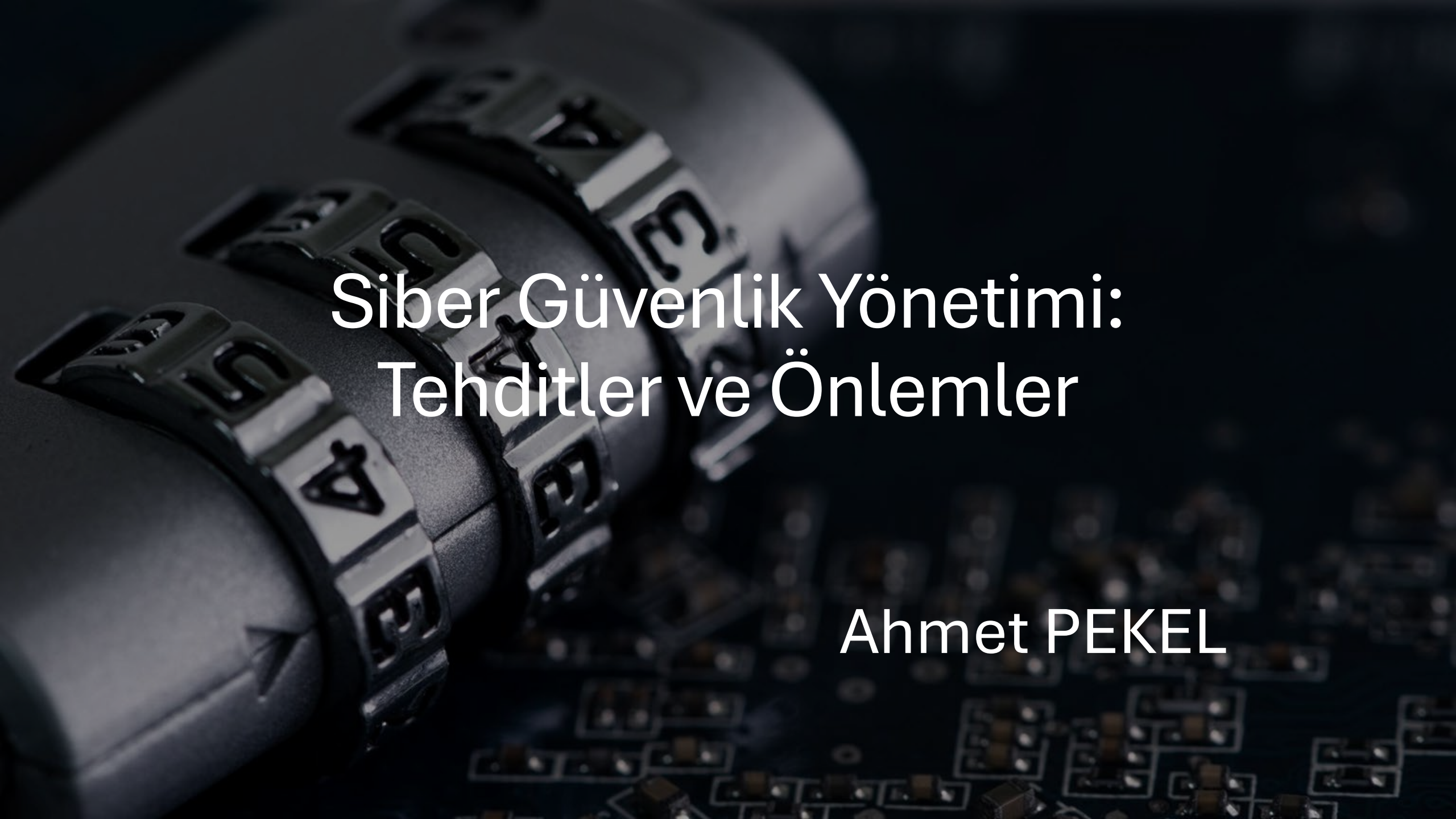
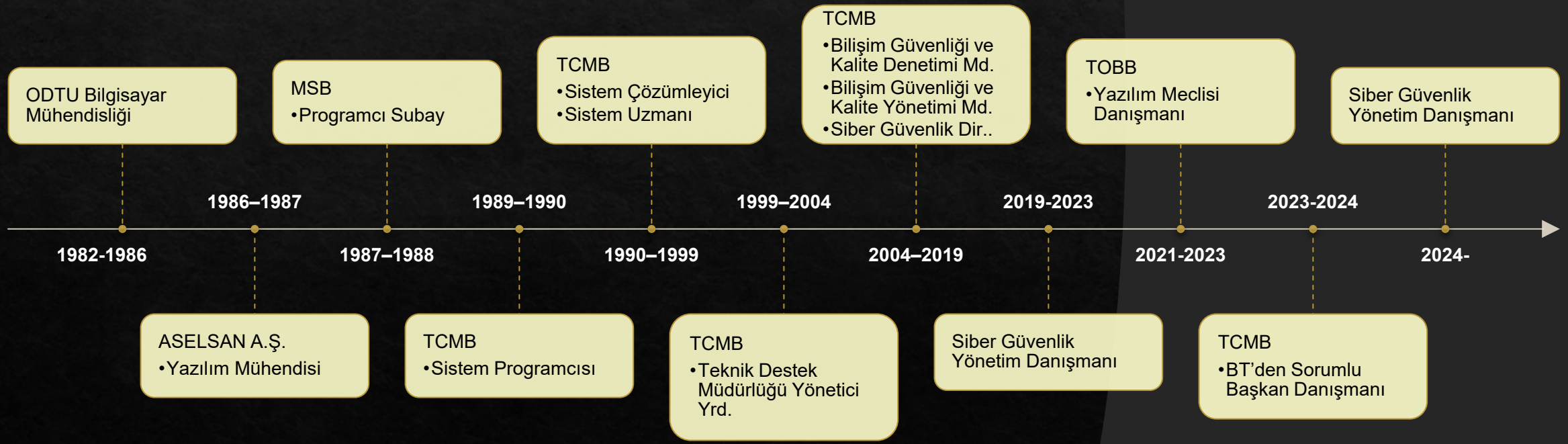


Siber Güvenlik Yönetimi: Tehditler ve Önlemler

Ahmet PEKEL

Ahmet PEKEL


1982-1986
ODTU Bilgisayar Mühendisliği
1986–1987
ASELSAN A.Ş.
•Yazılım Mühendisi
1987–1988
MSB
•Programcı Subay
1989–1990
TCMB
•Sistem Programcısı
1990–1999
TCMB
•Sistem Çözümleyici
•Sistem Uzmanı
1999–2004
TCMB
•Teknik Destek Müdürlüğü Yönetici Yrd.
2004–2019
TCMB
•Bilişim Güvenliği ve Kalite Denetimi Md.
•Bilişim Güvenliği ve Kalite Yönetimi Md.
•Siber Güvenlik Dir..
2019-2023
Siber Güvenlik Yönetim Danışmanı
2021-2023
TOBB
•Yazılım Meclisi Danışmanı
2023-2024
TCMB
•BT'den Sorumlu Başkan Danışmanı
2024-
Siber Güvenlik Yönetim Danışmanı

KAPSAM

- 11.00-11.45 Temel Kavramlar ve Yönetim İlkeleri
- 12.00-12.45 Bireyleri Hedef Alan Tehditler ve Önlemler

- 13.45-14.30 Siber Güvenlikte Fiziksel Güvenlik, Siber Saldırılardan Çıkarılan Dersler, Yeni Teknolojiler ve Siber Güvenliğe Etkisi
- 14.30-15.00 Soru/Yanıt


Temel
Kavramlar

Siber Güvenlik

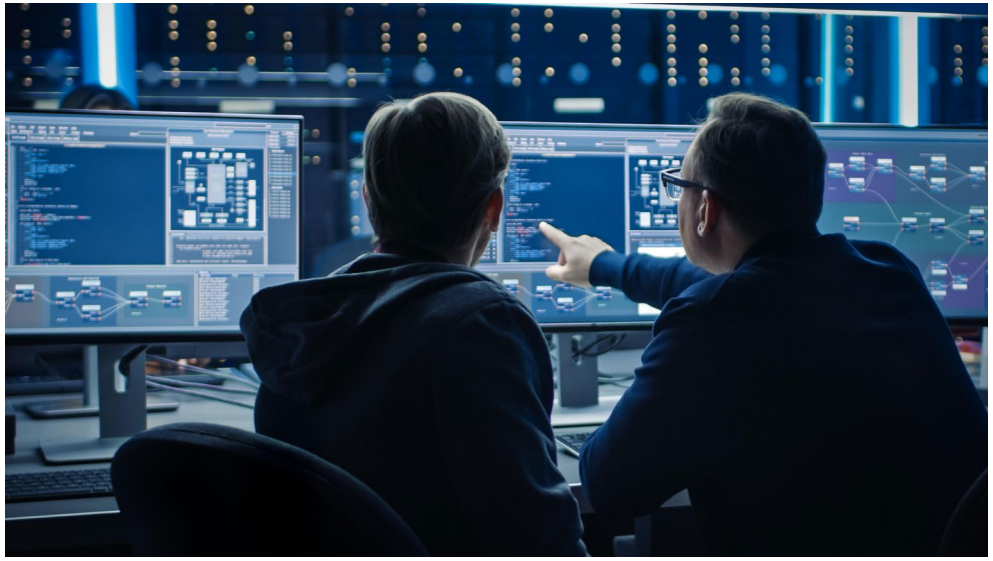
- Sistemleri, verileri, iletişim ağlarını ve programları siber saldırılardan korumak için alınan önlemler bütünüdür.

