BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ

TEMEL SİBER GÜVENLİK GEREKSİNİMLERİ

(TASLAK)

Rev: 0.2

Yayın Tarihi: 19 EKİM 2017

P.K. 74, 41470 Gebze / KOCAELİ
Tel: (0262) 648 10 00, Faks: (0262) 648 11 00
www.bilgem.tubitak.gov.tr
bilgem@tubitak.gov.tr

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

TANIMLAR

APT	Advanced Persistent Threat (Gelişmiş Siber Tehdit)
ASD	Australian Signals Directorate
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BT	Bilişim Teknolojileri
CD	Compact Disc
COBIT	Control Objectives for Information and Related Technology
DDOS	Distributed Denial of Service
DMZ	DeMilitarized Zone
DSS	Data Security Standard
DVD	Digital Versatile Disk
HTTPS	Secure Hypertext Transfer Protocol
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
OT	Operational Technology
PCI	Payment Card Industry
RDP	Remote Desktop Protocol
SANS	SysAdmin, Audit, Network and Security
SATA	Serial Advanced Technology Attachment
SIEM	Security Information and Event Management
SPF	Sender Policy Framework
SSH	Secure Shell
SQL	Structured Query Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
TS	Türk Standardı
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UK	United Kingdom
USB	Universal Serial Bus
VNC	Virtual Network Computing
XSS	Cross Site Scripting

1. GİRİŞ

Bu doküman, T.C. Kalkınma Bakanlığı desteği ile yürütülen Siber Güvenlik Eğitim ve Araştırma Projesi hedefleri doğrultusunda TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü tarafından hazırlanmıştır. Tüm dünyada kurum ve kuruluşlar, büyük miktarda veri kaybı, servis dışı kalmalar, kişisel bilgilerin açığa çıkması, kritik bilgilerin sızdırılması, fikir eserlerinin çalınması gibi çeşitli bilgi güvenliği ihlal olaylarıyla karşı karşıya kalmaktadır. Çok çeşitli tehditlerden kaynaklanan bu gibi ihlal olaylarına karşı elimizde yine çok çeşitli siber savunma araçları ve teknolojileri, güvenlik standartları, güvenlik eğitimleri ve sertifikaları, açıklık veri tabanları, kılavuzlar, iyi uygulamalar, güvenlik kontrol listeleri ve tavsiye edilen önlemler bulunmaktadır. Kurum ve kuruluşlar, tavsiye edilen tüm bu teknolojiler, önlemler, fikirler arasında kaybolmaya başlamıştır. Üstelik güvenlik durumunu geliştirmek isteyen bir kurum veya kuruluş tavsiye edilen birtakım güvenlik önlemlerini alırken, belirli bir insan kaynağı, zaman ve bütçe ile hareket etmek durumundadır. Bu durumda aşağıdaki sorular karşımıza çıkmaktadır:

- Kurum ve kuruluşlar bilgi güvenliğini geliştirmek için nereden başlamalıdır?
- Öncelikli olarak hangi alanlarda ne gibi çalışmalar yapmalıdır?
- Karşılaşılan her ihlal olayına özel bir önlem yerine olası birçok tehdidi karşılayabilecek kapsamda temel önlemler nelerdir?

1.1 Amaç ve Kapsam

Bu dokümanın amacı, kamu kurum ve kuruluşlarının güncel tehdit ve saldırılardan korunmak için uygulayacakları öncelikli güvenlik adımlarını ortaya koymaktır. Bu adımlar siber güvenlik önlemlerini içereceği gibi, diğer birçok güvenlik önleminin alınmasına temel oluşturacak faaliyetleri de kapsamaktadır. Önerilen süreçlerin önceliği, yürütüldüğü durumda kuruma siber güvenlik açısından en çok katma değer sağlayacak güvenlik süreçleri olarak belirlenmiş ve temel siber güvenlik gereksinimleri olarak adlandırılmıştır. Temel siber güvenlik gereksinimleri kamu kurum ve kuruluşları için olduğu gibi, her türlü kurum ve kuruluş tarafından uygulanabilir.

Kurum ve kuruluşlar, olağan kurumsal işleyişlerini ve verdikleri hizmetleri güvenli bir şekilde sürdürmek için hâlihazırda bir takım güvenlik süreçleri yürütmekte ve çeşitli önlemler almaktadır. Bu dokümanda yer alan gereksinimler listesinin kurumların mevcut güvenlik durumlarını değerlendirmelerinde ve bilgi güvenliğini iyileştirmek için yapacakları öncelikli çalışmaları planlamalarında rehberlik etmesi amaçlanmıştır.

Dokümanın devamında dünyada ve Türkiye'de karşılaşılan siber güvenlik tehditleri için genel bilgilendirme yer almaktadır. İkinci bölümde temel güvenlik gereksinimleri tanımlanmakta, önemi ve uygulama adımları anlatılmaktadır.

1.2 Dünyadaki Tehdit Spektrumu

2017 yılında SANS Enstitüsü'nün yayınladığı "2017 Tehdit Durumu Anketi: Kullanıcılar Ön Safta" anket raporuna göre 250'den fazla bilişim teknolojileri ve güvenlik çalışanıyla yapılan anket sonuçlarına göre oluşturulan kurum ve kuruluşlarda meydana gelen başlıca tehdit türleri (alfabetik sırayla) Tablo 1'de yer almaktadır [1].

