel bir sunucu kullanmakla oluşabilecek ek maliyetler ortadan kalkabilir.
- Merkezi sunucunun arıza yaşaması durumunda, kaynaklar iletişim kuramayabilirler (tek hata noktası). İstemciden istemciye hizmetlerde, bir istemciye erişilmezse, genellikle yeterli sayıda var olan diğer istemciler kullanılabilir.

- Uzaktaki bir sunucuya bağlanmak yerine komşu istemciler birbirleriyle daha verimli bilgi alışverişi yapabilirler.
- Sunucular istemcilere göre daha fazla bant genişliği, daha fazla CPU, daha fazla disk ve bellek gerektirir. Bu ihtiyaçlar, istemciden-istemciye çalışan ağlarda kaynağı boşta olan istemciler tarafından karşılanabilir.
- Paylaşılan bilgiler çoğu zaman aynı anda birden fazla istemcide bulunduğundan yedeklenmiş olarak düşünülebilir.

Bununla birlikte, istemciden-istemciye hizmetlerin kullanımı merkezileşme eksikliğinden dolayı bazı dezavantajlara sahiptir. Örneğin, istemciler arasında paylaşılan bilgiler zararlı yazılımlara karşı merkezi olarak taranamazlar.

Mimari

Gereksinimlere bağlı olarak, istemciden-istemciye hizmetler yalnızca yerel bir ağda veya internet ağında kullanılabilir. Kaynakları paylaşabilen BT sistemlerinin sayısı, birkaç istemciden yönetilemeyecek kadar çok sayıda istemciye kadar değişebilir.

Genel olarak iki tür istemciden-istemciye hizmeti vardır:

- Yerel istemciden-istemciye hizmetler

Yerel istemciden-istemciye hizmetlerde, istemciler tekil olarak kaynaklarını yerel ağda diğer istemcilerle paylaşabilirler. Bu paylaşımlar, genellikle doğrudan işletim sistemi tarafından yönetilebilir. Bu duruma örnek olarak, Windows işletim sistemlerinde kullanılan dosya ve yazıcı paylaşımları verilebilir. Bu servislere erişim genellikle parolalar veya IP adresi filtreleri ile sınırlandırılabilir. Genellikle bu tip hizmetler, yerel ağın dışına çıkmaz ve dış güvenlik duvarı tarafından reddedilir. Bu tür hizmetlerin kullanılmasında merkezi bir sunucuya gerek duyulmadığından, donanım ve yazılım tedariki için gerekecek maliyetler yönünden tasarruf sağlanır.

- Dış istemciden-istemciye hizmetler

Dış istemciden-istemciye hizmetler, yerel ağa erişimi olmayan kullanıcılarla bilgi alışverişi yapmak için kullanılabilir. Bunu yapmak için istemcilere, birbirleri üzerindeki servisleri kullanmalarına olanak tanıyan ek uygulamaların yüklenmesi gerekebilir. İstemciden-istemciye hizmetlerde, iki veya daha fazla BT sistemi arasında doğrudan bilgi alışverişi olacağından, sistemlerin birbirlerine nasıl bağlantı sağlayacağı hakkında ek bilgilere ihtiyaç duyulur. Bu nedenle, özellikle istemciden-istemciye hizmet sunan geniş ağlarda, hangi istemcide hangi kaynakların kullanıma sunulacağına dair genel bir tanımlama yapılmalıdır.

İstemciden-istemciye hizmetlerin çeşitleri aşağıdaki gibidir:

- Merkezi istemciden-istemciye hizmetler

İstemciye yüklenen bir uygulama, diğer istemciler hakkında bilgileri yöneten merkezi bir sunucuya bağlanır. Bunu yapmak için istemci önce, sunucuya kullanıma sunduğu kaynaklar hakkında bilgileri aktarır. Bu bilgiler aktarıldıktan sonra, istemci oturum açmış diğer istemciler hakkında bilgilere erişebilir. Bu bilgiler IP adresi, kullanıcı bilgileri ve sağlanan içerikle ilgili bilgilerdir. Merkezi sunucuya bağlantı başarısız olursa ya da merkezi sunucuda bir sorun çıkarsa bağlı istemcilerin iletişim bilgilerine artık erişilmez ve istemciler artık birbirleriyle bağlantı kuramazlar. Sonuç olarak böyle bir durum, tüm istemci-istemci ağının hizmet dışı kalmasına neden olur.

- Dağıtık istemciden-istemciye hizmetler:

Dağıtık tipteki istemciden-istemciye hizmetlerde, istemcileri yöneten merkezi bir sunucuya ihtiyaç yoktur. Bu tip bir hizmette, istemciler bilgi alışverişinde bulunmak için birbirlerine direkt veri bağlantıları kurarlar. Bir bağlantının doğrudan kurulduğu istemcilerin kaynakları paylaşılmak ile kalmaz, aynı zamanda bir bağlantı kurmuş olan diğer kullanıcılar hakkında bilgiler de edinilebilir.

Ağa üye olmak için gerekli iletişim bilgileri önceden bilinmelidir. Birçok ağ bağlı çok sayıda istemciden faydalandığından, iletişim bilgileri genellikle bir web sitesinde yayınlanır.

- Hibrit istemciden-istemciye hizmetler

Hibrit tip istemciden-istemciye hizmetler, merkezi tip istemciden-istemciye hizmetlere benzerler ancak bu sistemde bir merkezi sunucu yerine, birden çok sunucu bulunur. Merkezi istemci-istemci hizmetlerinde olduğu gibi, istemcilerin sağladıkları kaynak bilgilere ve istemcilere nasıl erişileceği hakkında diğer bilgiler sunucularda tutulur. Sunucular sırayla üzerinde tuttukları istemci bilgilerini diğer sunucularla paylaşır. Bu sayede istemciler, bilgileri farklı sunucular tarafından tutulan diğer istemcilerin kaynaklarına da erişebilirler.

İstemciden-istemciye hizmetlerin kullanımı yerine sunulabilecek alternatifler

Yalnızca birkaç hizmet istemciden-istemciye bağlantı kurulmasını gerektirir. Buna karşın paylaşılması istenen kaynaklar, merkezi bir sunucuda da tutulabilir. Merkezi bir sunucu kullanarak kuralların merkezi olarak uygulanması sağlanabilir. Aşağıda detayı verilen istemciden-istemciye hizmetler bu şekilde merkezi olarak verilebilir:

- Yazıcılar

Yerel ağda bir çok kişinin yazıcılara erişmesi gerekiyorsa, yazıcı hizmeti merkezi olarak sağlanabilir. Bu hizmet, ağ özellikli yazıcıların kullanımı veya yazıcı yönetim sunucuları kullanılarak yapılabilir.

- Dosya Paylaşımı

Yerel ağda birçok istemciye depolama alanı tahsis etmek yerine merkezi bir sunucuda iş ile ilgili dosyaların saklanması sağlanabilir. Bu sayede diğer istemciler ve kullanıcılar merkezi dosya sunucusu üzerinden dosya paylaşımını yapabileceklerdir. Eğer dosyalara iç ağ dışından yani dış bir ağdan da erişilmesi istenirse, dışa açık bir web sunucusu kullanılabilir.

- Mesajlaşma

İstemcilerin birbirleriyle mesajlaşması gerekiyorsa istemciden-istemciye mesajlaşma yerine merkezi bir sunucudan yönetilen kurumsal çözümler veya açık kaynak anlık mesajlaşma sistemleri tercih edilebilir. Bu sayede, mesajlarda paylaşılan dosyalar merkezi sunucu tarafından zararlı yazılımlara karşı kontrol edilebilir. Anlık mesajlaşma yazılımı aynı zamanda dış paydaşlarla iletişim için de kullanılabilir.

- VoIP ve internet telefon hizmet

VoIP çözümleri, sinyal iletimi ve medya aktarımı olarak ikiye ayrılır. Sinyalleşme için uçların yönetilebileceği sunuculara ihtiyaç duyulur. Sinyalleşme ile iki veya daha fazla kullanıcı arasında bir görüşme başlatıldıktan sonra, birçok çözüm yönteminde ses bilgisi doğrudan kullanıcılar arasında paylaşılır. Yerel ağ üzerinde gerçekleştirilen bu tip istemciden-istemciye hizmetler kullanışlıdır ve kullanılması önerilir.

Ancak, telefon görüşmelerinde kullanılan istemciden-istemciye hizmetler yerel ağın dışında kullanılmamalıdır. Örneğin, bu tür "internet telefonu" iletişim yöntemiyle dış muhataplarla iletişim kurulmasına izin verilmemelidir. Bu durum güvenlik açıklarına neden olabilir. Eğer böyle bir yöntem dış iletişim için de kullanılacaksa hem sinyalleşme hem de medya aktarımı için veriler vekil sunucuya (Proxy) benzer bir sunucuda paketlenmelidir. Bu şekilde, istemcilerin internetteki harici istemcilere doğrudan bağlantı kurulması önlenir.

Yerel istemciden-istemciye hizmetler için öneriler

Bilgi alışverişinde, istemciden-istemciye hizmetler yoluyla paylaşım yerine mümkünse özel sunucular kullanılmalıdır. Ancak, VoIP'de olduğu gibi bazı istisnai durumlarda istemciden-istemciye çözümlerin kullanılması gerekli olabilir. Bu nedenle ilgili kararların alınması gerekir;

- Hangi tip istemciden-istemciye hizmetler kullanılacak?
- Hangi bilgilerin paylaşılmasını izin verilecek?

Kullanıcılar, istemciden-istemciye hizmetlerin kullanımı konusunda bilgilendirilmelidir. İstemciden-istemciye hizmetlerin yalnızca yerel ağ ile sınırlı olmasını sağlamak önemlidir.