Siber Saldırgan

- Bilgisayar sistemine yetkisiz erişim sağlayan,
- Yasadışı olarak bir bilgisayar sistemine giren,
- Verilere yetkisiz erişim sağlamak için bilgisayar kullanan,
- Bilgisayarlı bir sistemde belirli bir hedefe ulaşmak veya belirli bir engeli aşmak için teknik bilgilerini kullanan kişidir.
- Siber saldırganlar genellikle hassas bilgilere erişmeyi, bunları değiştirmeyi veya yok etmeyi ya da bu bilgileri kullanıcılardan çalmayı ya da normal iş süreçlerini kesintiye uğratmayı amaçlarlar.

Siber Güvenlik Uzmanı

- Bilgi sistemlerinin güvenliğini sağlar; güvenlik olaylarını izleyerek, tehditleri saptayarak, araştırarak, çözümleyerek ve bunlara yanıt vererek, sistemleri siber güvenlik risklerinden, tehditlerinden ve güvenlik açıklarından korur.



Beyaz Şapkalı Güvenlik Uzmanı (*White Hat Hacker*): Bir kurumun güvenlik açıklarının ortaya çıkarılması amacıyla siber korsanların (*Black Hat Hacker*) kullandıkları teknikleri uygulayan ancak bunu etik kurallar çerçevesinde yapan güvenlik uzmanıdır.

Kırmızı Takım (*Red Team*): Bir kurumun tüm siber güvenlik yeterliliklerinin sınanması için saldırı benzetimi (*simulation*) yapan takıma verilen addır.

Mavi Takım (*Blue Team*): Bir kuruma karşı yöneltilebilecek olası saldırıları karşılamak amacıyla alınması gereken önlemleri belirleyen takımın adıdır.

Siber Saldırı

- Siber suçlular tarafından bir ya da daha çok bilgisayar kullanılarak tek ya da birden fazla bilgisayara veya ağa yapılan saldırıdır.
- Bir siber saldırıda, bilgisayarlar devre dışı kalabilir, veriler çalınabilir ve/veya ele geçirilen bir bilgisayar yeni bir saldırıyı başlatmak için kullanabilir.

Siber Saldırı Yöntemleri

- Kötücül yazılımlar (*malware*)
- Sistem ya da yazılım açıklıklarını sömürme
- Kullanıcı hesabı ele geçirme
- Hedefli saldırılar
- Kötücül kod yerleştirme
- Yanlış yapılandırılmış sistemlere yönelik saldırılar
- Kötücül istenmeyen (*spam*) iletiler
- Sahte sosyal hesaplar kullanılarak yapılan saldırılar
- Kötücül reklam kodları

Siber Saldırı Hedefleri

Siber saldırılarda en çok hedeflenen alanları aşağıdaki gibi özetleyebiliriz:

- Bireyler
- Sanayi kuruluşları
- Kamu
- Bilim-Teknik
- Sağlık
- Eğitim
- Destek hizmetleri
- Finans ve sigortacılık
- Konaklama ve yiyecek hizmetleri
- Satış ve kiralama hizmetleri
- Sanat ve eğlence
- İmalât
- Ödeme Sistemleri
- Emlâk
- Bilgi ve İletişim Teknolojileri

Siber Savaşlar ve Kritik Altyapılar

Siber savaşlarda en çok kullanılan saldırı noktaları kritik altyapılar olarak adlandırılan, ülkenin yaşamsal önemdeki kaynaklarıdır. Bunlar:

- Savunma,
- Enerji,
- Ulaşım,
- Finans,
- Sağlık,
- İletişim ve
- Su yönetimi altyapılarıdır.

Bu hedeflere yönelen siber saldırılar ülke düzeyinde yıkıcı etkiler oluşturabilmektedir.

Bir Siber Saldırının Olası Sonuçları - Örnekler

- Zararlı bir yazılımın, kurbanın bilgisayarına yüklenmesi sistemin donmasına ya da önemli bilgilerin açığa çıkmasına neden olabilir.
- Siber saldırılar elektrik kesintilerine, askeri gereçlerin arızalanmasına ve ulusal güvenlik sırlarının açığa çıkmasına neden olabilir.
- Tıbbi kayıtlar gibi değerli ve önemli verilerin çalınmasına neden olabilir.
- Telefon ve bilgisayar ağlarını bozabilir ya da sistemleri felç ederek verileri kullanılamaz hale getirebilir.
- Siber saldırılar toplum düzenini bozabilecek düzeyde etki oluşturabilir, saygınlık ve inandırıcılık kaybına neden olabilir.

Bilgi güvenliği, bilginin korunmasına yönelik bir dizi kuralın uygulanmasıdır

Bilgi güvenliğinde;

- Geç kalınamaz!
- “Bilmiyordum!” özür olarak kabul edilemez.
- Yönetim desteği gereklidir.

Bilgi güvenliği,

Varılması gereken bir hedef değil, sürekli iyileştirilmesi gereken bir süreçtir.

- Bilişim dünyasının en değişken alanıdır.
- Zaman ve çaba gerektirir.
- Maliyetlidir; eğitimli ve yetkin işgücüne gereksinim duyar.
- Riskleri tamamen ortadan kaldırmak anlamına gelmez; risklerin yönetilmesidir.
- Tek başına teknolojiyle çözülemez; bilinçli insanlarla mümkündür, kültürel değişim gerektirir.

Bilgiyi hedef alan tehditler

- Yetkisiz erişim,
- Bilginin bozulması ya da çalınması,
- Ağ trafiğini meşgul etme,
- Hizmet durdurma,
- Virüs, Truva atı (*trojan*) veya ajan programlarca (*spyware*) verilebilecek zararlar,
- Sosyal mühendislik,
- İnternet üzerinden yapılan karşı propaganda,
- Kritik altyapılara yönelik fiziki saldırılar.

Bilgiyi Hedef Alan Tehditler: Sonuçlar ve Önlemler

Bu tehditler nedeniyle,

- Ülke ekonomisi,
- Kamu emniyeti ve düzeni,
- Kişisel gizlilik,
- Kişisel, kurumsal ve ülkesel saygınlık ile
- Ticari rekabet olumsuz etkilenebilmektedir.

Tehditlere karşı;

- Bilgi,
- Yazılım,
- Donanım,
- Fiziksel alanlar,
- Hizmetler,
- Veri depolama ortamları,
- İletişim ortamları,
- İnsan ve
- Saygınlık korunmalıdır.

Bilgi Güvenliğinin Üç Temel İlkesi

- Gizlilik, bütünlük ve kullanılabilirlik

  - *Gizlilik*, bilgiye yetkisiz erişimi önlemenin güvencesidir;
  - *Bütünlük*, bilginin doğru ve değişmemiş olduğunun güvencesidir;
  - *Kullanılabilirlik*, gereksinim duyulduğunda yetkili kişiler tarafından bilgiye erişilebileceğinin güvencesidir.

Bilgi Güvenliği Yönetim Sistemi (BGYS)

- Bilgi Güvenliği Yönetim Sistemi, bilgi güvenliği altyapısını bir kuruluşta kurmak, işletmek, izlemek, gözden geçirmek ve iyileştirmek amacıyla geliştirilmiş, işlerliği ve sürekliliği güvence altına alınmış bir yönetim sürecidir.

Bilgi Güvenliği Yönetim Sistemi (BGYS)

- Sistem, aşağıdaki süreçleri kapsar:
  - Bilgi Güvenliği Politikası
  - Bilgi Güvenliği Örgütlenmesi
  - Varlık Yönetimi
  - Erişim Denetimi
  - Yükümlülüklere Uyum (yasalar, yönetmelikler ve yönergeler)
  - Bilgi Güvenliği İhlalleri Yönetimi
  - İnsan Kaynakları Güvenliği
  - Fiziksel ve Çevresel Güvenlik
  - Kriptografi
  - Bilgi Sistemleri Edinim, Geliştirme, Bakım
  - İletişim ve İşletim
  - İş Sürekliliği Yönetimi
  - Risk Yönetimi
- BGYS'nin kurulması için yönetimin desteği zorunludur.
- Kurumsal bir varlık olan bilginin korunmasından tüm kurum çalışanları sorumludur.

Güvenlik Açığı

Güvenlik açığı, siber saldırgan tarafından bir bilgisayar sisteminde yetkisiz eylemler yapmak için kullanılabilecek bir zayıflıktır.

Bir güvenlik açığından yararlanmak için, saldırganın bir sistem zayıflığına bağlanabilecek en az bir uygulanabilir araca ya da tekniğe sahip olması gerekir.

Güvenlik açıkları saldırı yüzeyi bileşenleri olarak da bilinir.

Güvenlik Açıklarının Yönetimi

Güvenlik açıklarının yönetimi (*Vulnerability Management*), aşağıdaki ortak süreçleri içeren döngüsel bir uygulamadır:

- Tüm varlıkları keşfetme
- Varlıklara öncelik verme
- Tam bir güvenlik açığı taraması yapma, değerlendirme
- Sonuçları raporlama
- Güvenlik açıklarını düzeltme
- Düzeltmeyi doğrulama ve yineleme

Güvenlik Açığı Türleri

- ***Bilgisayar Güvenliği Açıkları:*** Bu açıklar, güvenlik açığının nerede olduğu, neden olduğu veya nasıl kullanılabileceği gibi farklı ölçütlere göre çok sayıda türe ayrılabilirler. Bilgisayar güvenlik açıkları; bilgisayar yazılımlarındaki hatalar, virüs bulaşmış yazılımlar, eksik veri şifreleme, vb. şekilde sınıflandırılabilirler.
- ***Ağ Güvenliği Açıkları:*** Bu tür açıklar, bir ağın donanım veya yazılımında bulunan ve dışarıdan bir tarafın izinsiz girişine olanak sağlayan zayıflıklardır. Güvenli olmayan kablosuz erişim noktaları ve kötü yapılandırılmış güvenlik duvarları bu açıklara örnek olarak verilebilir.
- ***İşletim Sistemi Güvenliği Açıkları:*** Bunlar, bilgisayar korsanları tarafından kötüye kullanılabilecek belirli bir işletim sistemindeki var olan güvenlik açıklarıdır.