Tablo 1: Başlıca siber güvenlik tehdit türleri

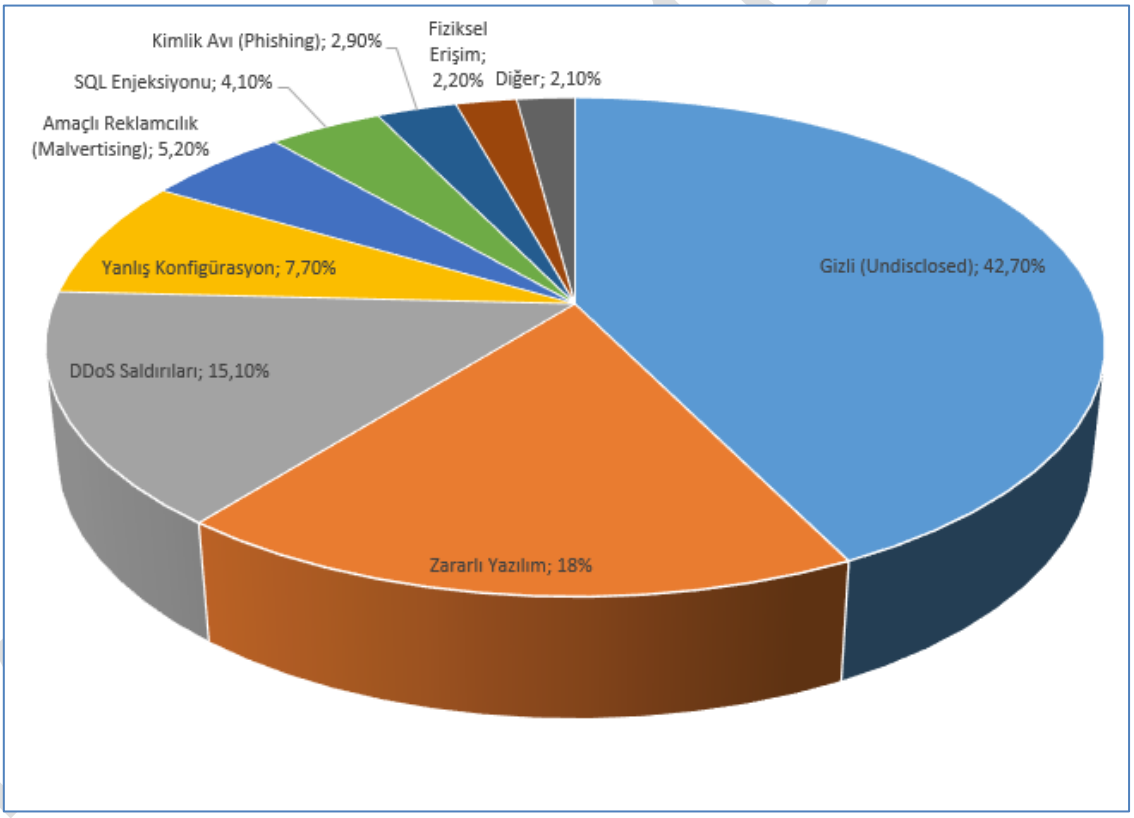
No.	Tehdit Türü
1	Araya Girme Saldırıları
2	Casus Yazılımlar
3	Çekirdek Seviyesindeki Sömürüler
4	Dağıtık Servis Dışı Bırakma Saldırıları
5	Fidye Yazılımlar
6	Gelişmiş Siber Tehditler (APT)
7	Hak Yükseltme
8	Harmanlanmış Tehditler
9	Kimlik Avı ve Hedef Odaklı Oltalama
10	Mobil Zararlı Yazılımlar
11	Polimorfik Zararlı Yazılımlar
12	Rootkitler
13	Solucanlar
14	SQL Enjeksiyonu, XSS ve diğer Web Uygulama Saldırıları
15	Truva Atları
16	Tuş Kaydediciler
17	Zararlı Yazılım İçermeyen Saldırılar
17.1	Bellek Tabanlı Saldırılar
17.2	Betik Saldırıları
17.3	Diğer Cihazların Ele Geçirilmesinden Kaynaklı Saldırılar
17.4	Gizli Kayıt Dosyaları
17.5	HTTPS Şifreleme Seviyesi Düşürme
17.6	İkili Dosyaların Diske Yazılması
17.7	Kimlik Sömürüsü veya Hak Yükseltme
17.8	Tarayıcıdaki Proseslerin Sömürülmesi
17.9	Tarayıcı Dışındaki Proseslerin Sömürülmesi
17.10	Zararlı İkili Dosyalar
18	Zincirleme Sömürüler

Avustralya ASD (Australian Signals Directorate) tarafından hazırlanan “Siber Güvenlik Olaylarını Azaltma Stratejileri – Azaltma Detayları” dokümanına göre kurum ve kuruluşların sıklıkla karşılaştıkları tehdit türleri aşağıda listelenmiştir [2]:

1. **Bilgi çalma hedefli siber tehditler:** Gelişmiş kalıcı tehditleri de içeren bu tehditler yüzünden kurum ve kuruluşların hem rekabet edebilirlikleri hem de kurumsal imajları ciddi bir biçimde etkilenmektedir. Bunun yanı sıra ülkenin ekonomik refahı zarar görebilmekte, kamu görüşü etkilenmekte, vatandaşlar özel bilgilerinin açığa çıkmasından dolayı olumsuz etkilenebilmektedir.
2. **Veriye erişimi ve/veya bilgisayarların/ağların düzgün çalışmasını engelleyen fidye yazılımlar ve diğer dış taraflar:** Fidye yazılımlar alınan yedekleri silebilmekte, diğer bilgisayarlara da bulaşıp, yerel disklerdeki, dosya paylaşımlarındaki ve çıkarılabilir medyadaki verileri şifreleyebilmektedir. Ayrıca işletim sistemi dosyalarını da şifreleyerek bilgisayarların düzgün çalışmasını engelleyebilmektedir.
3. **Kurum içi odaklı olarak bilginin ele geçirilmesini /bozulmasını ve/veya bilgisayarların /ağların düzgün çalışmasının engelleyen tehditler:** Daha fazla para kazanma, intikam alma, baskı, ideolojik vb. motivasyonlarla kurum içi ağlara ve bilgisayarlara erişen kişiler, müşteri/çalışan bilgisi ve/veya kurum tarafından üretilmiş fikri mülkiyetin çalınması şeklinde veri kaçırabilmekte, veriyi yok edebilmekte ve bilgisayarların/ağların düzgün çalışmasını engelleyebilmektedir.
4. **İş e-postalarına yönelik tehditler:** Bu tehdit türü sosyal mühendislik ve hedefli siber nüfuz teknikleri kullanarak hedef kurumun iş süreçlerindeki güven ilişkisini kötüye kullanma prensibine dayanmaktadır. Bu yöntemle ya çok benzer bir e-posta hesabı oluşturularak ya da gönderilen e-postalar ilgili/yetkili personelden gelen bir e-postaymış gibi gösterilerek para transferleri yapılması veya dolandırıcılık amaçlı kullanmak üzere kişisel bilgilerin verilmesi istenmektedir.

5. **Endüstriyel Kontrol Sistemlerine yönelik tehditler:** Endüstriyel Kontrol Sistemleri elektronik sensörler gibi bileşenler ve ağ tabanlı hesaplamalı donanımlar içeren operasyonel teknolojiler (OT) tabanlı sistemlerdir. Bu tür sistemler operasyonel güvenilirlik ve emniyet işlevlerini desteklemek amacıyla endüstriyel ekipmanları izlemekte ve/veya kontrol etmektedir. OT varlıklarının devamlı olarak üretim ortamında hizmet vermesi nedeniyle yaşam süreleri uzamakta ve güncellemeler çok nadir olarak yapılabilmektedir. Bu durum OT varlıklarının siber tehditlere karşı daha savunmasız kalmasına neden olmaktadır.

Dünya genelinde karşılaşılan tehditler analiz edildiğinde ise tehdit türü açısından zararlı yazılımlar ve DDoS saldırıları başı çekmektedir. "IBM X-Force Tehdit İstihbarat Raporu 2016" dokümanına göre dünya genelinde karşılaşılan tehditlerin türlerine göre dağılımı Şekil 1'de verilmiştir [3]. Şekle göre tehdit türlerinin dağılımında %40'tan fazlası gizli tutulmakla birlikte, %18'ini zararlı yazılımlar, %15'ini DDoS saldırıları, %7'sinden fazlasını da yanlış yapılandırmalar oluşturmaktadır.