Halka açık istemciden-istemciye hizmetlerin kullanılmasına yönelik öneriler

Genel olarak, yerel ağda kontrolsüz bilgi akışı önlenmelidir. İstemcilerin yerel ağda bulunmayan BT sistemlerine doğrudan bağlantı yapması, istenmeyen bir durumdur. Merkezileştirme eksikliği, bilgilerin kontrolsüz olarak yerel ağdan dışarı sızmasına (ör. gizli bilgiler) veya bilgilere dışarıdan erişilmesine – hatta güvenilir olmayan yazılımların iç ağa girmesine – (ör. zararlı yazılım) neden olabilir. Aşağıda verilen önlemler aracılığıyla kullanılması istenilmeyen istemciden-istemciye hizmetlerin engellenmesi sağlanabilir:

- Yerel paket filtreleri

Yerel paket filtreleri kullanılarak, istemcilerin iletişimi sınırlandırılabilir. Örneğin, iletişimin yalnızca belli sunucularla sınırlı kalması için filtre kuralları uygulanabilir. Sunucunun IP adresine ve izin verilen hizmetin bağlantı noktasına bağlı olarak, istenmeyen bir bağlantının kurulumu daha zor hale getirilebilir. Yerel paket filtreleri kullanılarak hem yerel hem de dış istemci-istemci ağlarının istenmeyen biçimde kullanımı önlenebilir.

- Güvenlik ağ geçidi üzerinden merkezi filtreleme (güvenlik duvarı)

Güvenlik duvarı, yerel ağ içinde veya dışında yalnızca gerekli olan bağlantılara izin vermelidir, bunun dışındaki tüm bağlantıları reddetmelidir. Güvenlik duvarı, istemcilerin yerel ağdan internetteki herhangi bir sistem ile iletişimini engelliyorsa, halka açık istemciden-istemciye ağların kullanımı önlenebilir.

- Güvenlik politikaları

Teknik tavsiyelere ek olarak, kullanıcıların halka açık istemciden-istemciye hizmetleri kullanmasını engelleyecek önlemler alınmalıdır. Bu durum, istemci ve kullanıcı güvenlik politikalarında kural haline getirilmelidir.

Kurumda istemciden-istemciye hizmetler kullanılacaksa, bunun kararı yönetim tarafından verilmelidir. Karara bilgi güvenliği birimi de dâhil edilmeli, riskler de dâhil olmak üzere verilen tüm kararlar kayıt altına alınmalıdır.

BTS.2.U24 Çıkarılabilir medyanın kullanımı

Günümüzde, istemcilerde taşınabilir ortamlardan veri alışverişi gerçekleştirilebilmektedir. Taşınabilir ortamlar; istemci üzerinde bulunan CD / DVD / Blu-ray okuyup yazan

donanımlar olabileceği gibi USB portları ile bağlantı sağlayan tak ve çalıştır özelliğine sahip donanımlarla da olabilir. Bunun dışında bazı istemcilerde hafıza kartlarını okuyabilen kart okuyucular dâhili olarak bulunabilmektedir. Çıkarılabilir medyalar ve harici veri depolama sürücüleri aşağıdaki potansiyel güvenlik sorunlarına neden olabilir:

- İstemcilerde, bu tür sürücüler aracılığıyla kontrolsüz bir şekilde önyükleme yapılabilir,
- Bu tür sürücüler aracılığıyla kontrolsüz bir şekilde yazılım kurulabilir,
- Veriler dışarı aktarılabilir veya kuruma ait lisanslı yazılımlar izinsiz olarak kopyalanabilir.

Çıkarılabilir medyadan önyükleme yapılırken veya üçüncü taraf yazılımları yüklenirken yalnızca güvenlik ayarları geçersiz kılınmaz, aynı zamanda bu durum BT sistemlerine virüslerin veya diğer zararlı yazılımların bulaşmasına yol açabilir.

Bu riskler, uygun idari veya teknik güvenlik önlemlerle giderilmelidir. Bu amaçla uygulanabilecek tedbirler, avantajları ve dezavantajlarını da içerecek şekilde aşağıda sunulmuştur:

Sürücülerin Çıkarılması

Çıkarılabilir medya için sürücülerin donanımdan tamamen ayrılması veya satın alma esnasında sürücüsüz olarak temin edilmesi yukarıda belirtilen tehlikelere karşı en güvenli korumayı sağlar. Genellikle, BT sistemlerinden bu donanımların tamamen iptal edilmesi mümkün olmayabilir. Ayrıca, böyle bir uygulamanın BT sisteminin yönetimini ve bakımını zorlaştırabileceği düşünülebilir. Bu sebeplerden ötürü böyle bir çözüm, gerçek anlamda özel güvenlik tedbirlerinin alınması gerektiği durumlarda değerlendirilmelidir. Bilgisayarların çıkarılabilir medyalara ihtiyacı olmadığı açık bir şekilde belirlenirse, satın alma sürecinde dâhili sürücüleri olmayan cihazların tercih edilmesi daha uygun olacaktır.

Sürücülerin Kilitlenmesi

Bazı sürücü tipleri için kontrolsüz kullanımı önleyebilecek kilitlenebilir sürgülü cihazlar bulunmaktadır. Tedarik aşamasında, bu çözüme ihtiyaç olup olmadığı değerlendirilmelidir. Dâhili bellek kartı okuyucuları gibi bazı sürücü tipleri için kilitlerin kullanılamadığı unutulmamalıdır. Ek olarak, kilitlerin, üretici tarafından yeterli sayıda farklı anahtarlar ile sunulmasına da dikkat edilmelidir. Bu yöntemin dezavantaj olarak, sürücü kilitleri için tedarik ve anahtar yönetim maliyetleri ortaya çıkacaktır. Bu nedenle, bu çözüm yalnızca daha yüksek koruma gereksinimleri veya özel güvenlik gereksinimleri için tercih edilmelidir.

BIOS veya işletim sisteminde devre dışı bırakılma

BIOS ayarlarında sürücülerin önyükleme için etkinleştirilebileceği ayarlar vardır. BIOS ara yüzüne erişim parola ile kısıtlanıp ilgili ayarlar yapılarak çıkarılabilir medyalardan veya taşınabilir veri ortamlarından kontrolsüz önyüklemeler engellenebilir. Ayrıca, mevcut sürücüler ve ara yüzler, günümüzde kullanılan işletim sistemleri aracılığıyla da devre dışı bırakılabilir.

Böylece, çıkarılabilir medyadan izinsiz olarak harici bir yazılım yüklenmesi veya bilgi kopyalanması engellenebilir. Sürücüler, BIOS veya işletim sisteminde devre dışı bırakılırsa, donanımın değiştirilmesi gerekmeyecektir. İşletim sistemindeki ilgili ayarların merkezi olarak yapılabileceği unutulmamalıdır. Bu prosedürün etkili olması için, kullanıcılara sürücüleri tekrar etkinleştirebilecek yetkiler tanımlanmamalıdır.

Şifreleme

Yalnızca bir tür kimlik doğrulama sonrası (parola, parmak izi, vb.), onaylanmış taşınabilir ortamlara erişimin mümkün olmasını sağlayan ürünler bulunmaktadır. Örnek bir çözüm olarak, belirli şifreleme anahtarlarıyla şifrelenmiş olan taşınabilir veri ortamları gösterilebilir. Bu tür ürünler, sadece manipüle edilmiş mobil veri taşıyıcılarını yetkisiz erişime karşı korumakla kalmaz, aynı zamanda kayıp veya hırsızlık durumunda mobil veri taşıyıcıları üzerindeki verilerin korunmasını da sağlar.

Kullanım talimatları

Çoğu durumda, kullanıcıların harici, yerleşik veya çıkarılabilir medya sürücülerini veya depolama ortamlarını kullanmasına izin verilir ancak bu kullanımlar uygun politikalar tarafından düzenlenmelidir. BIOS ayarları aracılığıyla, çıkarılabilir ortamdan önyükleme devre dışı bırakılmalıdır. Böylece, sürücüleri sökmeye, işletim sisteminden kapatmaya ve devre dışı bırakmaya gerek olmayacaktır.

Sürücüler ve depolama ortamlarının kullanımıyla ilgili talimatlar, mümkün olduğu kadar açık bir şekilde tanımlanmalıdır. Örneğin, her şey genel olarak yasaklanabilir. Politikalar tüm kullanıcılar tarafından bilinmeli ve politikalara uyumluluk izlenmelidir. Çıkarılabilir medyadan aktarılmış programların kurulması ve çalıştırılması yasaklanmalıdır, bu durum mümkün olduğunca teknik olarak önlenmelidir.

USB aygıtlarının kullanımı

USB arabirimi aracılığıyla; taşınabilir diskler, CD/DVD okuyucu ve yazıcılar ve USB bellekleri gibi çeşitli ek cihazlar istemcilere bağlanabilir. Ek olarak büyük depolama kapasitelerini sağlayabilen USB bellekler, anahtarlık formunda ve herhangi bir cebe sığacak şekilde olabilir. USB veri depolama aygıtlarının sürücüleri günümüzde kullanılan

işletim sistemlerine halihazırda entegre edilmiştir ve kullanımları için herhangi bir yazılım kurulumuna gerek yoktur. Bunun yanı sıra, USB yazıcılar ve USB kameralar da verileri saklamak için kullanılabilirler. Bu durum, USB portundan bağlantı yapabilen herhangi bir cihaz için de geçerlidir.

Veri ve programlar, USB veri depolama aygıtları kullanılarak, kontrolsüz bir şekilde içeri veya dışarı aktarılabilirler. Bu nedenle, USB depolama ortamı genel olarak geleneksel depolama ortamı ile aynı şekilde ele alınmalıdır. USB arabirimi diğer aygıtlar için kullanılıyorsa, USB depolama ortamının çalışmasını önlemek çok zordur. Örneğin, bir fareyi bağlamak için sadece USB portunun kullanılması tercih edilmişse bu portu kullanarak farklı aygıtlar kullanılabilir. Bu gibi durumlarda genellikle bir "USB kilidi" kullanmak veya ara yüzü diğer mekanik yollarla devre dışı bırakmak anlamsızdır. Bu nedenle ara yüzlerin kullanılmasına yönelik kısıtlamalar işletim sistemi seviyesinde veya ek programların yardımıyla yapılmalıdır. Alternatif olarak, cihazların eklenip eklenmediğinin merkezi olarak izlenmesi tercih edilebilir. Veri depolama aygıtlarını harici arabirimlere bağlamak için, sürücüler veya çekirdek modüller genellikle işletim sistemi tarafından yüklenir veya yapılandırma dosyalarına (Windows kayıt defteri) giriş yapılır. Bu unsurlar izlenerek değişiklikler algılanabilir. Değişiklikler tespit edildikten sonra, bir log kaydı oluşturulabilir ve ilgili kişiler bir bilgilendirilebilirler.