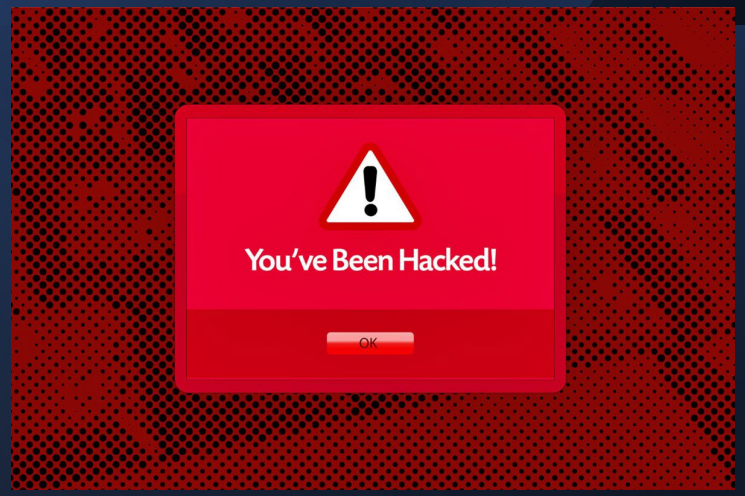
Güvenlik Açığı Türleri (devam)

- ***İnsan Kaynaklı Güvenlik Açıkları:*** Siber güvenlikte en zayıf halkalardan biri de siber güvenlik bilinci gelişmemiş insandır. Kullanıcı hataları; önemli bilgileri kolayca açığa çıkarabilir, saldırganlar için yararlanılabilir erişim noktalarını oluşturabilir veya sistemlerin çalışamaz duruma gelmesine neden olabilir.
- ***Süreç Kaynaklı Güvenlik Açıkları:*** Bazı güvenlik açıkları, belirli süreç denetimlerinin eksikliğinden kaynaklanabilir: düzenli sızma testlerinin yapılmaması ya da yaptırılan testlerden sonra iyileştirme çalışmasının yapılmaması gibi.

Kötücül Yazılımlar (Malware)

- Bunlar virüsler, fidye yazılımları ve casus yazılımlar olarak adlandırabileceğimiz bir dizi kötü amaçlı yazılımlardır.
- Kötücül yazılımlar siber saldırganlar tarafından geliştirilen, verilere ve sistemlere zarar vermek ya da bir ağa yetkisiz erişim sağlamak için tasarlanmış kodlardan oluşur.
- Bunlar genellikle e-posta üzerinden gönderilen bir bağlantı ya da dosya biçiminde sunulur ve kullanıcının kötücül yazılımı çalıştırması için bağlantıyı tıklamasını ya da dosyayı açmasını gerektirir.

Kötücül Yazılım Türleri



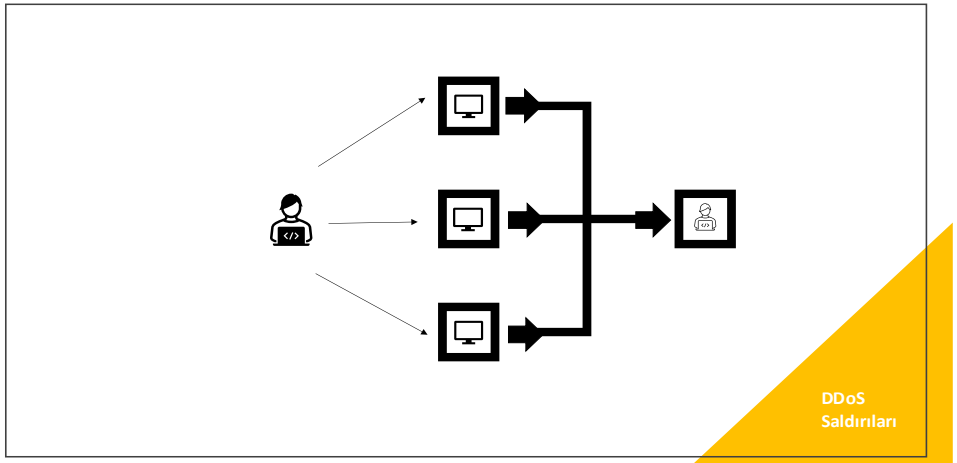
- Kötücül yazılım türleri şöyle özetlenebilir: *Trojan* (Truva Atı), *Spyware* (Casus Yazılım), *Adware* (Reklâm Yazılımı), *Bloatware* ya da *Crapware* (bilgisayarlara önceden yüklenmiş, bilgisayarları yavaşlatabilen promosyon yazılımları), Virüs, *Ransomware* (Fidye Yazılımı), *Scareware* (Korkutucu Yazılım), *Worm* (Kendisini Çoğaltan Solucan Yazılım, Kurtçuk), *Rootkits* (kendisini gizleyen, uzaktan denetim sağlayan yazılımlar).

Oltalama Saldırısı (*Phishing*)

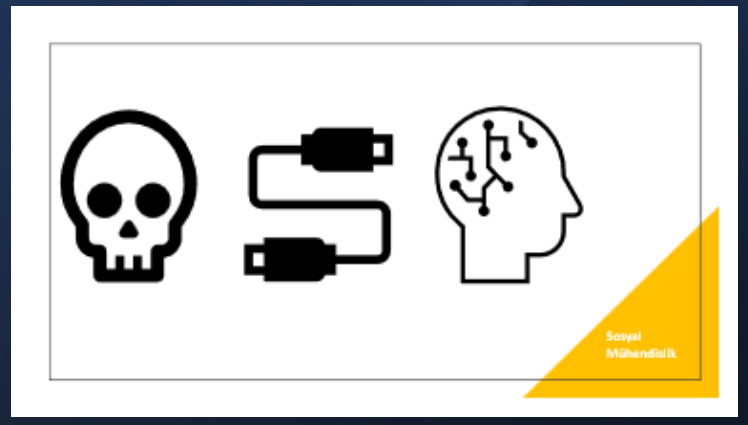
- Oltalama saldırısı, genellikle kimlik bilgileri ve kredi kartı numaraları olmak üzere kullanıcı verilerini çalmak için kullanılan bir tür sosyal mühendislik saldırısıdır. Güvenilir bir kişi kılığına giren saldırgan gönderdiği bir e-posta, anlık ya da kısa ileti ile hedef aldığı bireyi kandırır.
- Hedef alınan birey bu iletilerde yer alan bağlantı ya da eklentileri açtığında bilgisayarına saldırgan tarafından hazırlanmış kötücül yazılım yerleşir; oltalama saldırısı amacına ulaşır.

Dağıtımlı Hizmet Durdurma (DDOS) Saldırısı

- DDoS saldırısı hedef bir iletişim ağını ya da bilgisayar altyapısını bir İnternet trafiği seliyle baskılayarak bir sunucunun, hizmetin ya da ağın olağan trafiğini aksatmaya yönelik kötü niyetli bir girişimdir. Bir *DDoS* saldırısı, otobanı tıkayan beklenmedik bir trafik sıkışıklığını andırır, normal iletişim trafiğinin hedefine ulaşmasını engeller.
- DDoS saldırıları, saldırı trafiği kaynağı olarak birden çok ele geçirilmiş bilgisayar sistemi kullanılarak etkinlik sağlar. Kötüye kullanılan bilişim aygıtları; bilgisayarlar ve nesneağı [nesnelerin interneti: *IoT (Internet of Things)]* aygıtlarını ya da ağa bağlı diğer kaynakları içerebilir.



Sosyal Mühendislik



- Sosyal mühendislik, insan etkileşimleri yoluyla yapılan çok çeşitli ve kötü niyetli eylemler için kullanılan bir yöntemdir.
- Bu yöntem, kullanıcıları güvenlik yanlışları yapmaları ya da önemli bilgileri vermeleri için kandırmayı amaçlar.
- Sosyal mühendislik, siber saldırılar öncesinde hedefle ilgili bilgi toplamaya yönelik olarak yapılan bir ön çalışmadır, aynı zamanda.
- Saldırganlar bu yöntemle genellikle insani duyguları kötüye kullanırlar.

Siber Güvenlik Terimleri - devam

- **Derin Ağ** (*DeepWeb*)**:** Özel yazılımlarla ve yetkilendirmelerle erişilebilen bilgi ağlarıdır.
- **Karanlık Ağ** (*DarkNet* ya da *DarkWeb*)**:** Bir vekil sunucu (*Proxy, tor2web*) üzerinden, *candle, torch*, vb. yazılımlarla erişilebilen, İnternet'in gizli ve karanlık yüzüdür. Çalıntı kişisel bilgilerin ve uygunsuz içeriklerin yer aldığı, kaçakçılık ve silah satışı gibi amaçlarla kullanılan İnternet adresleri "karanlık ağ"dadır.
- **Tor:** "The Onion Routing" sözcüklerinin kısaltmasıdır; Türkçede "Soğan Tipi Yönlendirme" olarak adlandırılabilir. İnternet'e kimliksiz olarak erişim olanağı sağlayan ağ ve yazılım projesidir.
- **Derin Sahte** (*Deepfake*): Kişinin görüntüsünün başka bir kişinin ya da videoda yer alan bir kişinin görüntüsüyle değiştirilmesidir. Bu yapılırken ses ve görüntü uyumu için yapay zekâdan yararlanılmaktadır.
- **Sıfır Güven** (*Zero Trust*)**: "**Hiçbir kullanıcı ya da aygıta güvenme; her defasında doğrula" ilkesine dayanan güvenlik yaklaşımıdır.

Siber Tehdit İstihbaratı

- Siber tehdit istihbaratı, siber tehditlerle ilgili bilgilerin toplanması, çözümlenmesi ve yayılmasına odaklanan bir siber güvenlik çalışma alanıdır.