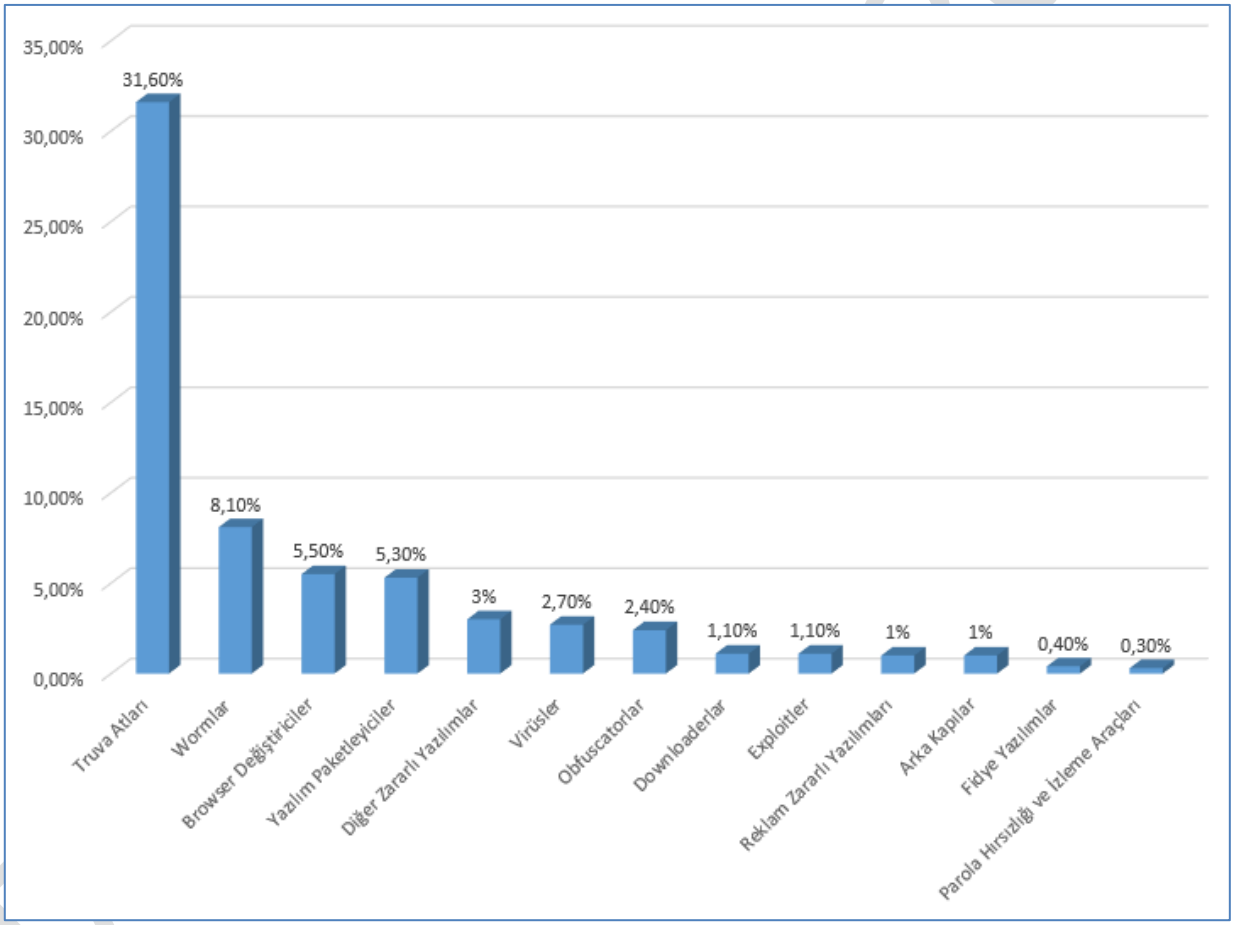


Şekil 1: Dünya genelinde tehditlerin türlere göre dağılımı

1.3 Türkiye'deki Tehdit Spektrumu

ITU tarafından hazırlanan "Global Siber Güvenlik Endeksi 2017" dokümanına göre Türkiye'nin siber güvenlik endeksi 0,581 olarak belirlenmiş olup, bu endekse göre Türkiye 165 üye ülke arasından 43. sırada yer almaktadır [4].

2016 yılında yayımlanan "Microsoft Güvenlik İstihbarat Raporu" dokümanına göre, 2016 yılı ikinci çeyreği itibariyle zararlı yazılım barındıran bilgisayar sayısının raporları alınan bilgisayar sayısına oranı sıralamasında Türkiye %31,4'lük bir oranla dünya ortalaması olan %21,2'lik oranın çok üzerinde yer almaktadır [5]. Raporları alınan bilgisayarlardan toplanan veriler dikkate alındığında Türkiye'deki bilgisayarlarda tespit edilen tehditlerin dağılımı Şekil 2'de yer almaktadır. Şekle göre truva atları zararlı yazılım türleri arasında açık ara başı çekmektedir.



Şekil 2: Türkiye'deki zararlı yazılımları barındıran bilgisayar sayısının rapor edilen bilgisayar sayısına oranı

2013-2014 yıllarında T.C. Kalkınma Bakanlığı desteğiyle Siber Güvenlik Enstitüsü tarafından yapılan "Kritik Altyapılarda Bilgi Güvenliği Yönetimi" projesi kapsamında Türkiye genelinde yaygın hizmet veren kritik kamu kurum ve kuruluşlarıyla görüşmeler yapılmıştır. Bu görüşmeler kapsamında kurum ve kuruluşlara, son beş yıl içinde verdikleri hizmetlerdeki bilginin gizliliğini,

bütünlüğünü veya hizmetin sürekliliğini etkileyen olayların yaşanıp yaşanmadığı sorulmuştur. Bu soruyla, kurum ve kuruluşların hizmetlerine kapsamlı olarak etkisi olmuş siber güvenlik olaylarının belirlenmesi amaçlanmıştır. Kritik kamu kurum ve kuruluşları araştırmanın yapıldığı tarih itibariyle son beş yıl içinde en az bir bilgi güvenliği ihlal olayından geniş çaplı etkilendiğini bildirmiştir. Bu olayların hizmet kesintisine, bilginin kaybedilmesine, bilginin değiştirilmesine veya açığa çıkmasına neden olduğu belirtilmiştir. Belirtilen siber güvenlik olaylarının nedenleri üç grup altında ele alınabilir:

1. **İnsan faktörü:** Bilgi güvenliği ihlal olaylarının bir kısmı, yetkili kullanıcı haklarıyla yapılan işlemlerden veya bilginin kasıtlı olarak dış taraflara verilmesinden kaynaklanmaktadır. Hesap parolasının zayıflığı nedeniyle hesabın ele geçirilerek kullanılması, hesap sahibinin parolasını başka kişilerle paylaşıyor olması, görevi değişen veya işten ayrılan personelin kapanmamış hesabı ile işlem yapılması ve sorumlunun tespit edilememesi gibi durumlarla karşılaşılmaktadır. Birtakım bilgilerin açıklanması uygun olan zamandan önce açıklanması, kurumlarca yayınlanan bazı listelerde kişilere ait kritik olabilecek ayrıntılı bilgiler bulunması insan faktörü kaynaklı bazı olaylardır.
2. **Saldırganlar ve zararlı yazılımlar:** Kuruluş itibarını etkileyen bazı olaylar da kuruluş ana sayfasının veya kurumsal bilgilerin saldırganlar tarafından ele geçirilmesi şeklinde olmaktadır. Saldırganlar kurum ağından veya kurumsal ağın dışından sistemlere erişim sağlamışlardır. Bu olayların ötesinde hedefli saldırılara ilişkin bilgi paylaşılmamıştır. Verilen hizmetlere büyük çapta etkisi olan diğer bir tehdit zararlı yazılımlardır. Bu tehditten kaynaklı olaylar çoğu zaman, oldukça çok sayıda istemci bilgisayara sahip olan kurumsal ağlarda kullanılan işletim sistemlerinin ve yazılımların yama yönetimindeki aksaklıklardan kaynaklanmaktadır.
3. **Yazılım güncelleme ve yaygınlaştırmada yaşanan uyumsuzluklar:** Kurumlarda hizmetlerin verilmesini sağlayan bilgi sistemleri altyapı yazılımlarının ve kurumsal yazılımların hatalardan arındırılması, yeni özelliklere sahip olması veya kurumsal süreçlerle uyumlu hale getirilmesi gibi amaçlarla zaman zaman güncellenmesi gerekmektedir. Kurumsal yazılımların gerek hatalardan arındırma gerek uygulamadaki değişiklikler nedeniyle zaman zaman güncellenmesi gerekmektedir. Bu güncellemelerin yapılması ve yaygınlaştırılması sırasında çeşitli yazılım veya ortam uyumsuzluklarından kaynaklanan hizmet kesintileri veya veri kayıpları yaşanabilmektedir.