BTS.2.U25 BT güvenli kullanım politikası [kullanıcı]

BT sistemlerinin güvenli ve doğru kullanımını teşvik etmek için, karşılanması gereken asgari koşulları ve alınması gereken güvenlik önlemlerini zorunlu kılan bir politika hazırlanmalıdır. Bu politikanın elektronik formda bir intranet sunucusunda yayınlanması ve tüm kullanıcılar tarafından erişilebilir olması tavsiye edilir. Her yeni kullanıcı, bilgi teknolojisini kullanmadan önce politikanın varlığından haberdar olduğunu teyit etmelidir. Politikada yapılacak herhangi bir değişiklikten sonra ya da rutin olarak en az iki yılda bir verilecek eğitimlerle, kullanıcıların bu konudaki farkındalığı artırılmalıdır.

Örnek olarak hazırlanmış taslak bir politikada olması gerekenler aşağıda sunulmuştur:

Amaç ve tanımlar

Kılavuzun ilk kısmı, kullanıcıların bilgi güvenliği açısından duyarlı hale getirilmelerini ve motive edilmelerini amaçlamalıdır. Aynı zamanda, ortak bir dil ve ortak anlayış için politika içinde kullanılan terimler ve kısaltmalar (PC, sunucu, ağ, istemciler, kullanıcılar, hassas varlıklar vb.) bu bölümde tanımlanır.

Kapsam

Bu bölümde, politikanın kurumun hangi birimleri için geçerli olduğu belirtilmelidir.

Mevzuat ve iç düzenlemeler

Bu bölümde, uyulması gereken önemli kanun ve/veya mevzuatların (örnek olarak Kişisel Verileri Koruma Kanunu ve Telif Hakkı Yasası gibi) bilgileri yer almalıdır. Örnekler kullanarak, bu mevzuat ve yasaların ilgili BT ortamı kullanımı üzerindeki etkileri açıklanmalıdır. Ayrıca bu kısımda, kurum içinde kullanılan ilgili bütün düzenlemeler bir liste halinde sunulabilir.

Sorumluluklar

Bu bölümde, BT'nin kullanımıyla ilgili olarak birimlerin ve kullanıcının hangi sorumlulukları taşıdıkları tanımlanmalıdır. Özellikle; kullanıcı, BT teknikeri, denetçi, veri koruma görevlisi ve güvenlik yönetimi ekibinin rolleri farklılaştırılmalıdır.

İletişim

Politika, kullanıcıların bilgi güvenliği ile ilgili konularda iletişime geçebilecekleri kişileri ve iletişim bilgilerini (telefon, e-posta vb.) içermelidir. Kullanıcılara çok farklı iletişim bilgileri verildiğinde, kafa karışıklığına neden olabileceği unutulmamalıdır. Sadece birkaç farklı irtibat noktası tanımının yapılması tavsiye edilir, bu durumda kullanıcılar gerektiğinde doğru yere yönlendirilebilir (yardım masası uygulaması gibi).

Uygulanacak ve gözetilecek güvenlik önlemleri

BT kullanım politikasının son bölümünde, hangi güvenlik önlemlerinin kullanıcı tarafından izleneceğini veya uygulanacağını belirlemek gereklidir. Koruma gereksinimlerine bağlı olarak, bu rehberde önerilen önlemlerden daha fazlası da ele alınabilir. İşyerinde uygulanabilecek temel güvenlik önlemleri için bazı örnekler, PC'de güvenli oturum açma ve kapatma olaylarının kayıt altına alınması, internet hizmetinden faydalanır iken parola ve davranış kurallarının doğru şekilde ele alınması olarak verilebilir.

BTS.2.U26 Uygulamaların korunması

Uygulamalardaki güvenlik açıklarından yararlanılmasını zorlaştırmak için, ASLR ve DEP / NX'in çekirdek içinde etkinleştirilmesi ve uygulamalar tarafından kullanılması önerilir. Çekirdeğin güvenlik özellikleri ve standart kütüphaneler b-heap ve yığın koruması devre dışı bırakılmamalıdır. Daha detaylı bilgi edinmek için konuyla ilgili kaynakların incelenmesi tavsiye edilir.

BTS.2.U27 İstemcilerin kontrollü olarak hizmet dışı bırakılması

Bir istemciyi hizmet dışı bırakırken aşağıda belirtilen durumlar öncelikli olarak sağlanmalıdır.

- Önemli verilerin kaybolmaması,

- İstemci diski üzerinde hassas verilerin bırakılmaması.

Özellikle, BT sistemlerinde hangi verilerin depolandığı ile ilgili genel bilgi sahibi olmak önemlidir.

Veri Yedekleme

İstemciyi hizmet dışı bırakmadan önce, ihtiyaç duyulan ve yerel olarak saklanan veriler harici bir ortama, bir yedekleme sistemine veya bir dosya sunucusuna aktarılarak yedeklenmeli veya arşivlenmelidir. Bu işlemden sonra, tüm verilerin sağlıklı bir şekilde yedeklendiği doğrulanmalıdır.

İstemcinin dizin hizmetlerinden ve veri tabanlarından çıkarılması

İstemcinin kendisiyle ilişkili herhangi bir ağ ayrıcalığı varsa bunlar silinmelidir. Örnek olarak; güvenlik ağ geçidinde ve vekil sunucularda bulunan kayıtlar verilebilir. Ayrıca, IP adresi veya MAC adresi kullanılarak ağ hizmetlerine erişim için yapılan tanımlamaların silinmesi de örneklere eklenebilir. İstemci, ağda kullanılan dizin hizmetleri veya veri tabanlarında (Windows etki alanı, Active Directory, NIS vb.) kayıtlı ise, ilgili kayıtlar silinmeli veya en azından devre dışı bırakılmalıdır.

İstemcideki verilerin silinmesi

Sabit disklerde korumaya değer hiçbir bilginin artık yer almadığı teyit edilebilir olmalıdır. Diskleri sadece biçimlendirmek yeterli değildir, diskler silindikten sonra üzerine en az bir kez tamamen veri yazılmalıdır. Disk üzerindeki verileri, işletim sisteminin silme işlevleriyle mantıksal olarak silmenin veya disklerin yeniden biçimlendirmenin aslında verileri sabit disklerden kaldırmadığı unutulmamalıdır. Bu gibi durumlarda, çoğu zaman uygun yazılımlar kullanarak, fazla çaba göstermeden veriler yeniden oluşturulabilir.

Aşınma seviyesi, yedek kapasitenin düşmesi ve beklenen ömrünün azalması nedeniyle SSD'lerin üzerine tekrar yazılması tavsiye edilmez. SSD'ler için, SSD tarafından sağlanan güvenli silme işlevini kullanmak ve ardından sonucu kontrol etmek önerilir.

Yedekleme medyasının silinmesi

BT sistemlerinin kullanımdan kaldırılmasından sonra, üzerinde depolanan verilere artık ihtiyaç duyulmazsa ilgili yedekleme ortamının silinmesi gerekebilir.

Diğer bilgilerin kaldırılması

Potansiyel olarak hassas olan herhangi bir veri (belirli konfigürasyon bilgileri gibi), bir istemcide sabit disk dışındaki herhangi bir yerde mevcut olabilir. Bu bilgiler, istemci kullanım dışına çıkarılmadan önce kaldırılmalıdır. İstemciyi, hizmet dışına çıkartırken

kullanılmak üzere bir kontrol listesi oluşturulması ve kontrol listesinde yukarıda verilen önerilerin kullanılması tavsiye edilir.

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.2.U28 İstemcilerin şifrelenmesi (G)

Veri medyası ile ilgili gizli bilgiler çeşitli şekillerde şifrelenebilir ve böylece yetkisiz erişime karşı korunabilir. Örneğin; tüm disk birimi, tek bir bölüm veya sadece belirli dosyalar şifrelenebilir. Güvenlik açısından, veri barındıran medyanın tamamının şifrelenmesi tercih edilir, çünkü bu yöntemin uygulanması daha az kullanıcı müdahalesi gerektirir ve bir işlemle tüm veriler yetkisiz erişime karşı korunmuş olur. Bu yöntemde, yalnızca önyükleme yapılırken veya ilgili disk bölümüne ilk kez erişildiğinde, kullanıcı kimlik doğrulaması yapılması gerekir. Belirli dosyaların veya klasörlerin şifrelenmesi durumunda, sabit diskin şifrelenmemiş alanlarında hassas veri saklanması riski devam edecektir. Ayrıca bu tercihte, şifreleme otomatik olmadığından kullanıcının şifreleme programını elle başlatması gerekecektir.

Disk bölümleri tek tek şifrelenmiş olsa dahi gizli kalması gereken bazı verilerin şifrelenmiş alan dışında kalma riski olabilir. Bu nedenle, veri ortamının tamamen şifrelenmesi, hassas verilerin yetkisiz erişime karşı güvenilir şekilde korunması için en iyi ve en etkin yoldur.

Disk şifreleme, bir yazılımla ya da donanım desteği ile uygulanabilir. Bu kapsamda piyasada birçok yazılım çözümü bulunmaktadır. Kurum güvenlik gereksinimleri göz önünde bulundurularak, bu çözümlerin hangisinin kurum için en ideal çözüm olduğu analiz edilmelidir.

Harici diskler ve dizüstü bilgisayarlar gibi üzerinde veri bulunan taşınabilir aygıtların tamamen şifrelenmesi önerilmektedir. Gizlilik gereksinimleri yüksekse, masaüstü olarak kullanılan istemcilerdeki veri barındıran aygıtların da tamamen şifrelenmesi önerilir.

Şifreleme programına ek olarak diski şifrelemek için bir şifreleme anahtarı gereklidir. Şifreleme anahtarları düzgün bir şekilde oluşturulmalı ve şifrelenmiş diskten ayrı bir ortamda saklanmalıdır. Bu amaçla, örneğin akıllı kartlar veya USB bellekler kullanılabilir. Güvenlik analizlerinde bu durum dikkate alınmalıdır.

Şifrelenmiş birimlerde depolanan veriler de düzenli olarak yedeklenmelidir.

Bazı şifreleme programları şifrelenmiş alanları "gizleme" seçeneği sunar. Bu tür işlevlerin uygulanması zor olduğundan ve yanlış çalışma sonucu veri kayıplarına yol açabileceğinden bu yöntemin yalnızca özel durumlarda kullanılması önerilmektedir.