- Siber tehdit istihbarat kaynakları:
  - açık kaynaklar,
  - sosyal paylaşım uygulamaları,
  - insan kaynaklı istihbarat,
  - teknik istihbarat,
  - aygıtlarca üretilen günlük kayıtlar,
  - adli olaylar,
  - internet trafiği,
  - derin ve karanlık bilgiağları.

Güvenlik Operasyon Merkezi (SOC)

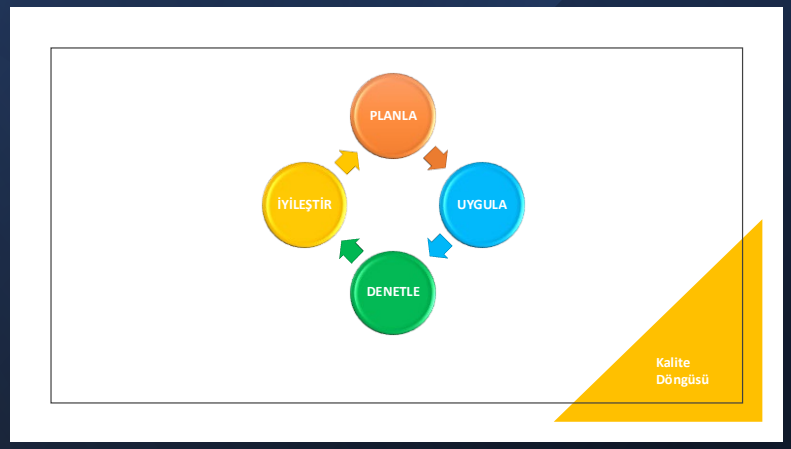
- Güvenlik Operasyon Merkezi, BT altyapısındaki çeşitli güvenlik olaylarını izlemek, tehditleri saptamak, çözümlemek ve bunlara yanıt vermek için oluşturulan merkezi bir güvenlik birimidir.
- Birincil amacı, siber saldırıların etkisini en aza indirmek, çok önemli verileri korumak ve bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamaktır.

Siber Dayanıklılık

- Siber dayanıklılık, bir kuruluşun siber saldırıları öngörme, bunlara karşı koyma, bunlardan kurtulma ve bunlara uyum sağlama yeteneğidir.


Siber
Güvenlik
Yönetimi

Güvenlik bir kalite hedefidir



Bir kuruluşta uygulanmakta olan siber güvenlik yönetim sürecinin olgunluğu kuruluşun güvenlik konusundaki yetkinliğini belirler.

Bir kuruluşta güvenlikle ilgili kalite hedefine ulaşabilmek için aşağıdaki süreçlerin doğru kurgulanması gerekir:

- Bilişim Altyapısının Tasarımı, Kurulumu, İşletimi
- Güvenlik Süreçlerinin Tanımlanması, Uygulanması
- İzleme ve Denetim
- Çalışanların Düzenli Eğitimi
- Süreç İyileştirme

Siber güvenlik yönetimi ilgili süreçlerin yönetimidir

Aşağıdaki bileşenlerce desteklenir:

- Siber Güvenlik Stratejisi
- Siber Güvenlik Politikaları
- İnsan Kaynakları Politikaları
- Teknoloji Politikaları
- Risk Yönetimi
- Önceliklerin Belirlenmesi
- Önlemlerin Geliştirilmesi
- Bütçe ve Finansman Desteği
- Denetim

Siber Güvenlik Sürecinin Yönetilmesi Neden Önemlidir?

Siber saldırılarla;

- Kuruluşların iletişim, yazılım, donanım altyapısı zarar görebilir; kuruluşlar maddi ve manevi kayıplara uğrayabilir.
- Siber saldırılarla bilişim altyapısı, belli bir süre için ya da sürekli olarak çalışamaz duruma getirilebilir.
- Kuruluşlarca işlenen ve saklanan veriler siber saldırganların eline geçebilir.
- Ele geçen bilgisayarlar saldırganlarca köle bilgisayarlar durumuna getirilebilir; bunlar, bir başka saldırı için atlama noktası olarak kullanılabilir.
- Kuruluşların güvenlik açıkları, bağlantılı oldukları diğer paydaşlara ait bilişim altyapılarına da zarar verebilir.
- Alınmayan önlemler nedeniyle yürürlükteki yasa ve düzenlemelere karşı aykırılıklar oluşabilir; kuruluşlar yaptırımlarla karşılaşabilir.

Siber Güvenlikle İlgili Düzenlemeler ve Amaçları

Ekonomik ve sosyal etkinliklerin sürdürülebilmesi için ortak güvenlik ölçütlerine göre ulusal ve uluslararası düzeyde hazırlıklı olunmasına, ortak planlama yapılmasına ve bilgi paylaşımına gereksinim vardır. Bu kapsamda hazırlanan ve onay gören metinlere uyumluluğun sağlanması gerekir.

Bu metinler,

- Siber güvenlik yeteneklerini geliştirme,
- Olay bildirme altyapısını oluşturma,
- Kriz yönetimi,
- Risk yönetimi,
- Veri koruma,
- Denetleme ve değerlendirme,
- İşbirliği olanaklarını geliştirme (eğitimler, tatbikatlar vb.) gibi süreçlerin işletilmesinde yardımcıdırlar.

Düzenlemeler ve Amaçları

- Kişisel Verilerin Gizliliği ve Korunması
- Siber Suçla Mücadelede İşbirliği
- Vatandaş Güvenliği
- Siber Suçlara İlişkin Uluslararası Anlaşmalar
- Kurumsal Bilgi Güvenliği Politikası
- Bölgelerarası Güvenli Bilgi Akışı
- Kurumlararası Güvenli İletişim
- Siber Güvenlik Yönergeleri
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı
- Bölge Ülkeleri Arasında Güvenli Bilgi Akışı

Siber Güvenlikle İlgili Standartları Hazırlayan Kuruluşlar

Etik Kurallar → Standartlar → Yasal Düzenlemeler

Siber güvenlik kapsamında uluslararası düzeyde yararlanılabilecek standartları hazırlayan belli başlı kuruluşlar aşağıda verilmektedir :

- NIST- National Institute of Standards and Technology
- ISO- International Organization for Standardization
- IEC- International Electrotechnical Commission
- SANS- SysAdmin, Audit, Network and Security
- CSC- Computer Sciences Corporation
- ISACA- Information Systems Audit and Control Association

Bilgi ve İletişim Alanlarını İlgilendiren Düzenlemeler

- 5846 sayılı Fikir ve Sanat Eserleri Kanunu (2001)
- 5070 sayılı Elektronik İmza Kanunu (2004)
- Türk Ceza Kanunu'ndaki "Bilişim Alanında Suçlar" Hk. Hükümler (2005)
- 5651 sayılı İnternet Yayınları ve Suçları Hk. Kanun (2007)
- 5809 sayılı Elektronik Haberleşme Kanunu (2008)
- 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun (2014)
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hk. Kanun (2014)
- 6698 Kişisel Verilerin Korunması Kanunu (2016)
- Bunlara ek olarak uluslararası yükümlülükler ve ilgili yönetmelikler

KVKK Kapsamında Alınması Gereken Teknik Önlemler

- Yetki Matrisi Oluşturma
- Yetki Kontrol Erişim Kayıtlarını Tutma
- Kullanıcı Hesap Yönetimi Altyapısını Oluşturma
- Ağ Güvenliği Altyapısını Oluşturma
- Uygulama Güvenliği Altyapısını Oluşturma
- Şifreleme Altyapısını Oluşturma
- Sızma Testi Yaptırma
- Saldırı Tespit ve Önleme Sistemleri Konumlandırma
- Sistem Olay (Log) Kayıtlarını Tutma
- Veri Maskeleme
- Veri Kaybı Önleme Yazılımlarını Kurma
- Yedekleme Yapma
- Güvenlik Duvarları Konumlandırma
- Güncel Anti-Virüs Sistemlerini Kullanma
- Veri Silme, Yok Etme ya da Kimliksizleştirme (anonim hale getirme) Süreçlerini Uygulama
- Anahtar Yönetimi Yapma

KVKK Kapsamında Alınması Gereken İdari Önlemler

- Kişisel Veri İşleme Envanterinin Hazırlanması
- Kurumsal Politikaların (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.) Oluşturulması
- Veri Sorumluları Arasındaki Sözleşmelerle Veri Sorumlusu ve Veri İşleyenler Arasında İmzalanacak Sözleşmelerin Güncellenmesi
- Gizlilik Taahhütnamelerinin Güncellenmesi
- Kurum İçi Periyodik ve/veya Rastgele Denetimlerin Planlanması
- Risk Analizlerinin Yapılması
- İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi) Gibi Belgelerin Güncellenmesi
- Kurumsal İletişimin (Kriz Yönetimi, Kurum'u ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.) Güçlendirilmesi
- Eğitim ve Farkındalık Çalışmalarının (Bilgi Güvenliği ve Kanun) Yapılması
- Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim Yapılması

Siber Güvenlik Çalışma Alanları

- Bilgi Güvenliği Yönetişimi
- Bilgi Güvenliği Mimarisi
- Siber Güvenlik Mühendisliği
- Siber Güvenlik Olay İzleme ve Önleme
- Tersine Mühendislik / Zararlı Yazılım Çözümleme
- Siber Bilgi Toplama (İstihbarat)
- Siber Güvenlik Sızma Testleri
- Şifreleme (*Crypthology*)
- Kimlik ve Erişim Yönetimi
- Adli Bilişim
- Mobil Güvenlik, Nesneağı Güvenliği, Bulut Güvenliği, Yapay Zekâ Güvenliği
- Bilgi Güvenliği Risk Yönetimi
- Siber Güvenlik İçin İnsan Kaynağı Yetiştirme
- Siber Güvenlik Konusunda Bilinç Düzeyini Artırma ve Duyarlılığı Geliştirme
- Ulusal ve Uluslararası Düzenlemelere, Standartlara ve Denetim Çerçevelerine Uyum