1.4 Gereksinimlerin Belirlenme Kriterleri

Kamu kurumları için güvenlik gereksinimlerinin en temel içeriği barındırması hedeflenmiştir. Bu amaçla, bu dokümanda öncelikli olarak ele alınması gereken önlemleri kapsayan ve aynı zamanda diğer güvenlik önlemlerinin temelini oluşturabilecek bir yapı sunulmuştur. Kurum ve kuruluşların karşı karşıya olduğu tehdit ve saldırılar, bunların sonucunda yaşanan bilgi güvenliği olayları incelenmiştir. Olası saldırılara karşı korunmada en çok katma değeri sağlayacak öncelikli güvenlik süreçleri nelerdir sorusu yanıtlanmaya çalışılmıştır. Her tehdide karşı o tehdide özel olan önlemler yerine, daha kapsayıcı olarak daha geniş bir tehdit grubuna karşı koruyucu önlemlerin alınmasını sağlayan güvenlik gereksinimlerine öncelik verilmiştir.

Temel Siber Güvenlik Gereksinimleri yaygın kullanılan güvenlik standartları veya uyum yapıları (ISO/IEC 27001, COBIT, PCI DSS vb.) ile birlikte uygulanabilir ve bu çalışmaları destekler.

1.5 Nereden Başlamalı?

Temel siber güvenlik gereksinimleri Şekil 3'te yer alan 10 adet başlık altında belirlenmiş olup, güçlü bir savunma temeli oluşturmak için yapılması gerekenleri açıklamaktadır.

Bir kurumun güvenlik iyileştirmesi için öncelikle temel gereksinimlerine göre kurumun mevcut durumunun değerlendirilmesi, ardından yapılması gerekenlerin belirlenmesi ve bir uygulama planı hazırlanarak planın hayata geçirilmesi tavsiye edilmektedir.

Kurum ve kuruluşlar tarafından temel siber güvenlik gereksinimlerde belirtilen adımların tümünün bir anda uygulanması beklenmemektedir. Mevcut durum belirlendikten sonra her gereksinim için hedef bir seviye belirlenerek, hedef seviyeye ulaşmak için aşamalı bir plan yapılabilir. Planda yer alacak aşamalar, kapsamın genişletilmesi, adımlardaki ilerleme ve gereksinimin uygulanma sürecinin operasyonel süreçler haline gelmesi şeklinde tanımlanabilir.

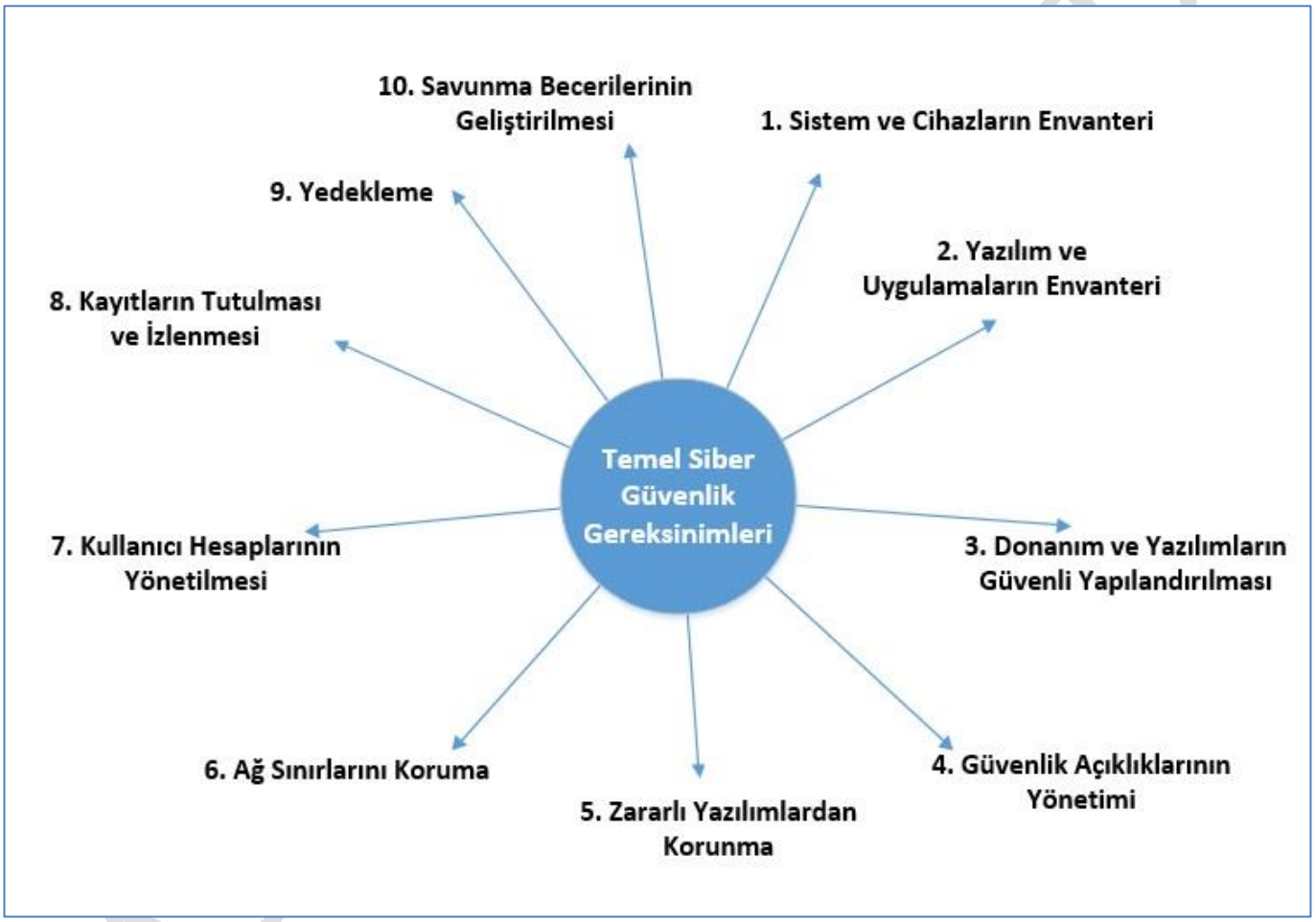
Kurumlar gereksinimlerin uygulanmasında mevcut durumlarına ve risklerine göre farklı stratejiler izleyebilirler. Aşağıda kurum ve kuruluşlar tarafından kullanılabilecek örnek stratejiler tanımlanmıştır:

- Kurum ve kuruluşlar tarafından yapılacak değerlendirme sonucunda en zayıf oldukları alanlardaki önlemlerden başlamak,
- Gereksinimlerde yer alan uygulama adımlarını gerçekleştirmek için ihtiyaç duyulan süre, insan kaynağı veya bütçe dikkate alınarak önceliklendirmek,
- Gereksinimlerde yer alan adımları birden çok sorumlu veya takım tarafından eş zamanlı olarak gerçekleştirmek.