Şifreleme ürünü kullanımı

Alınan tüm önlemlere rağmen çalınan taşınabilir bir istemciden hassas verilerin istenmeyen kişilere geçmesini engellemek için bir şifreleme programı veya mevcut bir işletim sistemi güvenlik çözümü kullanılmalıdır. Piyasada bulunan ürünlerin yardımıyla, sadece bazı dosyaların, diskteki bazı bölümlerin veya sabit diskin tamamının, yalnızca gizli anahtara sahip olanların okuyabileceği ve kullanabileceği şekilde şifrelenmesi mümkündür.

Şifreleme güvenliğinde dikkat edilmesi gereken noktalar şunlardır:

- Kullanılan şifreleme algoritması, kullanılan anahtar bilinmeden şifreli metnin çözülmesine imkân tanımayacak kadar iyi olmalıdır. Bunun için son teknoloji ve oldukça karmaşık şifreleme anahtarları kullanılması önerilir.
- Mümkünse, rastgele bir anahtar oluşturulmalıdır.
- Şifreleme algoritması, şifrelenmiş dosyalar ve anahtarlar bir veri ortamında birlikte saklanmamalıdır. Anahtarın ayrı bir ortamda saklanması tavsiye edilir. Şifreleme anahtarları, çipli kartlar veya USB diskler gibi çıkarılabilir bir ortamda saklanmalıdır.

Şifreleme, çevrimiçi veya çevrimdışı olarak yapılabilir. Çevrimiçi, tüm sabit disk (veya bölüm) verilerinin, kullanıcı müdahalesi gerekmeden şifrelenmiş olduğu anlamına gelir. Çevrimdışı şifreleme, kullanıcı tarafından başlatılır ve kullanıcı hangi dosyaların şifrelenmesi gerektiğine tek tek karar verir.

Kendinden şifrelenen sabit sürücüler

Sabit disklerdeki gizli veriler yetkisiz erişimi önlemek için, mümkünse tamamen şifrelenmelidir. Kendinden şifrelenebilen aygıtlar, şifreleme için özel bir donanım olan şifreleme denetleyicisine sahiptir ve bu nedenle performansları daha yüksektir. Bu tarz çözümler, genellikle tek bir kullanıcı tarafından kullanım için tasarlanmıştır, yani çok sayıda kullanıcı tarafından kullanılan istemciler için geçerli bir çözüm olmayabilirler.

Kendiliğinden şifrelenen diskler ile çalışıldığında, diskin kapatılması durumunda tüm veriler şifrelenir ve RAM'de depolanan anahtar bir güvenlik riski oluşturur. Bu durum, bu yöntem tercih edilirken dikkate alınmalıdır.

Kendiliğinden şifrelenen sabit sürücüler bir TPM (trusted platform module) ile birleştirilmemelidir çünkü böyle bir kombinasyonda sabit diskin şifresi başka bir istemci ile

çözülemez. BT sistemi hasar görürse, sabit diskteki verilerin artık şifresi çözülemez, çünkü sabit disk TPM modülü sayesinde yalnızca ilgili istemcide çalışır hale getirilmiştir.

Kendiliğinden şifrelenen sabit sürücüler genellikle AES (Advanced Encryption Standard) yöntemini kullanırlar. Bilgiyi şifrelemek için kullanılan anahtar "Veri Şifreleme Anahtarı" (DEK – Data Encrypt Key) olarak adlandır. DEK'in sadece şifreleme denetleyicisinde olması sağlanmalıdır ve DEK manipülasyonlara karşı korunmaktadır. DEK, rastgele donanım olayları temel alınarak oluşturulmalıdır. DEK, “Kimlik Doğrulama Anahtarı” (AK – Authentication Key) ile şifrelenir. AK genellikle bir parola seçilerek kullanıcı tarafından oluşturulur. Bazı kendiliğinden şifrelenen sabit sürücülerde, AK ayrıca bir ortamda örneğin bir çip kartta veya taşınabilir bir USB bellekte saklanabilir ve ayrıca bir şifre ile şifrelenebilir. Bu durum, iki faktörlü kimlik doğrulamanın uygulanmasını sağlar.

DEK ve AK'ye ek olarak, parola veya şifreleme anahtarının saklandığı medyanın kaybolması halinde kullanılmak üzere algoritmayı çözmeyi sağlayan bir ana anahtar (master key) vardır. Kurulum sırasında böyle bir anahtar oluşturulmalı, gerektiğinde kullanılması için bu bilgi güvenli bir ortamda saklanmalıdır. Şifreli bir sabit diskin şifresinin unutulması durumunda takip edilmesi gereken süreçler tanımlanmalıdır. Böyle bir durumda şifreleme, ana anahtar kullanılarak sıfırlanmalı ve kullanıcı için yeni bir şifre belirlemelidir.

Kullanıcı başarıyla doğrulandıysa, DEK şifresi çözülür. DEK ile sabit diskteki tüm veriler, kullanıcı herhangi bir şey hissetmeden şifrelenir. Bilgisayar kapanırsa veya kendinden şifrelenen aygıtların (KŞA) sürücü entegrasyonu çözülürse, tüm veriler DEK ve AK ile şifrelenmiş olur.

Genel olarak, sabit disk tarafından şifreleme işlemi için kullanılan anahtar uzunluğu yeterince uzun olmalıdır. Şifreleme algoritmasını güvenli disk şifreleme modunda çalıştırmak gerekir. Aksi takdirde, şifreli metin iki sektör arasında taşınırsa, şifrenin çözülme riski ortaya çıkabilir.

Kendiliğinden şifrelenen sabit diskler satın alınmadan önce, sabit disklerin BT sisteminin diğer donanımlarıyla uyumlu olup olmadığı kontrol edilmelidir. Ayrıca, seçilen sabit diskin okuma ve yazma hız oranı dikkate alınmalıdır. Kendinden şifrelenen sabit disk modellerinin çok azı mevcut bir "Single Sign On (SSO)" mimarisine entegre edilebilir. Ayrıca, istemci üzerindeki normal sabit disklerin, kendinden şifrelenen sabit disklere (donanımla birlikte verilen bir programla veya yeni bir kurulumla) dönüştürülüp dönüştürülemeyeceği kontrol edilmelidir.

Kendiliğinden şifrelenen bir sabit diskin kurulumu, bu konuda yetkin sistem yöneticileri tarafından yapılmalıdır. Bunu yapmak için, önce yeni bir DEK oluşturulmalı, bir parola

atanmalı ve güvenli bir şekilde saklanması gereken bir ana anahtar (master key) oluşturulmalıdır. Varsayılan DEK başlatma şifresi öncelikle istemcinin kullanıcısı tarafından güvenli bir şifre ile değiştirilmelidir.

Kendiliğinden şifrelenen sabit sürücünün onarılması, satılması veya imha edilmesi halinde içerisinde değerli bilginin olmadığından emin olunmalıdır. Onarım, satış veya imha işleminden önce DEK yeniden üretilmeli veya "ATA Secure Erase" silme komutu uygulanmalıdır.

BTS.2.U29 Sistem izleme (E)

Kritik sistem olaylarına müdahale edebilmek için istemcilere yönelik uygun bir izleme sistemi oluşturulmalıdır. Bu sistem, istemcilerin durumunun ve işlevselliğinin sürekli izlenmesini içerir. Eğer hatalar oluşursa veya tanımlanmış eşik değerler aşılırsa bu durum otomatik olarak ilgili personele bildirilmelidir.

Bu amaçla istemci durum bilgisi, genellikle olayların değerlendirildiği merkezi bir sisteme aktarılır. Bununla birlikte, sistem olaylarını aktarabilmek için ağ ara yüzününe ilişkin bir takım ayarların değiştirilmesi gerekebilir. Örneğin SNMP'nin (Basit Ağ Yönetimi Protokolü) etkin hale getirilmesi gerekebilir. Böyle bir izleme istenmiyorsa, bu özellikler devre dışı bırakılmalıdır.

BTS.2.U30 Referans sistem kurulumu (GBE)

Temel konfigürasyonun, yapılan konfigürasyon değişikliklerinin, güncellemelerin ve yamaların istemcilere aktarılmadan önce kullanıcılar tarafından önceden test edilebileceği referans bir istemci kurulumunun oluşturulması önerilir. Bu referans kurulum, temel ayarları, güvenlik yamalarını ve güncellemelerini, ayrıca üretici tarafından yayınlanan normal güncellemeleri içermelidir.

Böylece bir referans kurulum hazır tutulduğunda istemciler klonlama gibi bir yöntemle hızlı bir şekilde hazırlanabilir ve daha sonra sadece birkaç ayarın yapılması yeterli olabilir. Kullanılacak bu "referans kurulum" dikkatle planlanmalı ve mutlaka test edilmelidir.

Referans kurulum ve yapılandırma, istemcilerde bulunan tüm donanım ve yazılımlarla uyumlu çalışabilir olmalıdır. Bu durum, tüm istemcilerin aynı donanım ve yazılım yapılandırmasına sahip olacağı anlamına gelmez. Bununla birlikte, farklı istemcilerin yapılandırması, kurulumun referans karakterini korumak için yeterince benzer olmalıdır.

Kullanıcıları etkileyen uygulama ve ayarları test ederken, yapılacak testlerin yönetici haklarıyla yapılmaması, istemcilerin teslim edileceği kullanıcılarla aynı yetkilere sahip hesaplar ile yapılması önerilir.

İsteğe bağlı olarak; aygıt sürücüsü, işletim sistemi yaması, sistemle ilgili uygulamalar gibi farklı test türleri için farklı test sistemlerinin kullanılması avantajlı olabilir. Bununla birlikte, böyle bir test ortamında, işletim sistemi ortamı ile uygulamalar arasındaki etkileşimlerin tümünün tam olarak kapsanamayacağının farkında olmak önemlidir. İstemciler için özel güvenlik gereksinimleri söz konusu olduğunda, belirli dağıtım senaryoları için yalnızca aynı donanım ve yapılandırılmış BT sistemlerinin kullanılması gerekli olabilir.

Verimliliğin artırılması ve hataları en aza indirmek için, sık tekrarlanan standart testlerin yer aldığı kontrol listeleri oluşturulabilir.

Tüm testler anlaşılır bir şekilde kayıt altına alınmalıdır. Güvenlik güncellemelerini ve yeni aygıt sürücülerini test ederken bu durum ayrıca önem kazanır. Çünkü kurulumun yanlış yapılması veya hatalı konfigürasyondan dolayı etkilenen istemciler, ağ erişimini kaybedebilir hatta istemcilerin önyüklemeleri bozulabilir. Özellikle bu gibi durumlarda testlerin kayıt altına alınması, sorun giderme için gereken süreyi önemli ölçüde azaltabilir.