Siber Güvenlik Altyapısında Çevre Güvenliği

- Güvenlik Duvarı (FW)
- Saldırı Önleme Sistemleri (IPS/IDS)
- DDoS Önleme Sistemleri
- Web Uygulama Güvenlik Duvarı (*WAF: Web Application Firewall*)
- Gelişmiş Kalıcı Saldırı Önleme Sistemleri (*APT: Advanced Persistent Threat*)
- Sızma Testleri

Siber Güvenlik Altyapısında Sistem Güvenliği

- Zararlı Yazılım Koruma Sistemi
- Şifreleme Sistemleri
- Merkezi Sertifikasyon Sistemi
- PKI (Açık Anahtar Altyapısı)
- Yazılım Güvenlik Denetimi
- Güvenli Uzaktan Bağlantı Sistemi
- Tek Seferlik Parola Üretim Sistemi
- Veri Sızıntısı Önleme Sistemi
- Veri Sınıflandırma Yazılımı
- Taşınabilir Aygıt Yönetim Sistemi
- Ağ Erişim Kontrol (NAC) Sistemi
- Kablosuz (*Wireless*) Güvenlik Sistemleri
- Sistem Güçlendirme

Siber Güvenlik Altyapısında Kimlik ve Erişim Yönetimi

- Kimlik Yönetim (IDM) Sistemi
- Erişim Yönetim (AM) Sistemi
- Yetkili Erişim Yönetim (PAM) Sistemi
- Yetki Gözden Geçirme Sistemi

Siber Güvenlik Altyapısında Güvenlik Bilgisi ve Olay Yönetimi

- Güvenlik Bilgisi ve Olay Yönetimi (SIEM) Sistemi
- Olay İzleme ve Önleme Araçları
- Siber Bilgi Toplama Araçları (TI)
- Zararlı Yazılım Çözümleme Araçları
- Zayıflık Yönetim Sistemleri

Siber Güvenlik Altyapısında Bilgi Güvenliği Yönetişimi

- Bilgi Güvenliği Yönetim Sistemi
- Güvenlik Politikası
- Uyum (Standartlar, Düzenlemeler, Yönergeler)
- Farkındalık Eğitimleri
- Risk Yönetimi

Temel Güvenlik İlkeleri

Kurum ve kuruluşlarda oluşturulması planlanan siber güvenlik altyapısı için aşağıdaki temel ilkelerin öncelikli olarak göz önünde bulundurulması gerekmektedir:

- Güvenlik hedeflerinin iş hedefleriyle uyumluluğu
- Uygun ve güncel teknoloji kullanımı
- Derinlemesine savunma yöntemlerinin kullanılması
- Güvenlik temelli tasarım
- Kişisel gizlilik temelli tasarım
- Bilmesi gereken ilkesinin uygulanması
- En az yetki düzeyinde çalışma
- Saldırı yüzeyinin küçültülmesi
- En zayıf halkanın belirlenmesi
- Güvenlik yönetiminin yetkin çalışanlarca yürütülmesi

Saldırı Yüzeyini Küçültmenin Yolları

Saldırı yüzeyinin küçültülmesinde izlenmesi gereken ana konular aşağıda verilmektedir:

- Altyapıdaki karmaşıklığının ortadan kaldırılması
- Güvenlik açıklarının saptanması, önlem alınması
- Ağın bölümlere ayrılması; bölümlerin birbirinden yalıtılması
- Gereksiz bağlantı noktalarının kapatılması

Siber Güvenlik Uzmanlıkları

- Siber Güvenlik Danışmanı
- Siber Güvenlik Mimarı
- Siber Güvenlik Mühendisi
- Siber Güvenlik Olay İzleme / Önleme Uzmanı
- Tersine Mühendislik / Zararlı Yazılım Çözümleme Uzmanı
- Siber Güvenlik Sızma Testi Uzmanı
- Kırmızı Takım (Siber Atak) Mühendisi
- Mavi Takım (Siber Savunma) Mühendisi
- Bilgi Güvenliği Risk Yöneticisi
- Şifreleme (*Crypthology*) Uzmanı
- Adli Bilişim Uzmanı
- Siber Güvenlik Denetim Uzmanı
- Güvenli Yazılım Denetçisi
- Zayıflık Yönetimi Uzmanı
- Bilgi Güvenliği Uyum Uzmanı

Siber güvenlikte göz ardı edilmemesi gereken konular

Siber güvenliğin çoğu kez yalnızca teknik önlemlerle sağlanabileceğine ilişkin yanlış bir kanı bulunmaktadır. İşte bu yönüyle dikkate alınması gereken kimi konular aşağıda özetlenmektedir:

Bütçe: Siber atakların gerçekleştirilmesi kolay ve ucuz, savunması ise zor ve pahalıdır. Siber güvenliğe yeterli bütçe ayrılabilmelidir.

Eğitim: İlk ve orta öğretimden başlayarak anne ve babaları da kapsayacak şekilde sanal ortamda dikkat edilecek konularda farkındalık oluşturulmalıdır.

Danışmanlık: Mevcut durumu görebilmek ve nereden başlamak gerektiği sorusuna yanıt verebilmek için danışmanlık alınması değerlendirilmelidir.

Risk Yönetimi: Riskleri azaltma, ortadan kaldırma ve aktarma (transfer etme) konuları değerlendirilmelidir.

Sigortalama: Siber güvenlik risklerinin aktarılması (transfer edilmesi) için sigortalama konusu değerlendirilmelidir.

Yasal Düzenlemeler: Siber güvenliğe ilişkin yasal düzenlemelere uyum gözetilmelidir.

Kurumlararası İşbirliği: Sorunların hızlı çözümü için kurumlar arasında bilgi paylaşımı ve işbirliği yapılmalıdır.

Uluslararası İşbirlikleri: Siber dünyada sınırların olmadığı dikkate alındığında, yukarıda ifade edilen işbirliği ülkeler açısından da geçerlidir.

Kritik altyapılar: Ülke genelindeki kritik altyapı bileşenleri açısından risk öncelik sırası belirlenmeli, koruma önlemleri alınmalı ve düzenli sınama çalışması yapılmalıdır.

Strateji ve politikalar: Taktik önlemlerin stratejik hedefler konulmadan başarıya ulaşması beklenmemelidir. Alınacak önlemler strateji ve politikalarla desteklenmelidir.

Bireyleri Hedef Alan Tehditler ve Önlemler

Saldırılar ağırlıklı olarak bireyleri hedef alıyor.

Birey düzeyinde alınabilecek önlemler neler?

2025, 1. Çeyrek istatistiklerine göre(*),

- Siber saldırıların %4'ü siber savaş kapsamında gerçekleşmiş (nedenler:politik, jeopolitik, ekonomik çatışmalar).
- Saldırılar büyük oranla (%71'le) siber suçlar kapsamındadır.
- Bu sınıftaki saldırılar ağırlıklı olarak bireyleri hedef almaktadır.
- Geriye kalan %11, siber istihbarat, siber bilgi toplamadır.
- %5'i siber eylemdir (haktivizm).

(*) www.hackmageddon.com

Parola Güvenliği

- Bilgisayarlarda ilk kuruluşla birlikte gelen yetkili kullanıcı hesap ve parolaları değiştirilmelidir.
- Güçlü parola seçilmelidir. Başkalarınca tahmin edilmesi kolay olan doğum tarihi ya da kişi adı gibi özel bilgilerin kullanılmaması gerekir.
- Parolanın gücünü artırmak için büyük harf, küçük harf ve özel karakterler kullanılmalıdır; parolalar en az 8 karakterden oluşmalıdır.

parola	uzunluk (karakter)	tahmini kırılma süresi	güvensiz/riskli/görece güvenli/ güvenli
123456	6	dakikalar içinde kırılabilir	güvensiz; çok kısa, sadece sayılardan oluşuyor; çok bilinen ve çok kullanılan parolalardan …
qwerty123456	12	saatler içinde kırılabilir	riskli; sadece harf ve sayıları içeriyor .
qwerty:123456;	14	yıllar içinde kırılabilir	görece güvenli; boyu uzun, harf ve sayılara özel karakter eklenmiş ; ancak, bilinen kalıpları (qwerty, 123456) içeriyor.
ak:s391;xb86#t10	16	kırılması milyonlarca yıl sürebilir	güvenli: boyu daha uzun; harf, sayı ve özel karakterler i içermesi parolanın gücünü artırıyor.

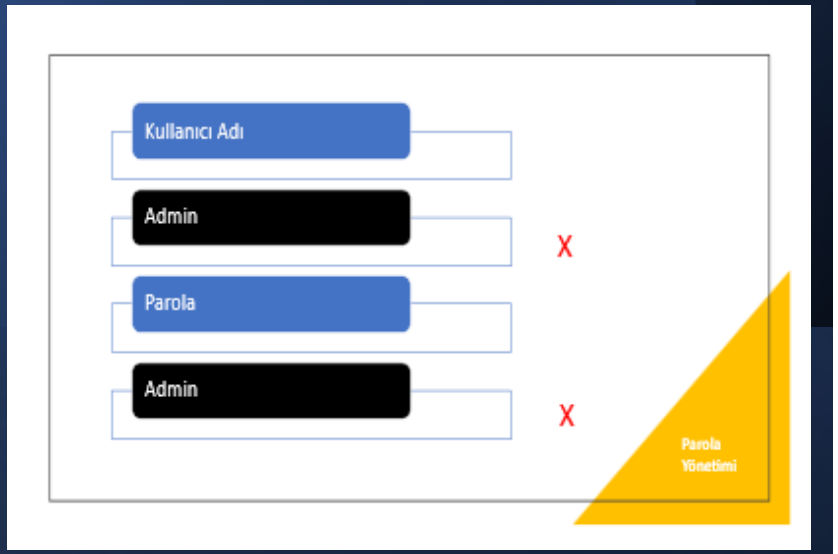
Parolanız ne kadar güvenli?