Temel siber güvenlik gereksinimleri teknik içeriklidir. Belirtilen uygulamaların devamlılığının sağlanması için uygulamaların bir güvenlik programı kapsamında yapılması ve bir program yürütücüsünün belirlenmesi, kurumsal güvenlik politika ve prosedürleriyle desteklenmesi ve kurumsal denetim süreçlerine entegre edilmesi tavsiye edilmektedir.

2. TEMEL SİBER GÜVENLİK GEREKSİNİMLERİ

Temel siber güvenlik gereksinimleri Şekil 3'te yer alan 10 adet başlıktan ve bunların uygulama adımlarından oluşmaktadır.



Şekil 3: Temel siber güvenlik gereksinimleri başlıkları

Temel siber güvenlik gereksinimleri sonraki alt bölümlerde detaylandırılmaktadır. Her bir alt bölümün adı gereksinim adı olarak tanımlanmaktadır. Alt bölümler gereksinim için açıklama metni ile başlamakta ve sonrasında "Önemi" ve "Uygulama Adımları" başlıklarını içermektedir. "Önemi" bölümü gereksinimin gerekçesi ve saldırıları engellemedeki önemini belirtmekte, "Uygulama Adımları" bölümü de gereksinimi uygulama konusunda atılacak detaylı adımları tarif etmektedir.

2.1 Temel Güvenlik Gereksinimi #1: Sistem ve Cihazların Envanteri

Ağa bağlanan tüm cihazların envanteri tutulmalı, envanterde bulunmayan onaylanmamış cihazların ağa bağlanması engellenmelidir.

Önemi:

Kurum ağına bağlanan belirli bir koruma seviyesine sahip olmayan yaması yapılmamış bilgisayarlar, varsayılan ayarlarıyla gelen yeni cihazlar, test sistemler gibi cihazlar saldırganlar için kolay hedefler oluşturarak saldırganların kurum ağına kolaylıkla sızmasına neden olmaktadır. Bu nedenle ağa bağlanan tüm cihazlar takip edilmeli, yeni bağlanacak bir sistem gerekiyorsa kurum ağından izole edilmelidir. Kurum ağına bağlı olan sistemlerin bilgisi açıklık yönetimi ve takibinin temelini oluşturur.

Uygulama Adımları:

1. Envanterin ilk hali için tarama araçları yardımıyla ağ taranarak aktif olan IP adreslerindeki sistemler tespit edilir. Tarama için gönderilen paketlere yanıt vermemek üzere yapılandırılmış bilgisayar veya cihazlar için ağı dinleyerek cihazların varlığını tespit edebilen tarama araçları kullanılabilir.
2. Tarama sonuçları ve sistemler ve cihazlar hakkında bilinen bilgiler birleştirilerek envanter oluşturulur. Ağa bağlı olan her türlü cihaz oluşturulan envanterde bulunmalıdır. Envanterde masaüstü bilgisayarları, taşınabilir bilgisayarları, sunucuları, ağ cihazları, yazıcılar, depolama alan ağları, IP telefonlar, sanal bilgisayarlar, kameralar vb. yer almalıdır. Cihazlar hakkında bilinen veya edinilen bilgilere göre envanterde en az aşağıdaki bilgiler bulunmalıdır:
   - Cihazın adı / tanımlayıcısı,
   - Cihazın IP numarası,
   - Cihazın MAC adresi,
   - Cihazın kullanım amacı,
   - Cihazı kullanan sorumlu kişi ve birimi
3. Yeni tedarik edilen veya ağa yeni bağlanacak sistem ve cihazların envantere girişinin yapılması için süreç oluşturulur. Envantere girişi yapılmamış sistem ve cihazların ağa bağlanmasına izin verilmez.
4. Kurumun sistem ve cihaz envanteri ile ağda bulunan sistemler arasında fark oluşması durumunda bildirim yapılabilmesini sağlayacak bir sistem kurulur.

2.2 Temel Güvenlik Gereksinimi #2: Yazılım ve Uygulamaların Envanteri

Kurumda kullanılan tüm yazılımların ve uygulamaların envanteri tutulmalı, onaylanmamış yazılım ve uygulamaların kurulması ve kullanılması engellenmelidir.

Önemi:

Kurum ağında kullanılan belirli bir güvenlik seviyesine sahip olmayan yazılım ve uygulamalar, saldırganların sisteme sızması için kolay hedefler oluşturur. Kullanıcılar açıklığı bulunan web tarayıcı gibi yazılımlar kullanarak saldırganlar tarafından hazırlanmış veya ele geçirilmiş web sayfalarına eriştiklerinde kullandıkları bilgisayarlara arka kapı programlar ve bot yazılımlar yüklenerek bilgisayarları ele geçirilebilir. İş ihtiyaçları dışında, güvenilir kaynaklardan yüklenmemiş bazı yazılımlar da sistemlerin saldırganca uzaktan kontrolünü sağlayacak zararlı yazılımlar içerebilir. Yazılım envanterinin ve kontrolünün bulunmadığı bir ağda bir defa ağa giren ve yazılımlardaki açıklıkları kullanarak ilerleyen bir saldırganı durdurmak zorlaşır.

Kurum ağında kullanılan yazılım ve uygulamaların bilgisi, sistem yöneticilerinin kurum ağında güncel saldırılarda kullanılabilecek güvenlik açıklıkların varlığı konusunda bilgi sahibi olmalarını sağlayarak açıklık yönetiminin temelini oluşturur.

Uygulama Adımları:

1. Donanım envanterinden yola çıkılarak, donanımlar üzerindeki yazılımlar ve uygulamaların envanteri oluşturulur. Bunun için işletim sistemlerinin ve üzerindeki yazılımları tanıyan ve sürüm bilgilerini veren araçlar kullanılabilir.
2. Kurumda kurulmasına izin verilen onaylanmış yazılımların ve sürümlerin listesi oluşturulur. Bu yazılımlar kullanıcıların erişebileceği bir şekilde sunulabilir veya bilgisayarlara kullanıma hazır olarak kurulabilir.
3. Bilgisayarlara kurulu yazılım ve sürüm bilgilerini veren araçlarla bilgisayarlardaki yazılımlar takip edilerek, onaylanmamış yazılımların kurulması ve kullanılması engellenir.
4. İş ihtiyacı nedeniyle kullanılan ancak güvenlik riski oluşturan yazılımların çalıştığı sistemlerin ağ erişimi bulunmamalı, bu mümkün olamıyorsa yazılımlara erişim mutlaka ağ ve sistem bazında sınırlandırılmalıdır. Bu yazılımların bulunduğu bilgisayarlardaki antivirüs güvenlik seviyeleri en üst düzeye çekilmeli, işletim sistemi ve yazılımların güncelleştirmeleri yapılmalıdır.

2.3 Temel Güvenlik Gereksinimi #3: Yazılımların Güvenli Yapılandırılması

Kurumda kullanılan tüm cihazlar ve yazılımlar güvenli olarak yapılandırılmalı, yapılandırma değişikliklerinin kontrollü olarak yapılması sağlanmalıdır.