BTS.2.U31 Yerel güvenlik duvarı kullanımı (GBE)

Bir kurumun tüm ağı uygun bir güvenlik duvarı ile korunmalıdır. Ayrıca, her bir istemcide uygulama veya ağ düzeyinde uygun erişim kısıtlamalarının kullanılması önerilir.

Yerel bir paket filtresi, bir istemciyi aynı alt ağdan başlatılan saldırılara karşı koruyabilir. Ek olarak, böyle bir paket filtresi her bir servis için daha detaylı bir erişim kontrolü sağlar.

Bununla birlikte, istemci kaynaklı ağ bağlantılarını kısıtlamak için yerel paket filtresi kullanılabilir. Böylece, ele geçirilmiş bir sistemin vereceği zararlar sınırlandırılabilir. Bu koruma yöntemi, bilgisayarın tamamen ele geçirilmesi halinde saldırgan tarafından devre dışı bırakılabilse de, en azından başlangıçta saldırganı yavaşlatacaktır. Böylece, saldırı tespiti ve olası engelleme çalışmaları için önemli ölçüde zaman kazanılabilir.

Ayrıca, yerel bir paket filtresinin loglama fonksiyonu, belirli saldırıların tespit edilmesine yardımcı olacaktır.

Hemen hemen bütün işletim sistemleri, belirli kurallara göre alınan/gönderilen paketleri inceleyen ve işleyen yerleşik filtre yeteneklerine sahiptirler. Filtre seçenekleri, işletim sistemine göre önemli farklılıklar gösterse de aşağıdaki filtreleme seçenekleri çoğu işletim sisteminde mevcuttur.

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

Örneğin paket filtre yardımıyla belirli bilgisayarlardan veya belirli alt ağlardan gelen paketler kolaylıkla engellenebilir.

Bazı uygulamaların, tekil IP adresleri veya IP adres aralıkları için bir hizmete erişim izni vermek veya vermemek için kendi mekanizmaları vardır. Bu mekanizmaların aksine, işletim sistemi seviyesinde kullanılan yerel paket filtreleme, yerleşik erişim kısıtlamasının yürürlüğe girmesinden önce hizmetin kendisini olası tehlikelere karşı koruyabilir.

Paket filtreleme kurallarının uygulanmasında iki genel strateji vardır:

Kara liste stratejisi: Bu strateji diğer adıyla izin verici strateji olarak anılır. Bu yöntem ile öncelikle her şeye izin verilir, engellenenler daha sonra kurallarla belirtilir. Açıkça belirtilmediği yani engellenmediği takdirde, bağlantıların tamamına izin verilir. Bu stratejinin avantajı, yönetim ve sorun giderme işlemleri için harcanan eforun düşük olmasıdır. Ancak bu stratejinin ciddi bir dezavantajı, unutulması veya gözden kaçması halinde güvenli olmayan ağ hizmetlerine erişimin açık olarak kalabilmesidir. Bu durum, potansiyel saldırılar için zemin oluşturur.

Beyaz Liste stratejisi: Diğer adıyla “kısıtlayıcı strateji”dir. Her türlü durum, açıkça izin verilmediği müddetçe yasaklanır. Beyaz listede bulunmayan her türlü erişim engellenir. Beyaz liste stratejisi, daha fazla güvenlik imkânı sunar ve bu nedenle ciddi bir gerekçe olmadığı müddetçe mutlaka bu yöntem tercih edilmelidir. Dezavantajları ise, yönetim maliyetlerinin daha yüksek olmasıdır. Çünkü erişim gereksinimlerinde yapılan her değişiklikte, yeni kurallar tanımlanması gerekecektir.

Özel güvenlik gereksinimleri olan istemcilerde, temel konfigürasyonun bir parçası olarak, tüm bağlantı isteklerini dışarıdan reddeden kurallara sahip yerel bir paket filtresi kurulması önerilir. İstemci ağa bağlı olduğunda bu politika etkin olmalıdır. İstemci tarafından hangi servislerin kullanılacağına bağlı olarak konfigürasyon sonrası, gerekli protokoller ve portlar etkinleştirilebilir.

Paket filtreleri, genellikle ağ trafiğinin ayrıntılı bir şekilde loglara kaydedilmesine izin verir. Bu nedenle, internet gibi güvensiz bir ağdan güvenlik duvarı ile ayrılmış güvenli ağlar içinde bulunan istemcilerde dahi yerel paket filtresi kurulması tercih edilmelidir. Bu sayede loglara kaydedilerek elde edilen bilgiler saldırıların tespit edilmesinde kullanılabilir. Ancak ağ trafik hareketlerini loglara kaydederken hiçbir gizlilik politikasının ihlal edilmediğinden emin olunmalıdır. Bu konuda bir çalışma yapılacağı zaman, konuyla ilgili taraflar (veri koruma sorumlusu, çalışan temsilcisi vb.) sürece dâhil edilmelidir.

ICMP sorunsalı

İnternet Kontrol Mesajı Protokolü (ICMP), IP paketlerinin iletimi esnasında yaşanan hataları bildiren mesajları iletmek için kullanılır. Örneğin bir paketin göndericisine, hedef ağa ulaşılamayacağını veya paketin hedef sisteme iletilmeyecek kadar büyük olduğunu belirten mesajlar bu protokol aracılığı ile iletilir. Ping ve traceroute araçlarının işlevi de ICMP protokolüne dayanmaktadır.

Birçok kullanışlı özelliğine rağmen, saldırganların bir ağ hakkında önemli bilgiler elde etmesine ve bu bilgileri doğrudan saldırılarda kullanmasına izin veren bazı ICMP mesaj türleri vardır. Diğer taraftan, güvenlik ağ geçidi üzerinde ICMP'yi tamamen engellemeye yönelik radikal yaklaşımlara gidilirse, ağ üzerinde yaşanan sorunların teşhisinde zorluk yaşanması gibi başka istenmeyen durumlar da oluşabilir. Bu nedenle ihtiyaç doğrultusunda, seçici ICMP filtrelemesi hem güvenlik duvarında hem de yerel paket filtresinde kullanılabilir. Uygulama esnasında, sistemin ya da istemcilerin ihtiyaçları göz önünde bulundurulmalıdır. Örneğin, iç ağ için harici ağa nazaran daha fazla sayıda ICMP mesaj türüne izin verilebilir.

Uygulama ve gözden geçirme

Kullanılan işletim sisteminin türüne bağlı olarak filtreleme ve log tutma özellikleri değişiklik gösterebilir. Yerel bir paket filtresi kurmadan önce mevcut dokümanların incelenmesi tavsiye edilir.

Paket filtre kurallarını ayarlarken dikkatli olunmalıdır. Çünkü kural hatası, istemcinin normalde erişebilmesi gereken bir kaynağa/hizmete erişememesine, ağ üzerinden bağlanarak istemcide çalışan bir sistem yöneticisinin sisteme erişimini kaybetmesine neden olabilir ve sonuç olarak istemci konsolundan yerel olarak bağlanarak düzeltmeler yapması gerekebilir.

Yerel paket filtresi devreye alındıktan sonra, bir yandan gerekli hizmetlerin hala ulaşılabilir olup olmadığı diğer yandan bir port taraması yaparak portların geriye kalanlarının devre dışı olup olmadığı kontrol edilmelidir.

BTS.2.U32 Açıklıklara karşı ek koruma tedbirleri (GBE)

İstemci özelindeki güvenlik gereksinimlerine bağlı olarak istemci üzerinde yer alan mevcut güvenlik işlevleri yeterli olmayabilir. Bu nedenle, ek güvenlik ürünlerinin kullanılması gerekebilir. Bunlara örnek olarak; erişim kontrolü, erişim hakları yönetimi ve doğrulama, loglama veya şifreleme ürünleri verilebilir.

İstemciler için, en temel olarak aşağıdaki maddeler sağlanmalıdır:

- İstemciyi sadece yetkili kişiler kullanabilmelidir. Bu amaçla uygun kimlik doğrulama mekanizmaları tercih edilmelidir.
- Kullanıcılar, yalnızca görevlerini yerine getirebilmek için gereken veriye erişebilmeli, uygun kullanıcı ayrıştırılması ve kullanıcı haklarının tahsisi sağlanabilmelidir.
- Usulsüzlükler ve manipülasyon girişimleri fark edilebilir olmalıdır. Log tutma, şifreleme ve dijital imza ile bunlar sağlanabilir.
- Veriler; kazara silinmelere, imha edilmelere veya kontrolsüz kayıplara karşı korunmalıdır (erişilebilirlik kontrolü). Örnek olarak yedekleme ürünleri bunu sağlayabilir.

İstemcilerdeki loglama seçenekleri yeterli kanıt elde etme konusunda ihtiyacı karşılamıyorsa, bu özellik güçlendirilmelidir. Bunu gerektiren yasal düzenlemeler ve kanunlar da bulunmaktadır. Örneğin kişisel verilere dair; "veri işleme sistemlerinde kişisel verilerin girilip girilmediğinden, değiştirilip değiştirilmediğinden veya kimin tarafından girildiğinden veya değiştirildiğinden emin olunması sağlanmalıdır".

Eğer BT sistemindeki belirli verilere bir sistem yöneticinin erişmesini kontrol etmek, engellemek ya da en azından bu erişimi loglara kaydetmek mümkün değilse, o zaman bu veriler şifrelenerek en azından doğru anahtara sahip olmayan sistem yöneticilerinin veriye erişmesi engellenebilir.

Önerilen minimum işlevsellik

İstemciler en azından aşağıdaki güvenlik özelliklerine sahip olmalıdır. Bunlar standart olarak mevcut değilse, bunu sağlamak için ek güvenlik ürünleri alınmalıdır.