Parola Güvenliği

parola	uzunluk (karakter)	tahmini kırılma süresi	güvensiz/riskli/görece güvenli/ güvenli
123456	6	dakikalar içinde kırılabilir	güvensiz; çok kısa, sadece sayılardan oluşuyor; çok bilinen ve çok kullanılan parolalardan …
qwerty123456	12	saatler içinde kırılabilir	riskli; sadece harf ve sayıları içeriyor .
qwerty:123456;	14	yıllar içinde kırılabilir	görece güvenli; boyu uzun, harf ve sayılara özel karakter eklenmiş ; ancak, bilinen kalıpları (qwerty, 123456) içeriyor.
ak:s391;xb86#t10	16	kırılması milyonlarca yıl sürebilir	güvenli: boyu daha uzun; harf, sayı ve özel karakterler i içermesi parolanın gücünü artırıyor.

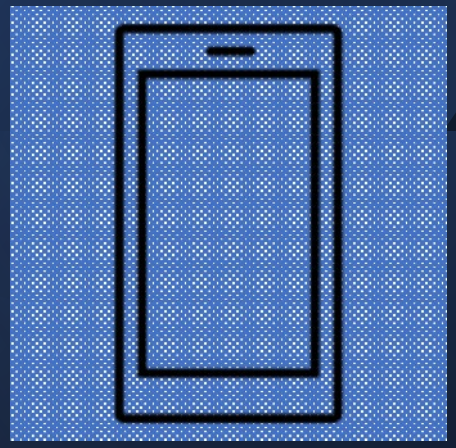
Parolanız ne kadar güvenli?

Parola Güvenliği



- Kolay hatırlayabildiğimiz, başkasının zor tahmin edebileceği bir parola kullanılmalıdır. Dünya genelinde en çok kullanılan ve kolay tahmin edilen parolalar şunlardır: 123456, *password, qwerty,* vb. Özellikle bu tür zayıf parolaların kullanımından kaçınılmalıdır.
- Tüm hesaplara aynı parolanın verilmesi alışkanlığından vazgeçilmelidir. Kurumsal hesaplar, sosyal paylaşım uygulamaları, banka hesapları, kişisel üyelikler ve e-ticaret siteleri için ayrı parolalar tanımlanmalıdır.
- Parolalar kimseyle paylaşılmamalıdır.

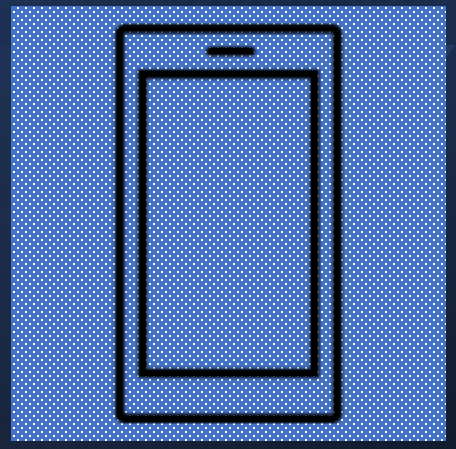
Akıllı Telefon Kullanımı

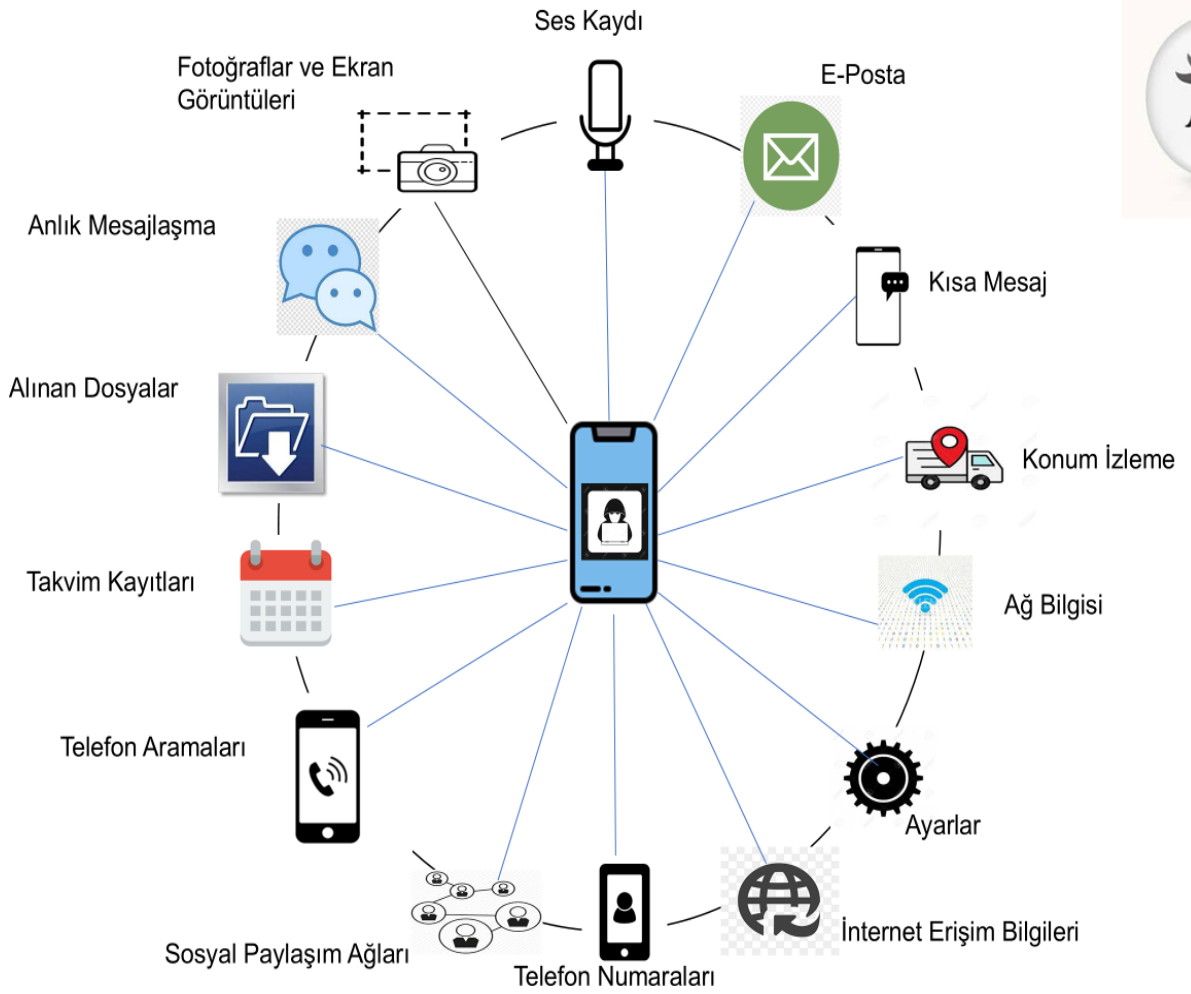


Akıllı telefonlarınızda alacağınız basit önlemlerle siber saldırıların kurbanı olmaktan kurtulabilirsiniz:

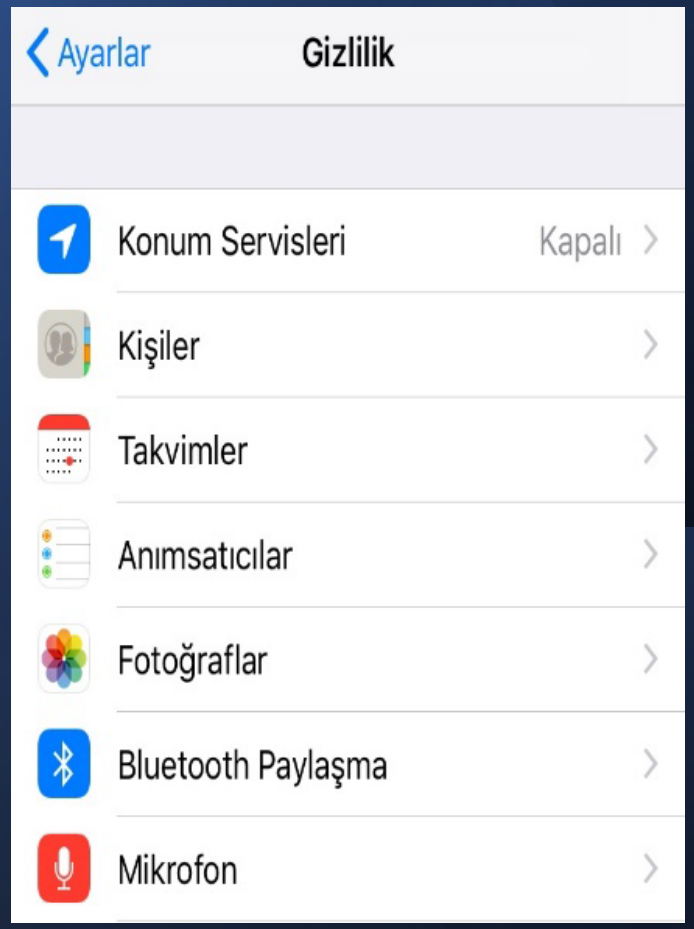
- Akıllı telefonlarımızın konum servisleri ve kişisel erişim noktası ile Wi-Fi ve Bluetooth paylaşımları yalnızca gereksinim olduğunda açılmalıdır.
- Akıllı telefon uygulamalarının kişisel bilgilerimize erişme isteğine karşı dikkatli olunmalıdır.
- Güvenilirliğinden emin olunmayan uygulamalar yüklenmemelidir.