Önemi:

Cihazların ve yazılımların varsayılan yapılandırmaları kurulum ve kullanım kolaylığı için hazırlanmıştır. Üzerlerinde tanımlı varsayılan hesaplar ve parolalar, kurulu gereksiz yazılımlar, açık servis ve portlar saldırganlar tarafından sömürülebilir. Güvenli yapılandırma, bir başka deyişle sıkılaştırmalar ile donanım ve yazılımlar olası zafiyetlerinden arındırılarak donanım ve yazılımların saldırı alabileceği noktalar azaltılır.

Uygulama Adımları:

1. Güvenli yapılandırma için donanım veya yazılıma özel güvenlik sıkılaştırma tavsiyeleri uygulanır. Prensip olarak varsayılan ve kullanılmayan hesaplar kapatılır, işletim sistemlerinde veya yazılımlarda kullanılmayan servisler veya özellikler devre dışı bırakılır, açık olan ve kullanılmayan portlar kapatılır.
2. Ağ cihazlarını da içerecek şekilde kurumda kullanılacak olan tüm işletim sistemlerinin hem güncelleştirmeler hem de ayarlar bakımından sıkılaştırılmış imajları oluşturulur ve kurumda bu standart imajların kullanılması sağlanır.
3. Standart güvenli imajların son açıklıklar ve saldırı şekillerine karşı güncelliği sağlanır.
4. Sistemlerde standart yapılandırmalardan sapmalar veya istisnai durumlar sıkı bir şekilde takip edilir. Yönetici haklarına sahip yeni kullanıcılar eklenmesi, yeni portlar açılması, yeni servisler, grup politikası ve yerel politikalardaki değişiklikler bir saldırganın sistemdeki hareketinden kaynaklanabileceği için dikkatle izlenir.
5. Cihazların uzaktan yönetimi sadece SSH gibi güvenli yöntemlerle yapılır, cihazlar sadece bu bağlantılara izin verecek şekilde yapılandırılır. Telnet, VNC, RDP gibi güçlü şifrelemeyi desteklemeyen protokollerin kurum dışından zorunlu olarak kullanılması gerekiyorsa, bu bağlantılar sadece SSL, TLS veya IPSEC gibi ikinci bir şifreleme kanalı üzerinden yapılmalıdır.

2.4 Temel Güvenlik Gereksinimi #4: Güvenlik Açıklıklarının Yönetimi

Kurum sistemlerinde var olan güvenlik açıklıkları devamlı olarak takip edilmeli ve yönetilmelidir.

Önemi:

Yazılım ve donanımlar üreticiler tarafından sunulduktan sonra sık aralıklarla yazılım ve donanımlarda yeni hatalar ve açıklıklar keşfedilir. Açıklıklar ortaya çıktıktan çok kısa bir süre içinde saldırganlar tarafından kullanılmaya başlanır. Bu açıklıkları otomatik olarak kullanan zararlı yazılımlar da ortaya çıkar. Bilinen bu açıklıkların kurum sistemlerinde olup olmadığını tespit etmek, tespit edilen açıklıkları kısa süre içinde kapatmak bu saldırılara karşı önemli bir koruma

sağlar. Üretici firmalar bulunan yeni açıklıkları kapatan ve hataları düzelten yamalar ve güvenlik güncelleştirmeleri yayınlamaya başlar. Yama ve güvenlik güncelleştirmelerinin zamanında yapılması saldırganların sömürebileceği birçok açıklığı devre dışı bırakır.

Uygulama Adımları:

1. Web tarayıcıları ve e-posta istemcileri de dâhil olmak üzere kurumda kullanılan tüm yazılımların en güncel sürümleri kullanılır. Kurum sistemlerinde üretici tarafından desteği verilmeyen, yama ve güvenlik güncelleştirmeleri yayınlanmayan yazılımlar kullanılmaz.
2. Kurumda kullanılan yazılım ve uygulama envanteri ile yamaların yönetimi ilişkilendirilir.
3. Özellikle kurumsal uygulamaların veya uygulamaları destekleyen yazılımların güncelleştirmeleri test sistemlerde uygulanarak güncelleştirmelerin uygulamanın çalışmasında bir sorun oluşturmadığı görüldükten sonra yaygınlaştırma yapılır.
4. Sistemlerde yüklü yamaların takibi otomatik olarak yapılır.
5. İnternet'e açık sistemler, zararlı yazılımdan korunma yazılımı gibi yükseltilmiş haklarla çalışan yazılımlar ve güvenlik güncelleştirmeleri içeren yamalar önceliklendirilir.
6. Yamaların yaygınlaştırılması için hedef süre belirlenerek yamaların zamanında uygulanması sağlanır.
7. Açıklıkların var olduğu ancak yamaların yüklenemediği durumda açıklıkla ilgili servislerin veya özelliklerin kapatılması, erişim kontrolleri ile açıklık bulunduran servislere erişimin kısıtlanması, olası saldırıları tespiti için izlemenin arttırılması gibi önlemler alınır.
8. Kurum ağındaki sistemler düzenli aralıklarla açıklık tarama araçlarıyla taranır. Tespit edilen açıklıklar, açıklıkların ve bulundukları sistemin kritikliğine göre yapılan bir öncelik sıralaması ile ele alınır. Açıklık yama yapılarak, açıklığın kapatılmasını sağlayacak önlemleri alarak veya makul bir risk olarak kabul edilerek ele alınabilir.
9. Bu işlemlerin yapılmış olduğunu doğrulamak için sistemler tarama araçlarıyla tekrar taranarak açıklık tarama sonuçları önceki sonuçlarla karşılaştırılır. Kabul edilen açıklıklar ileride bu açıklığı kapatacak yeni yamalar çıkması ve farklı önlemler alınabilmesi açısından takip edilir.
10. Kullanılan güvenlik açığı tarama araçlarının tanıdığı güvenlik açıklıkları düzenli olarak güncellenir. Tarama araçlarının üzerinde çalıştığı sistemlerin yama ve güvenlik güncelleştirmeleri yapılır.

2.5 Temel Güvenlik Gereksinimi #5: Zararlı Yazılımlardan Korunma

Zararlı yazılımlardan korunma önlemleri, kurumdaki tüm sistemler için etkin olacak ve farklı bulaşma yollarını kapsayacak şekilde uygulanmalıdır.

Önemi:

Zararlı yazılımlar İnternet'te en sık karşılaşılan önemli tehditlerden biri olup, son kullanıcı cihazları, e-posta ekleri, web sayfaları, çıkarılabilir ortamlar gibi farklı yollardan sistemlere sızabilir. Zararlı yazılımlardan korunma, kurumdaki tüm sistemler için, zararlı yazılımların tespit edilmesi, yayılmasının engellenmesi ve yazılımların çalıştırılmasının kontrol edilmesini sağlamalıdır.