- Tanımlama ve Kimlik Doğrulama: Belirli bir sayıda başarısız kimlik doğrulama girişiminden sonra istemci kendini kilitlemeli ve kilitlenen hesabı sadece BT sorumlusu açabilmelidir. İstemcilerde oturum açmak için kullanılan parola, en az sekiz karakter uzunluğunda olmalı ve bu parola sistem kaynaklarında şifrelenmemiş olarak saklanmamalıdır.
- Yetki yönetimi ve kontrolü: En azından okuma ve yazma erişiminin ayırt edilmesi için, sabit diskler ve dosyalar üzerinde bir yetki yönetimi ve kontrolü olmalıdır. Standart kullanıcıların işletim sistemi hizmetlerine ve dosya sistemine erişimleri olmamalıdır.
- Yönetici ve standart kullanıcı arasındaki rol ayrımı: İstemci üzerindeki yetkilerinden dolayı yönetici ve kullanıcı arasında net bir ayrım yapılmalıdır. Bu yetkileri de yalnızca yöneticiler atayabilir veya kaldırabilir olmalıdır.
- Oturum açılması, kapatılması ve hak ihlalleriyle ilgili girişimler kayıt altına alınabilir olmalıdır.

Bu güvenlik özelliklerinden bir veya daha fazlası işletim sistemi tarafından desteklenmiyorsa, bunları sağlayan ek güvenlik ürünlerinin kullanılması tavsiye edilmektedir.

Güvenlik ürünleri için ek gereksinimler şunlardır:

- Kullanıcılar tarafından hızlı bir şekilde kabul görmesi için kullanıcı dostu bir ara yüze sahip olmalıdır,
- BT operasyonları ve kullanıcıları için bilgilendirici ve anlaşılır dokümanlara sahip olmalıdır.

Güvenlik ürünleri için sahip olması beklenen ek özellikler:

- Yönetici, denetçi ve normal kullanıcı arasında rol ayrımı yapılabilmelidir. Sadece yönetici ayrıcalık atayabilir veya iptal edebilir olmalıdır. Ayrıca yalnızca denetçinin günlük (log) verilerine erişimi olmalıdır.
- Yönetici işlemleri kayıt altına alabilmelidir.
- Yapılandırılabilir filtre fonksiyonları ile protokolleri desteklemelidir.
- Verileri uygun bir şifreleme algoritmasıyla şifreleyebilmeli ve bir arıza durumunda veri kaybını (elektrik kesintisi, iptal) engelleyebilmelidir.

Bu işlevlerin gerçekleştirilmesi hem donanım hem de yazılım ile sağlanabilir.

Geçici çözüm

Uygun bir güvenlik ürününün kısa sürede temin edilmesi mümkün değilse geçici olarak alternatif güvenlik çözümlerinin uygulanması tavsiye edilir. Alternatif çözümler daha çok idari kurallar ile sağlanabilir.

BTS.2.U33 Uygulama beyaz listesi (GBE)

İstemcilerin, çalışmalarını yürütebilmek için sadece gerekli olan temel uygulamaları çalıştırabilme yetkisine sahip olması beklenir. Beyaz liste tekniği ile yalnızca izin verilen programların yürütülmesi sağlanır. Beyaz liste tekniğini uygulayabilmek için kullanılabilecek özel mekanizmalar ve üçüncü taraf çözümler bulunmaktadır.

Basit bir yaklaşım ile dosya yolu kullanılarak beyaz liste tekniği uygulanabilir. Örnek olarak çalışmasına izin verilen uygulamalara, işletim sistemi dosyalarına ve onun altındaki program dizinlerine çalışabilir izni verilir. Bunun dışında geriye kalan bütün dizinlerin dosya çalıştırma yetkisi kaldırılır. Bu sayede, kötü amaçlı bir programın tarayıcı önbelleğinden veya geçici dosyaların bulunduğu “temp” klasöründen çalışması engellenmiş olur.

Alternatif olarak, uygulamalar için çalışma izni tek tek manuel olarak verilebilir. Bu güvenlik yaklaşımında sadece önceden tanımlanmış uygulamalar çalıştırılabileceği için, bir güvenlik katmanı daha eklenmiş olacaktır. Bu yöntemin olumsuz tarafı ise, gerekli olan tüm işletim sistemi bileşenlerinin yürütülebilmesine ihtiyaç duyulacağı için fazla çaba gerektirecek olmasıdır. Ayrıca güncellemelerden sonra beyaz listedeki değişen programları yenileme ihtiyacı, beraberinde ek çaba ve iş yükü getirecektir.

BTS.2.U34 Uygulama izolasyonu (GBE)

Farklı işletim sistemleri, uygulamaların izole edilebilmesi için farklı seçenekler sunar. Bunlar arasında AppContainer (Windows), Linux Containers (LXC) veya Docker gibi konteyner çözümleri ve Hyper-V (Windows), KVM / Xen (Linux), VMware Workstation veya Virtualbox gibi işletim sistemleri tarafından sağlanan sanallaştırma çözümleri yer alır. Ayrıca, başka üreticilerin özel çözümleri de bulunabilir. Uygulama izolasyonu; internet içeriğini kullanan veya harici sitelerden veri açan uygulamaları diğer uygulamalardan ve sistem kaynaklarından izole ederek, önemli ölçüde güvenlik sağlar.

BTS.2.U35 Kök sertifikaların aktif yönetimi (GB)

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

BTS.2.U36 Güvenli önyükleme ve TPM yongası kullanımı (B)

UEFI uyumlu sistemlerde, önyükleyici, sistem çekirdeği ve gerekli tüm aygıt yazılım bileşenleri, öz kontrol mekanizmasına sahip anahtarlar tarafından imzalanmalı ve gereksiz anahtarlar devreden çıkarılmalıdır. TPM yongası, gerekli olmadığı durumda devre dışı bırakılmalıdır.

BTS.2.U37 Yetkisiz oturum açma olaylarına karşı korunma(GBE)

Bir saldırgan tarafından ele geçirilmiş kimlik bilgileriyle istemciye erişimi engellemek için, çok faktörlü kimlik doğrulaması kullanılmalıdır.

BTS.2.U38 Acil durum eylem planlaması(E)

Acil durumlara hazırlık kapsamında, istemcideki bir sorunun olumsuz sonuçlarını en aza indirmek için olumsuzluk durumunda neler yapılması gerektiğiyle ilgili bir plan yapılmalıdır.

Bu plan yapılırken aşağıdaki hususlar dikkate alınmalıdır:

- İstemciler için acil durum planlaması mevcut acil durum planına entegre edilmelidir.

- Bir sistem hatası veri kaybına neden olabilir. Bu nedenle, genel veri koruma planlamasının bir parçası olarak, istemciler için bir veri koruma planlaması oluşturulmalıdır.
- Bakım ve servis sözleşmeleri kapsamında yedek parça, belirli bir süre içinde temin edilebilmelidir.
- Sistem yapılandırması kayıt altına alınmalıdır. Bu sayede sistemin yapılandırması hakkında önceden bilgi sahibi olunmasa dahi acil durum esnasında sistemler geri yüklenebilir.

Acil durum önyükleme ortamı oluşturulması

Bir istemciyi sıfırdan kurmak için, kötü amaçlı bir yazılım sisteme zarar verdiğinde sistemi kurtarmak için veya bir sabit sürücü arızası durumunda sistemi başlatabilmek için bir önyükleme medyası hazır olarak bulundurulmalıdır. Bu medya, işletim sistemleri ilk kez kurulurken hazırlanabileceği gibi, daha sonradan da ayrıca hazırlanabilir. Acil durum önyükleme ortamının kapsamı ve içeriği, istemcinin durumuna göre değişkenlik gösterebilir.

Acil durum önyükleme ortamı aşağıdaki problemler için kullanılabilir:

- Yanlış kullanım nedeniyle veri kaybı,
- Kullanımı ve yeniden başlatmayı engelleyen işletimsel ve yönetimsel hatalar,
- Sisteme zararlı yazılımların bulaşması,
- Sistemin bir saldırgan tarafından ele geçirilmesi,
- Donanım sorunları.

Aşağıdaki programlar acil önyükleme ortamı için "temel bileşenler" olarak önerilir:

- Güncel imzalara sahip zararlı yazılımlardan korunma programları,
- Sistemin yapılandırma dosyalarını veya veri tabanlarını düzenlemek için gerekli programlar (dosyalar, kayıt defteri veya benzerleri için editörler),
- Önyükleme sektörünü ve sistem diskinin MBR'sini (Ana Önyükleme Kaydı) geri yükleme programları,
- Yedekleme / kurtarma programları,
- Donanım hatalarını analiz etmek için tanılama/teşhis programları,
- Ek olarak, güvenliği ihlal edilmiş bir sistemin adli soruşturması gibi daha detaylı analiz için gerekli olacak yardımcı programlar eklenebilir.

Tüm programların ve uygulama kütüphanelerinin yalnızca önyükleme ortamından yüklenilebilir olması önemlidir. Kurulu sistemdeki bileşenlerin kullanılamaz olabileceği göz önünde bulundurulmalıdır. Önyükleme ortamı oluşturulurken, bilgisayarın sabit

disklerine erişmek için gereken tüm programlar da medya içerisinde yer almalıdır (ör: sabit disk denetleyicileri için sürücüler ve sabit disk şifreleme veya sabit disk sıkıştırma için programlar, vb.)

Önyükleme medyasında, istemci konfigürasyon dokümanı da güncel olarak bulunursa, hata ayıklama verimliliği artırılabilir.

Acil durum önyükleme ortamının kendisi virüslerden ve diğer kötü amaçlı yazılımlardan arındırılmış olmalıdır. Bu nedenle, sadece güvenilir kaynaklardan (ör. doğrudan üreticiden) gelen veya dijital imzası kontrol edilen programlar önyükleme medyasında yer almalıdır. Önyükleme medyasını ilk defa oluştururken ve daha sonra yapılan her değişiklikte, medya zararlı yazılımlardan korunma programı ile mutlaka tekrar taranmalıdır.

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

İşletim sistemi yapılandırması veya güncellemesi gerekirse, acil durum önyükleme medyası ve içerisinde saklanan dosyalar da güncellenmelidir.

Acil durum önyükleme medyasının sistem yöneticileri için hızlıca erişilebilir olması gerekir, böylece bir arıza durumunda zaman kaybı en aza indirilmiş olur. Öte yandan yetkisiz kişilerin bu bilgilere erişimi olmaması için medya güvenli bir yerde saklanmalıdır.

BTS.2.U39 Kesintisiz güç kaynakları (E)

İstemcilerin kullanılabilirlik gereksinimleri yüksek ise bir kesintisiz güç kaynağına (UPS) bağlanmaları önerilir. Bu şekilde; elektrik kesilmesi halinde ya güç kaynağı devreye girene kadar ya da istemciler düzgün bir şekilde kapatılana kadar enerji sağlanarak istemciler hizmet verebilir. Kesintisiz ve sabit bir güç kaynağı hakkında daha ayrıntılı bilgi, BTS.1 Sunucu Yönetimi için uygulama notlarında bulunabilir.