Akıllı Telefon Kullanımı



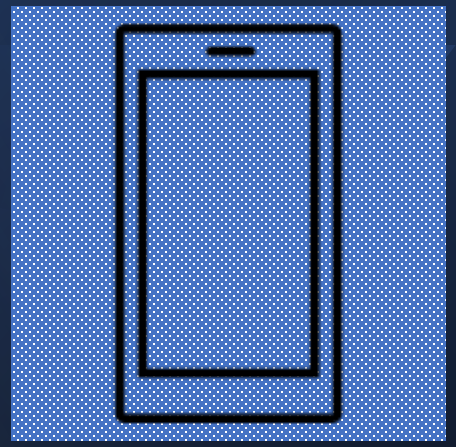


Akıllı Telefon Kullanımı



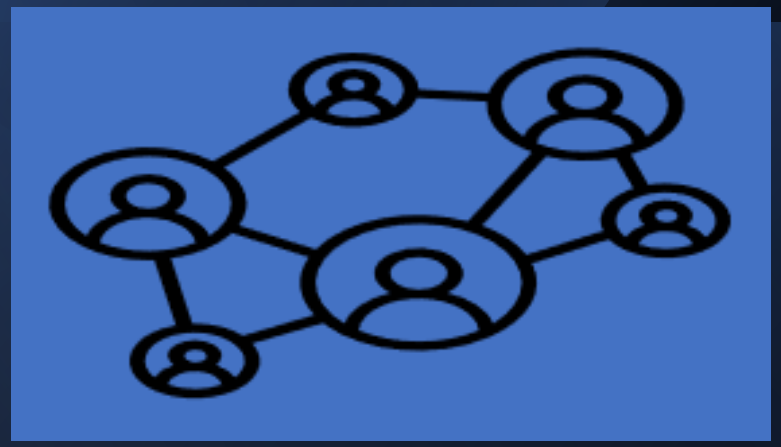
- İşletim sistemi ve uygulamalar güncel tutulmalıdır.
- Herkese açık kablosuz ağlara bağlanmaktan kaçınılmalıdır.
- Cep telefonu numarası gizli tutulmalıdır.
- Bilgiler iletişim ağlarında dikkatli paylaşılmalıdır.
- Kişisel bilgiler, belgeler veya önemli dosyalar telefonda saklanmamalıdır.
- Akıllı telefonlar elden çıkarılırken ilk satın alındıktan sonra yüklenen her şey silinmeli, telefon fabrika ayarlarına döndürülmelidir.

Akıllı Telefon Kullanımı



- Film dosyasında coğrafi olarak etiketlenen fotoğrafların sayısı sınırlandırılmalıdır.
- Akıllı telefonlar kullanılmadığı sürelerde kilitli tutulmalıdır.
- Güçlü parolalar kullanılmalıdır.
- Aygıtta bulunan güvenlik olanakları (varsa) kullanılmalıdır.
- Destekleniyorsa bir antivirüs uygulaması kullanılmalıdır.
- Uygulama izinleri yönetilmelidir; gerekli değilse mikrofon, kamera gibi izinler ilgili uygulamaya açılmamalıdır.
- Veriler düzenli olarak yedeklenmelidir.
- Telefon pili, bilgisayarınız ve arabanız gibi güvenilen bağlantı noktalarında doldurulmalıdır.
- İzin aşırılmış (*jailbreak*) telefonlar kullanılmamalıdır.

Sanal ortamdaki sosyal paylaşımlar



- Eğitim bilgileri (üniversite, lise, ilkokul vb.)
- İşyeri bilgileri (yöneticiler, elemanlar, arkadaşlar, iş çevresi vb.)
- Aile bilgileri (birinci derece yakınlar, ikinci derece yakınlar vb.)
- Uğraşlar
- Siyasi görüş
- Sağlık durumu
- Ticari değeri olan veriler

Sosyal Paylaşım ve İletişim Uygulamalarını Neden Kullanıyoruz?

- İletişim kolaylığı sağlaması
- Bilgiye hızlı erişilebilmesi
- Sosyalleşme aracı olması
- Çoğu uygulamanın ücretsiz olması!!!

Sosyal Paylaşım ve İletişim Uygulamalarının Kullanımında Nelere Dikkat Etmeliyiz?

- Kullanılan hesaplarda iki aşamalı (ya da çoklu) doğrulama yöntemi yeğlenmelidir.
- Paylaşılan bilgiler, resimler ve görüntüler dolandırıcılar ve suç örgütleri için çok şey anlatabilir; dikkatli olunmalıdır.
- Gizlilik ayarları (herkese açık, sadece arkadaşlara açık gibi) denetlenmeli, izinler sınırlı verilmelidir.

Kablosuz Ağlarda İletişim Güvenliği

Kablosuz ağlar diğer ağlara göre daha korunmasız olarak konumlandırılmış olabilir.

- Halka açık yerlerde kablosuz bağlantı ile ücretsiz İnternet kullanımında dikkatli olunmalıdır. Bu tip bağlantıların pek çoğu güvenlik risklerine açıktır; çoğu bağlantı şifresizdir.
- İstemcide, doğrudan bağlanma (otomatik bağlantı) seçeneği kullanılmamalı, bağlantı denetimli yapılmalıdır.

Modem Güvenliği

- İlk modem parolası değiştirilmelidir.
- Kablosuz ağın güvenliğini sağlamak için her zaman WPA2 kullanılmalıdır.
- Kablosuz ağ adres bilgileri dış dünyadan gizlenmelidir.
- WPS (yönlendirici üzerindeki bir düğmeyle parola olmadan -doğrudan- bağlanma) devre dışı bırakılmalıdır.
- Riskli veya doğrulanmamış hizmetler kullanılmamalıdır (Örneğin; Evrensel Tak ve Çalıştır (UPnP), uçtan uca ağ bağlantısı için TCP/IP kullanan dağıtımlı, açık bir ağ standardıdır.)

Kişisel Bilgisayar Güvenliği

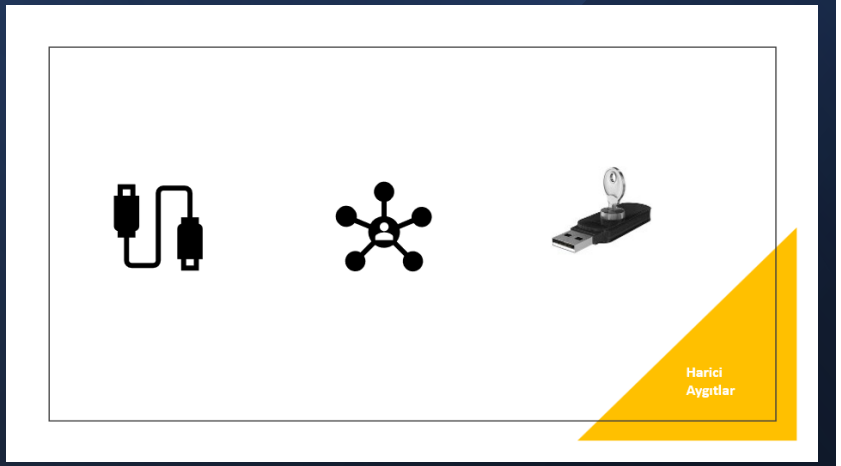
- Lisanslı yazılımlar kullanılmalıdır.
- Yazılım güncellemeleri düzenli olarak yapılmalıdır.
- Kişisel güvenlik paketi kullanılmalıdır.
- Sorun belirleme ve güvenlik analizleri için bilgisayarlarda sistem ve güvenlik kayıtlarının alındığından (log) emin olunmalıdır.
- Kullanmadığımız zamanlarda bilgisayarlarımızın ekranları kilitli tutulmalıdır.
- Açılan oturumlarda “beni hatırla” seçeneği kullanılmamalıdır.
- Tarayıcı ayarlarında zararlı bileşenlere önlem olarak, otomatik açılan pencereler engellenmelidir.

Kurumsal Bilgisayar Güvenliği

Kişisel bilgisayar güvenliği konusunda söz edilenlere ek olarak;

- Kurumsal bilgisayarlar kişisel amaçlı kullanılmamalıdır.
- Kurumsal e-posta adresleri, çevrimiçi alışveriş sitelerinde ya da özel amaçlı iletişim topluluklarında paylaşılmamalıdır.
- Kurumsal bilgisayarlarda Yerel Yönetici (Local Administrator) yetkileri ile çalışılmamalıdır.

Taşınabilir Bilişim Aygıtlarının Güvenliği



- Dizüstü bilgisayar, tablet, harici bellek ve akıllı telefonların unutulma ya da çalınma risklerine karşı veriler, şifreli olarak saklanmalıdır.
- Açılışlarında güçlü parola ve biyometrik araçlar kullanılmalıdır.
- Virüs ya da zararlı yazılım çekincesi nedeniyle CD'ler, USB bağlantılı aygıtlar paylaşılmamalıdır.

Sosyal Mühendislik Saldırılarına Karşı Alınabilecek Önlemler

- E-posta, SMS, X (eski Twitter), Facebook, Instagram iletilerinin kaynağının güvenilir olduğundan emin olunmalıdır.
- İleti yoluyla gelen bağlantılara tıklanmamalı, adres kısmı kopyalanarak tarayıcıya yazılmalı, güvenli bir bağlantı olup olmadığı (SSL -Secure Sockets Layer- Sertifikası) kontrol edilmeli, erişilen sayfalarda kişisel bilgilerin istenmesi durumunda giriş yapılmamalı, iletişim protokolünün çevrimiçi alışveriş sitelerinde "https", dosya indirirken "secure ftp (sftp)" olmasına dikkat edilmelidir.
- Bankadan arıyor süsü vererek hesap parolalarını soran kişilere güvenilmemelidir.
- Fidye saldırılarına karşı bir önlem olarak önemli görülen bilgiler (kaybından zarar göreceğimizi düşündüğümüz) düzenli olarak yedeklenmelidir.
- Kullanılmayan hesaplar kapatılmalıdır.
- Üzerinde kişisel bilgilerin olduğu belgeler imha edileceği zaman kâğıt kırpma makinesinde okunamaz duruma getirilmelidir.

İnternette dolaştığımız sayfaların güvenli olup olmadığını nasıl anlarız?