Uygulama Adımları:

1. Kişisel ve kurumsal güvenlik duvarları, ağ ve sunucu tabanlı saldırı tespit/önleme sistemleri, antivirüs yazılımları, zararlı/casus yazılımları önleme sistemleri vb. gibi yazılımlar zararlı yazılımları tespit etme özellikleri ile yapılandırılarak tüm sistemler için etkin olacak ve farklı bulaşma yollarını kapsayacak şekilde konumlandırılır. Bu kaynaklardan tespit edilen zararlı yazılım bildirimleri takip edilir.
2. Zararlı yazılımlardan korunma sistemlerinin etkinliğini sürdürmek için sistemler (yazılımın kendisi ve imza dosyaları) güncel tutulur.
3. Sistemler çıkarılabilir ortam aygıtları (USB bellekler, USB harici diskler, CD/DVD'ler, harici SATA cihazları vb.) ve ağ paylaşım alanlarındaki içerikleri otomatik olarak çalıştırmayacak şekilde yapılandırılır. Çıkarılabilir ortam aygıtları sistemlere takıldığında, sistemlerin bu aygıtlarda otomatik olarak zararlı yazılım taraması yapması sağlanır.
4. Web içerik filtrelemesi uygulanır. Beyaz listeler yoluyla sadece izin verilen web içerikleri ve web sitelerine erişilebilmesi veya siyah listelerle zararlı alan adları ve IP adreslerine erişimin engellenmesi sağlanır.
5. E-posta içerik filtrelemesi uygulanır. İzin verilen eklenti tipleri belirlenir, eklentiler (sıkıştırılmış olanlar da dâhil) taranır. E-postalardaki bağlantılar, pdf ve Microsoft eklentiler analiz edilir ve zararlı yazılımlardan arındırılır.
6. E-posta taklitçiliğini önlemek için SPF (Sender Policy Framework) veya Sender ID gibi kontroller uygulanır.

2.6 Temel Güvenlik Gereksinimi #6: Ağ Sınırlarını Korunma

Birbirinden farklı güvenlik seviyesine sahip ağlar arasında trafik sınırlanmalı ve izlenmelidir.

Önemi:

Saldırganlar, kurumlarda İnternet'e açık sistemleri değil, aynı zamanda İnternet'e erişim sağlayan kullanıcılar gibi bilgisayarları kendilerine hedef seçebilir ve sömürülen bir bilgisayar üzerinden kurumdaki farklı hedeflere atlayarak zincirleme olarak daha önemli sistemleri ele geçirebilir. Ağların ayrılması saldırganların kurum ağında ilerlemesini ve kurumun kritik bilgilerini bulunduran sistemlere erişimini zorlaştırır. Sınırlarda geçirilen veya engellenen trafik verileri güvenlik olaylarının tespit edilmesi için önemli bilgiler sağlar.

Uygulama Adımları:

1. İnternet, dışarıya hizmet veren sunucular, kurum içi sunucular ve kullanıcıların bulunduğu ağlar gibi farklı güvenlik ihtiyaçları olan ağlar ayrılmalıdır.
2. Ağların arasında trafik kontrolü için güvenlik duvarları ve erişim kontrol listeleri kullanılır.
3. Varsayılan olarak her şeyi engelle/düşür kuralıyla izin verilen servisler ve portlar dışındaki tüm trafik engellenir.
4. Trafiğe izin veren her kural için onaylanmış iş gereksinimi, gereksinimin sahibi ve kuralın geçerli olacağı süre belirtilir.
5. Bilinen zararlı IP adresleri (kara listeler) ile erişim engellenir veya beyaz listeler yoluyla sadece beyaz listedeki erişimlere izin verilir.
6. İnternet, dış DMZ ve kurumsal sunucuların sistem ve ağlarına normalden farklı saldırı mekanizmalarını arayan ve bu sistemlerin ele geçirilmesini tespit eden/engelleyen ağ tabanlı IDS/IPS sensörleri yerleştirilir.
7. Kurum ağından İnternet'e giden trafiğin uygulama katmanında filtre yapabilen bir vekil sunucudan geçmesi sağlanır.

2.7 Temel Güvenlik Gereksinimi #7: Kullanıcı Hesaplarının Yönetilmesi

Kullanıcı hesaplarına özellikle erişim ayrıcalıklarına sahip sistem yöneticisi gibi haklar iş gereksinimlerine göre verilmeli, hesapların tanımlanması, gözden geçirilmesi ve kapatılması süreçleri tanımlanmalıdır.

Önemi:

Saldırganların sistemlerde tanımlı ancak etkin olmayan kullanıcı hesaplarını ele geçirip, işlemler yaparak fark edilmelerini zorlaştırırlar**.** Görevi değişen veya işten ayrılan personelin hesabı ile işlem yapılması ve sorumlunun bulunamaması en sık karşılaşılan bilgi güvenliği olaylarından

biridir. Kullanıcılara sistemlerde yönetici ayrıcalıkları yerine sadece gerektiği kadar haklar verilmesi, sistemlerin ele geçirilmesi durumunda kullanıcı haklarıyla çalışan zararlı yazılımlarının haklarını da kısıtlayacağı için olası zararı azaltır.

Uygulama Adımları:

1. Tüm hesaplar için erişim, Aktif Dizin veya LDAP gibi merkezi bir kimlik doğrulama sistemi üzerinden doğrulanacak şekilde yapılandırılır.
2. Erişim hakları kullanıcılara "Bilmesi Gereken Prensibi[1]"ne göre verilir.
3. Tüm sistem hesapları ve erişim hakları düzenli olarak gözden geçirilir ve iş süreci sahibinin onayladığı hesaplar ve haklar dışındaki tüm hesaplar devre dışı bırakılır.
4. Bir çalışanın veya yüklenicinin işinin sona ermesi durumunda, hesapların derhal devre dışı bırakılmasına sağlayacak bir hesap kapatma süreci uygulanır.
5. İş ihtiyacı sona eren veya tanımlı bir süre (örneğin 3 ay) içerisinde kullanılmayan hesaplar devre dışı bırakılır.
6. Kullanıcı parolaları kullanıcılara güvenli bir şekilde iletilir, ilk verilen parolanın değiştirilmesi ve güvenli bir parola atanması sağlanır.
7. Sistemlerde verilmiş ayrıcalıklı hakların (kime ve hangi amaçla verildiği gibi) ayrıntılı envanteri tutulur ve belirli aralıklarla gözden geçirilir.
8. Sistem yöneticisi yetkilerine sahip hesaplar sadece sistem yönetim eylemlerinde kullanılır.
9. Sistem yöneticisi haklarıyla yapılan işlemlere dair kayıtlar da tutulur ve düzenli olarak takip edilir.
10. Tüm hesapların kullanıcı adlarının ve kimlik doğrulama bilgilerinin ağlar arasında şifreli kanallar üzerinde iletilmesi sağlanır.
11. Hassas verilere veya sistemlere erişimi olan hesaplar için en az iki faktörlü kimlik doğrulaması istenir. Bunun için akıllı kartlar, sertifikalar, tek kullanımlık şifre üreten cihazlar veya biyometrik yöntemler kullanılabilir.

2.8 Temel Güvenlik Gereksinimi #8: Kayıtların Tutulması ve İzlenmesi

Bilgisayarlardaki önemli olaylar (kullanıcı faaliyetleri, hatalar, istisnai durumlar vb.) için kayıtlar üretilmeli ve analiz edilmelidir.

[1] Bilmesi Gereken Prensibi: Herhangi bir konu veya işi, ancak görev ve sorumlulukları gereği öğrenmekle, incelemekle, gereğini yerine getirmekle ve korumakla sorumlu bulunanların yetkisi düzeyinde bilgi sahibi olması ve erişmesi.

Önemi:

Sistemlerde tutulan güvenlik kayıtları, saldırıların fark edilmesini sağlayan ve saldırının ayrıntılarını ve saldırganların sistemlerdeki hareketlerini takip etmeye yarayan önemli bilgilerdir. Kayıtların uygun şekilde tutulmadığı veya takip edilmediği durumlar olayların zamanında fark edilememesine ve saldırı sonucu olası zararın boyutunun bilinememesine neden olur. Saldırganların yaptıkları işlemlere dair kayıtları ortadan kaldırması da izlerini saklamak için sıklıkla başvurdukları bir yöntemdir.