BTS.2.U40 İşletim belgeleri (EB)

Sorunsuz bir işletim sağlayabilmek için sistem yöneticilerinin elinde, sistemlerin ve altyapının genel bir dokümantasyonun olması gerekir. Sistem yöneticilerine beklenmedik bir şekilde ulaşılamaması durumlarında kullanılmak üzere bu genel tanım, ilgili diğer personeller tarafından erişilebilir olmalıdır. Bu genel tanım, sistem kontrollerini gerçekleştirebilmek için de gereklidir (ör. Problemli ayarların kontrolü ve değişiklik durumunda tutarlılık kontrolü gibi).

Bu nedenle, yöneticilerin istemcide yaptıkları değişiklikler mümkünse otomatik olarak kayıt altına alınmalıdır. Sistem dizinleri ve dosyalarında yapılan değişikliklerde bu durum özellikle önemlidir.

Yeni işletim sistemleri kurarken veya mevcut işletim sistemlerini güncellerken, yapılan değişiklikler hassasiyetle ele alınmalı ve yapılan bütün değişiklikler kayıt altına alınmalıdır. Sistem parametreleri değiştirildiğinde bir istemcinin güvenlik özellikleri de dahil olmak üzere sistem fonksiyonlarının önemli ölçüde değiştirilmiş olabileceği göz önünde bulundurulmalıdır.

BTS.2.U41 Depolama alanlarını kapasite aşımından koruma (E)

İstemciler için sabit disk kotaları ayarlanırken, sabit disk kullanımında kullanıcıyı belirli bir disk aşım seviyesinde uyarabilen veya sadece yönetici rolüne sahip kullanıcılara yazma izni verebilen işletim sistemi mekanizmalarının kullanılabileceği dikkate alınmalıdır.

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: 05 Ocak 2020].

- keytool - Anahtar ve Sertifika Yönetim Aracı, Oracle, 2017. [Çevrimiçi]. Erişim: https://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html, [Erişim tarihi: 05 Ocak 2020]

- Mozilla CA: Sertifika Değişikliği Süreci, Mozilla Wiki. [Çevrimiçi]. Erişim: https://wiki.mozilla.org/CA:Root_Change_Process, [Erişim tarihi: 05 Ocak 2020]

- Güvenilen Kökleri ve İzin Verilmeyen Sertifikaları Yapılandırma, Microsoft, 2017. [Çevirimiçi]. Erişim: https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx [Erişim tarihi: 17 Eylül 2019].

- Son Kullanıcı Cihazları İçin Depolama Şifreleme Teknolojileri Kılavuzu, NIST Özel Yayın 800-111, Kasım 2007. [Çevrimiçi]. Erişim: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf, Son Erişim: 15/11/2019

- 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].

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
BTS.2.U1	Kullanıcı kimlik doğrulaması	Kullanıcıların parola kullanımını düzenleyen bir politika var mı?
		Kullanıcılar için yeterli karmaşıklıkta parola oluşturmalarına yardımcı olacak 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, fazla yetkilerin kaldırılması için bu durumun takibi yapılıyor mu?
		Geçici kullanıcı hesaplarının erişim yetkileri ile ilgili bir politika mevcut mu?
BTS.2.U2	Rollerin ayrıştırılması	Sistem yöneticileri ile standart kullanıcı rolleri

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		için farklı yetkilendirmeler yapıldı mı?
		Sistem yöneticilerine, sadece sorumlu olduğu alana dair yetkiler tanımlandı mı?
BTS.2.U3	Otomatik güncelleme mekanizmalarının etkinleştirilmesi	İstemcilerin herhangi bir otomatik güncelleme mekanizmasına sahip olup olmadıkları kontrol edildi mi?
		Güncellemelerin otomatik olarak veya son kullanıcı tarafından yüklenmesi seçeneği kurum gereksinimlere göre belirlendi mi?
		Kurumun yama ve değişim yönetimi stratejisine uygun olacak şekilde otomatik güncelleme mekanizmaları tanımlandı mı?
		Kritik güvenlik güncellemeleri için ayrı bir prosedür mevcut mu?
BTS.2.U4	Düzenli yedekleme	Yedeklerin depolandığı alanlar yetkisiz erişime karşı korunuyor mu?
		Yedeklerin saklandığı alanlar canlı sistemlerden ayrı tutuluyor mu?
		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?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Kullanıcılar, yedekleme politikası hakkında bilgilendiriliyor mu?
		Yedekten dönüş testleri düzenli olarak yapılıyor mu?
BTS.2.U5	Ekran Kilidi [Kullanıcı]	Tüm çalışanlar manuel ekran kilidi kullanımı hakkında bilgi sahibi mi ve aktif olarak kullanıyor mu?
		Hem kullanıcı hem de güvenlik ihtiyaçlarını dikkate alan otomatik ekran kilidi tanımlanmış mı?
BTS.2.U6	Zararlı yazılımlardan koruma programlarının kullanımı	Güvenlik politikasına uygun olarak, gerekli tüm istemcilerde 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?
		İnternet üzerinden bulaşabilecek zararlı yazılımlara karşı yeterli koruma sağlanıyor mu?
		Bir zararlı yazılım tespit edildiğinde, sistemin bütünü kontrol edilir mi?
		Zararlı yazılım tespit edilirse: zararlı yazılımın istemcilerde mevcut gizli verilere erişip erişmediği, koruma yazılımlarının işlevselliklerini devre dışı bırakıp bırakmadığı kontrol edilir mi?
		Veri alışverişi esnasında zararlı yazılımlardan

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		koruma sağlanıyor mu?
		Şifrelenmiş verilerin zararlı yazılımlardan korunduğu garanti ediliyor mu?
		Kullanıcıların, zararlı yazılımlardan koruma programlarının ayarlarında herhangi bir değişiklik yapabilmeleri engellendi mi?
BTS.2.U7	Loglama	İstemcilerde gerçekleştirilen işlemlerin logları tutuluyor mu?
		Loglar düzenli olarak değerlendiriliyor mu?
		Yapılan değerlendirmelerin sonucu kayıt altına alınıyor mu?
		Logların saklama süreleri için ilgili yasa ve mevzuatlar dikkate alındı mı?
BTS.2.U8	Önyükleme işleminin korunması	Planlanandan başka kaynaklardan önyükleme yapılmasını engelleyen teknik önlemler var mı?
		Sadece yetkili personelin acil durum önyükleme medyasına erişebilmesi sağlandı mı?
		Önyükleme ortamı oluşturulduktan sonra test ediliyor mu?
		Acil durumlarda kullanılmak üzere oluşturulan önyükleme ortamı oluşturulduktan sonra veya bu ortam üzerinde değişiklik gerçekleştirildikten sonra kötü amaçlı yazılım taraması yapılıyor mu?
		Önyükleme medyasının içeriği yazılı halde

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		tutuluyor mu?
BTS.2.U9	İstemciler için bir güvenlik politikası oluşturulması	İstemciler için mevcut bir güvenlik politikası var mı?
		İstemciler için hazırlanan güvenlik politikası, istenen güvenlik seviyesine ulaşmak için gerekli olan tüm stratejileri, gereksinimleri ve düzenlemeleri içeriyor mu?
		Güvenlik politikasının içeriği düzenli olarak güncelleniyor ve uygulamalarının kontrolü periyodik olarak denetleniyor mu?
BTS.2.U10	İstemci işletiminin planlanması	Bir istemci yönetim planı yapıldı mı?
		BT güvenlik hedefleri, görevler ve fonksiyonlar gibi tüm gereksinimler planlama öncesinde dikkate alındı mı?
BTS.2.U11	İstemcilerin tedarik edilmesi	İstemciler tedarik edilmeden önce, istemcide bulunması gerekli tüm özelliklerin mevcut olduğu bir talep listesi hazırlandı mı?
BTS.2.U12	Yazılımın uyumluluk kontrolü	Yazılımlar için uyumluluk kontrolü, test ve onay sürecine entegre edilmiş midir?
BTS.2.U13	Kod çalıştırılabilen ortamlara erişim	Kod çalıştırılabilen ortamlara erişim için gerekli güvenlik önlemlerinin yerine getirilmesiyle ilgili kontroller, kurum güvenlik politikasında belirtildi mi?
BTS.2.U14	Güncellemeler ve yamalar	Tüm organizasyon genelinde yama ve değişiklik yönetiminden sorumlu kişiler belirlendi mi?
		Etki alanı yüksek olan değişiklerde Bilgi

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		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?
BTS.2.U15	İstemcilerin güvenli kurulumu ve yapılandırılması	Kritik istemcilerde, konfigürasyon ve log dosyaları gibi alanlara erişim parola ile korunuyor mu?
		BT ağına, sadece izin verilen arayüzlerden ve uygulamalardan mı erişim sağlanıyor?
		İstemcide kritik hizmetlere her erişim için parola ile kimlik doğrulaması yapılıyor mu?
		İstemcide güvenlik ile ilgili loglar düzenli olarak tutuluyor mu?
		İstemcilerin güvenli kurulumu için fonksiyonel gereksinimleri ve güvenlikle ilgili özellikleri dikkate alan bir kurulum konsepti mevcut mu?
		Kurulum konsepti, kurulum için yapılması

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		gerekli konfigürasyonları içeren adım adım açıklamaların bulunduğu bir doküman içeriyor mu?
		Kurulum konsepti içerisinde, çevirimdışı kurulum yapılırken gerekli güvenlik tedbirleri ile ilgili bir politika mevcut mu?
		Kullanıcı hesapları oluşturulurken bu hesapların yetkileri gereksinimlere göre tanımlandı mı?
BTS.2.U16	Gereksiz bileşenlerin ve kullanıcı hesaplarının kaldırılması	Kullanımı sona eren hesapların yetkileri alınıyor ve bu hesaplar devre dışı bırakılıyor mu?
		Kullanılmayan kullanıcı hesapları, servisler ve uygulamalar devre dışı bırakılmış veya kaldırılmış mı?
		Kullanıcı hesaplarına tanımlanan yetkiler kayıt altına alındı mı?
BTS.2.U17	Kullanıma sunma	Kullanıma sunulacak istemcilerin yetkilendirme, yönetim, izleme ve loglama vb. açılardan hangi düzeyde ve nasıl olacağıyla ilgili kavramlar düzenli olarak gözden geçiriliyor mu?
BTS.2.U18	İletişim bağlantılarının şifrelenmesi	İstemciler, TLS'in güvenli versiyonunu destekliyor mu?
		İstemcilerin başka BT sistemleri ile yaptıkları bütün bağlantılar mümkünse TLS protokolü ile şifreleniyor mu?
		Güvenilir bir sertifika otoritesi seçimi yapıldı