Uygulama Adımları:

1. Kayıtların zaman bilgisinin doğru ve güvenilir olması için tüm sunucu ve cihazların düzenli aralıklarla zaman bilgisini alacakları bir zaman kaynağı tanımlanır.
2. Kayıtlarda ilgili sisteme göre en az hangi alanların bulunması gerektiği belirlenerek kayıt ayarları yapılır. Kayıtların istenen haliyle sadece cihazların üzerinde değil, bir kayıt sunucusuna gönderilerek kayıt sunucusunda tutulduğu doğrulanır.
3. Kayıt dosyalarının depolama alanlarını doldurmasını engellemek için kayıt tutulan cihazların üretilen kayıtlar için yeterli depolama alanına sahip olması sağlanır.
4. Kayıtlardaki olağandışı aktiviteler takip edilerek sistem sorumlularının bilgilendirilmesi sağlanır, düzenli aralıklarla raporlanır ve şüpheli olaylar ayrıntılı olarak incelenir.
5. Birden fazla kaynaktan gelen kayıtların toplanması, birleştirilmesi, kayıtların ilişkilendirilmesi ve analizi için, Güvenlik Olay Yönetimi ve Korelasyon Sistemi (SIEM) veya kayıt analiz araçları kullanılır.

2.9 Temel Güvenlik Gereksinimi #9: Yedekleme

Kritik bilgiler, yazılım ve sistemlerin yedekleri düzenli aralıklarla alınır, alınan yedeklerden geri dönülebileceği düzenli olarak test edilir.

Önemi:

Sistemlerdeki veriler saldırganlar, fidye yazılımları veya diğer zararlı yazılımlar tarafından şifrelenebilir veya silinebilir; kötü niyetli kullanıcılar, kasıtsız hatalar, donanım veya yazılımlardaki problemler gibi nedenlerle verilere erişilemeyebilir veya veriler güvenilmez hale gelebilir. Kurumlar bu tür durumlarında olağan işleyişlerinin sekteye uğramaması için verilere geri yükleyecek mekanizmalara sahip olmalıdır**.**

Uygulama Adımları:

1. Bilgi, yazılım ve sistem imajlarının kritikliği ve verilerin değişme aralıklarına uygun olarak düzenli aralıklarla otomatik olarak yedeklenmesi sağlanır.

2. Yedeklemenin düzgün çalıştığından emin olmak için yedekleme ortamındaki veriler geri döndürülerek düzenli aralıklarla test edilir.
3. Yedekler depolanırken veya iletilirken fiziksel olarak veya şifrelenerek uygun şekilde korunur.

2.10 Temel Güvenlik Gereksinimi #10: Savunma Becerilerinin Geliştirilmesi

Çalışanların bilgi güvenliği konusunda bilgi ve becerileri güncel saldırılara karşı koyma ve önlemler alma yönünde devamlı olarak geliştirilmelidir.

Önemi:

Kurumlarda bilgi güvenliği tehditlerine karşı teknolojik önlemler alınmakla beraber, bu önlemlerin tasarımı, uygulanması, sürdürülmesi ve takip edilmesi gibi önemli süreçler kurumdaki çalışanlar tarafından yapılmaktadır. Sistem yöneticileri, ağ yöneticileri, yazılım geliştiriciler, güvenlik yöneticileri, kullanıcılar, kurum yöneticileri gibi farklı roldeki çalışanların kurumun güvenlik önlemlerinin etkin şekilde uygulanmasını sağlamada sorumlulukları vardır. Bu sorumlulukları yerine getirebilmelerini sağlayacak bilgi ve becerilerin edinilmesi ve devamlı olarak geliştirilmesi bu önlemlerin gereğince uygulanabilmesini, etkin ve sürekli olmasını sağlar.

Buna ek olarak, saldırganlar oltalama veya fidye yazılımları gibi zararlı yazılımlar üzerinden insan davranış ve alışkanlıklarını hedef alarak sistemlere sızmaktadır. Teknik önlemlerin yanında insan davranışlarını kullanan saldırılara karşı farkındalık çalışmaları yapılarak bilgi güvenliğinin insan tarafı güçlendirilmelidir.

Uygulama Adımları:

1. Kurum çalışanlarının temel siber güvenlik gereksinimlerini gerçekleştirmek için gereken becerileri belirlenir. Var olan beceriler değerlendirilerek, bu becerilerin kazanılmasını sağlayacak güvenlik programları oluşturulur. Bu programlar sistem yöneticileri için teknik güvenlik eğitimleri, kullanıcılar için bilgi güvenliği farkındalık eğitimleri gibi kurumdaki roller bazında belirlenir.
2. Programdaki eğitimler sınıf eğitimleri, konferanslar, çevrimiçi eğitimler vb. şekilde sunulabilir. Ayrıca web sayfaları, duyurular, hatırlatmalar, el kitapları, broşürler vb. ile güvenlik bilinçlendirme çalışmaları desteklenebilir.
3. Bilgi güvenliği farkındalık eğitimleri, saldırganlar tarafından en çok kullanılan sömürü yöntemlerini ve kişilerin bunları engellemek için neler yapacaklarını ortaya koyar.
4. Farkındalık eğitimleri, kurumun güvenlik konusundaki gereksinimleri, kurumun güvenlik yaklaşımı, kurumda en sık karşılaşılan güvenlik olayları gibi kuruma özel bilgilendirmeleri

içerir.

5. Üst yönetimin güvenlik çalışmalarındaki rolü ve desteği görünür olmalıdır.
6. Eğitimler güncel saldırı yöntemlerini içerecek şekilde güncellenir.
7. Tüm çalışanların en az yılda bir kez farkındalık eğitimlerini alması sağlanır.
8. Çalışanların edinilmesi beklenen davranış alışkanlıkları düzenli olarak test edilir (E-posta ile gelen şüpheli bağlantıların tıklanmaması, bilgisayar başından kalkarken ekranın kilitlenmesi vb. gibi). Testlerin sonucuna göre kişilere özel tekrar eğitimler yapılabilir.

KAYNAKÇA

[1] "2017 Threat Landscape Survey: Users on the Front Line", SANS Institute, https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910, Ağustos 2017.

[2] "Strategies to Mitigate Cyber Security Incidents – Mitigation Details", Australian Government – Australian Cyber Security Centre – Australian Signals Directorate (ASD), https://www.asd.gov.au/publications/Mitigation_Strategies_2017_Details.pdf , Şubat 2017.

[3] "IBM X-Force Threat Intelligence Report 2016", http://www.foerderland.de/fileadmin/pdf/IBM_XForce_Report_2016.pdf, Şubat 2016.

[4] "Global Cybersecurity Index (GCI) 2017", International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, 2017.

[5] "Microsoft Security Intelligence Report", Vol. 21, http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_Key_Findings_Summary_English.pdf , Ocak – Haziran, 2016.

[6] "TS ISO/IEC 27002:2013 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri", Türk Standardları Enstitüsü, Aralık 2013.

[7] "Cyber Essentials Scheme: Requirements for Basic Technical Protection from Cyber Attacks", UK Government, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf, Haziran 2014.

[8] "Critical Security Controls for Effective Cyber Defense", The Center for Internet Security, https://www.cisecurity.org/controls/, Ocak 2016.