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		mı?
		SSL/TSL sertifikaları canlı ortamda kullanılmadan önce sertifikada hata olup olmadığı kontrol edilip, sertifikanın durumu periyodik aralıklarla doğrulanıyor mu?
BTS.2.U19	Kısıtlayıcı hakların tahsisi	Yetkili kullanıcı hesaplarının gerekli uygulamalara ve BT sistemlerine erişebilmeleri sağlandı mı?
		İstemcilerde erişim yetkilerinin kısıtlandırılması gerçekleştiriliyor mu?
		Sistem dosyalarına erişim, sadece yetkili sistem yöneticileri ile sınırlandırıldı mı?
		İstemciler, yalnızca yetkili kullanıcılara gerekli ayrıcalıkları sağlayacak şekilde yapılandırıldı mı?
		Kullanıcılara erişim haklarının verilmesi sırasında kurum güvenlik politikası dikkate alınıyor mu?
		Sistem dosyalarına, hangi uygulamaların ve kullanıcıların, ne zaman erişim yaptığı kayıt altına alınıyor mu?
		İstemcilerin yönetimi için kullanılan yöntemler güvenlik politikasında tanımlandı mı?
BTS.2.U20	Yönetim ara yüzlerinin korunması	Yönetim amaçlı yapılan bağlantılarda kullanılan protokoller ve yöntemler güncel teknolojiye uygun mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		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.2.U21	İstemci mikrofon ve kameralarının yetkisiz kullanımının önlenmesi	İstemcilerde dahili olarak bulunan kamera ve mikrofonların kurumsal olarak kullanımına ihtiyaç olup olmadığı değerlendirildi mi?
		Kullanım ihtiyacı olmayan dahili kamera ve mikrofonların iptal edilmesi, kullanılmadığı zamanlar kapatılması, etiketle kapatılması veya tamamen istemciden çıkartılması değerlendirildi mi?
		İstemcilerde bulunan kamera ve mikrofon aygıtlarına diğer yazılımların erişimi kontrol edilir mi?
BTS.2.U22	Oturumun kapatılması [Kullanıcı]	Tüm kullanıcılar, işlemlerini tamamladıktan sonra uygulamalardan ve BT sisteminden oturumlarını kapatarak çıkması konusunda bilgilendiriliyor mu?
		Kullanıcılar istemci üzerinde bir işlem yapmadıklarında, ekran kilidinin otomatik olarak devreye girmesi sağlanır mı?
		İstemcinin uzun süreli kullanılmadığı durumlarda oturumun güvenli bir biçimde otomatik olarak sonlandırılması sağlanır mı?
BTS.2.U23	İstemci-sunucu hizmetlerinin kullanımı	Kurum içerisinde hangi verilerin hangi istemci-sunucu hizmeti ile sağlandığı (yazıcı,

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		dosya paylaşımı, anlık mesajlaşma, VoIP, vs.) belirlenip kayıt altına alındı mı?
		Taraflar (istemci-sunucu) arası hizmetlerin yetkisiz kullanımını (kişi, bilgi, hizmet) engellemek için gerekli önlemler alındı mı?
		Taraflar arası hizmetlerin kullanımını kapsayan bir politika var mı?
		Taraflar arası hizmetlerin kullanımı yönetim tarafından onaylandı mı? Riskler kabul edilip belgelendi mi?
BTS.2.U24	Çıkarılabilir medyanın kullanımı	Çıkarılabilir medya ve harici veri depolama cihazlarının yönetilmesini düzenleyen bir kılavuz var mı?
		Çıkarılabilir medyanın yanlış kullanılmasını engelleyen teknik önlemler var mı?
		Harici cihazların ve veri ortamlarının izinsiz bağlanmasını önleyen teknik önlemler var mı?
		Takılı çıkarılabilir veri medyasının içeriğinin otomatik yürütülmesi engellendi mi?
		Tüm kullanıcılar çıkarılabilir medya ve harici veri depolama cihazları için sürücülerle ilgili tüm kurallardan haberdar edildi mi?
BTS.2.U25	BT güvenli kullanım politikası [Kullanıcı]	Güvenlik seviyelerini tanımlayan bir istemci güvenlik politikası var mı?
		Güvenlik politikasında tanımlanan kontrollerin istemcilerde uygulanıp uygulanmadığı düzenli

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		olarak kontrol ediliyor mu?
BTS.2.U27	İstemcinin kontrollü olarak hizmet dışı bırakılması	İstemciler hizmet dışı bırakılmadan önce, istemcilerin bağımlılıkları ve mevcut bilgilerin kullanılabilirliği dikkate alınıyor mu?
		İstemciler kullanım dışına ayrılmadan önce, istemcinin hizmet dışına çıkartılmasıyla ilgili detaylı bir planlama yapılıyor mu?
BTS.2.U28	İstemcilerin şifrelenmesi	Disk şifrelemesi kullanılıyor mu?
		Windows altındaki normal kullanıcılara erişim hakları ve yükleme yetenekleri kısıtlı şekilde verildi mi?
		Veri içeren medyalar kaybolduğunda veya imha edildiğinde ilgili tüm anahtarlar ve parolalar yok edilir mi?
		Standart kullanıcılara yönelik sistem bölümlerine yazma erişimi engellendi mi?
		İstemci başlatılırken şifreleme uygulaması (ör. Bitlocker) ile kullanmak için kurum gereksinimlerine uygun bir kullanıcı kimlik doğrulama yöntemi kullanıldı mı?
		Kurtarma şifresi ve kurtarma anahtarı gizli ve dikkatli bir şekilde korunuyor mu?
		Kullanıcılar kimlik doğrulama kaynaklarını kaybederlerse nasıl bir süreç işleteceklerini biliyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		İhtiyaç durumunda, disk şifreleme yazılımı kurtarma şifrelerine ve kurtarma anahtarlarına erişebilir mi?
BTS.2.U29	Sistem izleme (E)	İstemcilerin izlenmesine yönelik bir politika mevcut mu?
		İstemciler, değişik sistem ve güvenlik olaylarına karşı merkezi bir izleme aracı ile izleniyor mu?
		İstemcilerin izlenmesi sürecinde; hangi bildirimlerin kime, ne zaman ve hangi iletişim kanalı ile iletileceği netleştirilmiş mi?
BTS.2.U30	Referans sistem kurulumu (GBE)	İstemciler için dokümante edilmiş bir referans ortamı var mı?
		Referans sistemle ilgili yapılacak testler için kontrol listeleri var mı?
BTS.2.U31	Yerel güvenlik duvarı kullanımı (GBE)	Merkezi güvenlik duvarının yanı sıra istemcilerin ek güvenlik tedbirleri kapsamında yerel güvenlik duvarı/paket filtresi ile korunmasına yönelik bir politika mevcut mu?
		Güvenlik duvarında kısıtlayıcı strateji uygulanıyor mu?
		Güvenlik duvarı kullanım politikası oluşturuldu mu?
		Güvenlik duvarının yapılandırılması için temel bir konfigürasyon mevcut mu?
		ICMP filtrelemesi yapılıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Güvenlik duvarı kuralları düzenli olarak kontrol ediliyor mu?
BTS.2.U32	Açıklıklara karşı ek koruma tedbirleri (GEB)	Güvenlik kontrollerinin uygulanması ve sonuçları belgelendi mi?
		Güvenlik kontrolleri düzenli olarak gerçekleştiriliyor mu?
		Güvenlik kontrollerinde tespit edilen açıklıklar için gerekli önlemler alındı mı?
BTS.2.U33	Uygulama beyaz listesi (GBE)	Uygulama beyaz listesi kullanımının kurum güvenlik gereksinimlerini sağlamak için gerekli olup olmadığına karar verildi mi?
		İstemciler üzerinde yalnızca izin verilen uygulamaların çalıştırılmasına yönelik bir planlama yapıldı mı?
BTS.2.U34	Uygulama izolasyonu	Uygulama izolasyonu yönteminin kurum güvenlik gereksinimlerini sağlamak için gerekli olup olmadığı analiz edildi mi?
BTS.2.U35	Kök sertifikalarının aktif yönetimi	İstemcilerin gerekli hizmetleri güvenli bir şekilde alabilmesi için hangi kök sertifikalarına sahip olması gerektiği belirlendi mi?
BTS.2.U38	Acil durum eylem planlaması(E)	İstemcilerde meydana gelebilecek bir arıza için acil durum planı var mı?
		Acil durumlarda istemcileri kontrollü bir şekilde başlatabilmek için mevcut bir

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		önyükleme ortamı var mı?
		Arızalanan sistemlerdeki verilerin korunmasına yönelik bir planlama mevcut mu?
		Acil durum eylem planları düzenli olarak test ediliyor mu?
BTS.2.U39	Kesintisiz güç kaynakları	Kesintisiz güç kaynağının gücü ve açık kalma süresi ile ilgili gereksinimleri sağlayıp sağlamadığının kontrolü yapıldı mı?
BTS.2.U40	İşletim belgeleri	İstemcilerin işletiminin sağlıklı bir şekilde gerçekleştirilebilmesi için BT mimarisinin genel bir özeti belgelendirildi mi?
BTS.2.U41	Depolama alanlarını kapasite aşımından koruma	Kurum gereksinimlerine uygun olarak, depolama alanlarını kapasite aşımından korumak için kullanıcı ve uygulama verilerini arşivlemek amacıyla bir düzenleme var mı?

TÜBİTAK BİLGEM
Yazılım Teknolojileri Araştırma Enstitüsü

Çukurambar Mah. Malcolm X Cad. No: 22 06100 Çankaya - ANKARA
T 0312 284 92 22 **F** 0312 286 52 22
E epid.yte@tubitak.gov.tr

www.yte.bilgem.tubitak.gov.tr
www.dijitalakademi.gov.tr