- Bağlantı yapılan sayfalarda HTTPS olmasına dikkat edilmelidir.
- Sayfadaki gizlilik politikası okunmalı; kişisel verilerin nasıl toplandığı, kullanıldığı ve korunduğu konusunda bilgi edinilmelidir.
- Sayfadaki iletişim bilgileri denetlenmelidir.
- Sayfanın güven damgası doğrulanmalıdır.
- Kötücül yazılımların neden olabileceği temel göstergelere dikkat edilmelidir.

Sayfaya yapılmış belirgin dış müdahale belirtileri,

- Açılıp kapanan şüpheli pencereler,
- Kötü amaçlı reklâmlar (Bazı kötü amaçlı reklâmların yakalanması kolaydır. Bunlar genellikle yazım / dilbilgisi hataları içerirler, "mucize" tedavileri veya ünlü skandallarını ya da göz atma geçmişinizle eşleşmeyen ürünleri barındırırlar.),
- Kimlik avı (yasal görünebilirler, ancak yazım ve dilbilgisi yanlışları onları ele verir. Ek olarak kötü amaçlı yönlendirmeler barındırırlar.),
- Arama motoru uyarıları,
  - Bazı çok bilinen arama motorları, İnternet sayfalarını kötü amaçlı yazılımlara karşı tarar ve siteye kötü amaçlı yazılım bulaşmışsa bir uyarı yerleştirirler.

E-Toplantı Yazılımları Konusunda Alınabilecek Önlemler

- Kurumsal yazılım ürünleri tercih edilmelidir.
- Yazılımın güncel sürümleri kullanılmalıdır.
- Üye olunurken diğer sosyal paylaşım ortamlarının hesapları bağlantı yöntemi olarak kullanılmamalıdır.
- Parola korumalı toplantılar düzenlenmelidir.
- Girişte zor parola kullanılmalıdır.
- Sabit toplantı kimliği yerine her defasında yeniden üretilen toplantı kimlikleri kullanılmalıdır.
- Katılımcılar davet sahibince bekleme odasına alınmalı, yalnızca daha önceden belirlenen katılımcılar toplantıya alınmalıdır.
- Toplantılarda gizli içerik paylaşılmamalıdır.
- Toplantı başlamadan önce katılımcıların ekran ve dosya paylaşım yetkileri sınırlandırılmalıdır.
- Açık bağlantı adresi sanal ortamda yayımlanmamalıdır.


Siber
Güvenlikte
Fiziksel
Güvenlik

Siber Güvenlikte Fiziksel Güvenlik

1. Fiziksel Erişim Denetimi
2. Çalışma Alanlarının ve Tesislerin Güvenliğinin Sağlanması
3. Dış ve Çevresel Tehditlere Karşı Koruma
4. Yüksek Güvenlik Gerektiren Alanlarda Çalışmak
5. Dağıtım ve Yükleme Alanlarında Alınması Gereken Güvenlik Önlemleri

Fiziksel Erişim Denetimi

- Ziyaretçi giriş ve çıkışları uygun bir yöntemle kayıt altına alınmalıdır.
- Önemli noktalara erişimler kısıtlanmalı, dahası birden çok denetim önlemi alınmalıdır (Örneğin, Kart ve şifre).
- Kuruluş çalışanlarının, yüklenicilerin, varsa üçüncü şahısların ya da ziyaretçilerin kimlik kartlarını takmaları istenmelidir. Bu kartlar için ayrı renk ve desenler kullanılabilir.
- Dış destek için gelenlere verilen erişim yetkileri sınırlandırılmalıdır.
- Erişim yetkileri düzenli olarak gözden geçirilmeli ve kayıt altına alınmalıdır.

Çalışma Alanlarının ve Tesislerin Güvenliğinin Sağlanması

- Önemli veriler içeren çalışma odalarında erişim ile ilgili gerekli denetimler yapılmalıdır.
- Dışarıdan dinlemeye karşı gerekli önlemlerin alınması sağlanmalıdır.
- Sistem odası gibi önemli veri veya bilgi içeren yerler için ayrıntılı, açıklayıcı etiketlerden kaçınılmalıdır.
- Gizli bilgiler içeren yerlerin kat planları, konumu ya da iletişim bilgileri erişime kapatılmalıdır.
- Çok yüksek gizlilik içeren alanlarda elektromanyetik korumanın kullanılması konusu değerlendirilmelidir.

Dış ve Çevresel Tehditlere Karşı Koruma

- Deprem, sel, patlama, yangın, toplumsal olaylar ve doğal ya da insan kaynaklı yıkımlardan korunmak için güvenlik önlemleri alınmalıdır.
- Çevresel tehditler dikkate alınmalıdır (Örneğin, dış ortamdaki komşu şirketler, benzin istasyonu vb.).

Yüksek Güvenlik Gerektiren Alanlarda Çalışmak

- Güvenli alanlar olarak adlandırılan yerler için erişim denetim koşulları belirlenmelidir.
- Kamera, cep telefonu gibi kayıt aygıtları gizlilik gerektiren alanlara alınmamalıdır.
- Önemli veri ya da bilgilerin olduğu bir ortamda dış hizmet alınacaksa, çalışma bir refakatçi eşliğinde yapılmalıdır.

Dağıtım ve Yükleme Alanlarında Alınması Gereken Güvenlik Önlemleri

- Bina dışından yükleme ve dağıtım alanlarına erişim, belirlenen yetkili çalışanlar ile sınırlandırılmalıdır.
- Dağıtım ve yükleme alanlarının dış kapıları, iç kapılar açıldığında kapatılmalıdır.
- Teslimat için gelen araçların türü ne olursa olsun, herhangi bir tehlikeli madde içerip içermediği denetlenmelidir.
- Giren ürün / malzeme ne olursa olsun kaydedilmelidir.
- Gelen ürünün doğruluğu denetlenmeli, yolda herhangi bir değişiklik ya da bozulma tespit edilirse ilgili çalışana bilgi verilmelidir.
- Mümkünse, gelen ve giden gönderiler fiziksel olarak ayrılmalıdır.
- Kurum veya kuruluş içinde dışarıdan ulaşılabilen tüm noktalarda ek güvenlik önlemleri (acil çıkışlar gibi) alınmalıdır.

Siber Saldırılardan Çıkarılan Dersler

“Bir Fidye Yazılımı Saldırısı” ve Çıkarılan Dersler

- 2017 yılında ortaya çıkan Wannacry adlı kötücül yazılım bir fidye yazılımıydı; dosyaları şifreleyip yeniden açılması için para istiyordu; Windows’un SMB (Server Message Block) servisinin zafiyetini kullanıyordu (MS17-010, CVE-2017-0144).
- Saldırılardan bir süre önce, siber korsan topluluklarından biri olan TheShadowBrokers, NSA’in (National Security Agency, ABD) FUZZBUNCH istismar yazılımını sızdırmıştı.
- FUZZBUNCH’ın içindeki EternalBlue ve DOUBLEPULSAR istismar yazılımları kullanıldığında SMB açığı üzerinden yönetici haklarında komut çalıştırılabiliyordu.

“Bir Fidye Yazılımı Saldırısı” ve Çıkarılan Dersler

- Sözkonusu güvenlik açığını kullanan Wannacry ile dünya, bir sıfırıncı gün saldırısını yaşamış oldu.
- O anda Win XP, Win 7, Win 10, Win Server 2008, 2012, 2016 işletim sistemlerinde SMB açığı bulunuyordu. Win XP’nin ise o tarihte üretici firma desteği tamamen uygulamadan kalkmış durumdaydı.
- Saldırılardan en az 57 ülke etkilendi. Rus polisinin bilgisayarları kilitlendi, Avusturalya’da hız kameraları çalışmadı. Wannacry’ın türevi olan Petya, Ukrayna’da altyapı bakanlığını, posta hizmetlerini, büyük bir telefon şirketini ve çeşitli bankaları etkiledi. Bu yazılımların bir başka türevi olan Bad Rabbit; Rusya, Türkiye, Almanya ve Ukrayna’yı olumsuz etkiledi.

“Bir Fidye Yazılımı Saldırısı” ve Çıkarılan Dersler - Önlemler

- E-postalarla gelen bağlantıları doğrudan açmamak
- Güvenilmeyen kaynaklardan dağıtımı yapılan uygulamaların kuruluşlarını yapmamak
- Yazılım sürümlerini güncel tutmak
- Yama yönetimi altyapısını oluşturmak
- Yama yönetim sürecini güçlü bir şekilde uygulamak
- Ağdaki olağandışı hareketleri düzenli olarak gözlemlemek
- Kullanıcı yetkilerini düzenli olarak gözden geçirmek

“Bir Tedarik Zinciri Saldırısı” ve Çıkarılan Dersler

- 2020’nin sonlarında SolarWinds ürünlerini kullanan ve güncel yamalarını indiren kuruluşlar farklı isimlerdeki benzer kötücül yazılımlarla karşılaştı.
- Sunburst, Sunspot, Teardrop, Raindrop, Supernova, Cosmicgale bu adlardan bazılarıydı.
- Kötücül yazılım bulaştırılan güncelleme sunucusundan yama indirenler, gerçekte farkında olmadan arkakapı (backdoor) güncellemesi indirmiş oldular.
- Saldırıdan, SolarWinds firmasının 18.000’e yakın müşterisi etkilendi.

“Bir Tedarik Zinciri Saldırısı” ve Çıkarılan Dersler

solarwinds123

- Kötücül yazılım karmaşıktı; iki hafta uykuda kalmış, bu tür saldırılara karşı kuruluşlarda konumlandırılan tehdit yalıtma aygıtlarına (sandbox) takılmamıştı.
- Hedef sunucuya bulaştıktan belli bir süre sonra komuta ve denetim merkezi ile bağlantı kuran yazılım, bulaştığı sistemdeki hesap bilgilerini toplamaya ve merkeze iletmeye başlayacaktı.

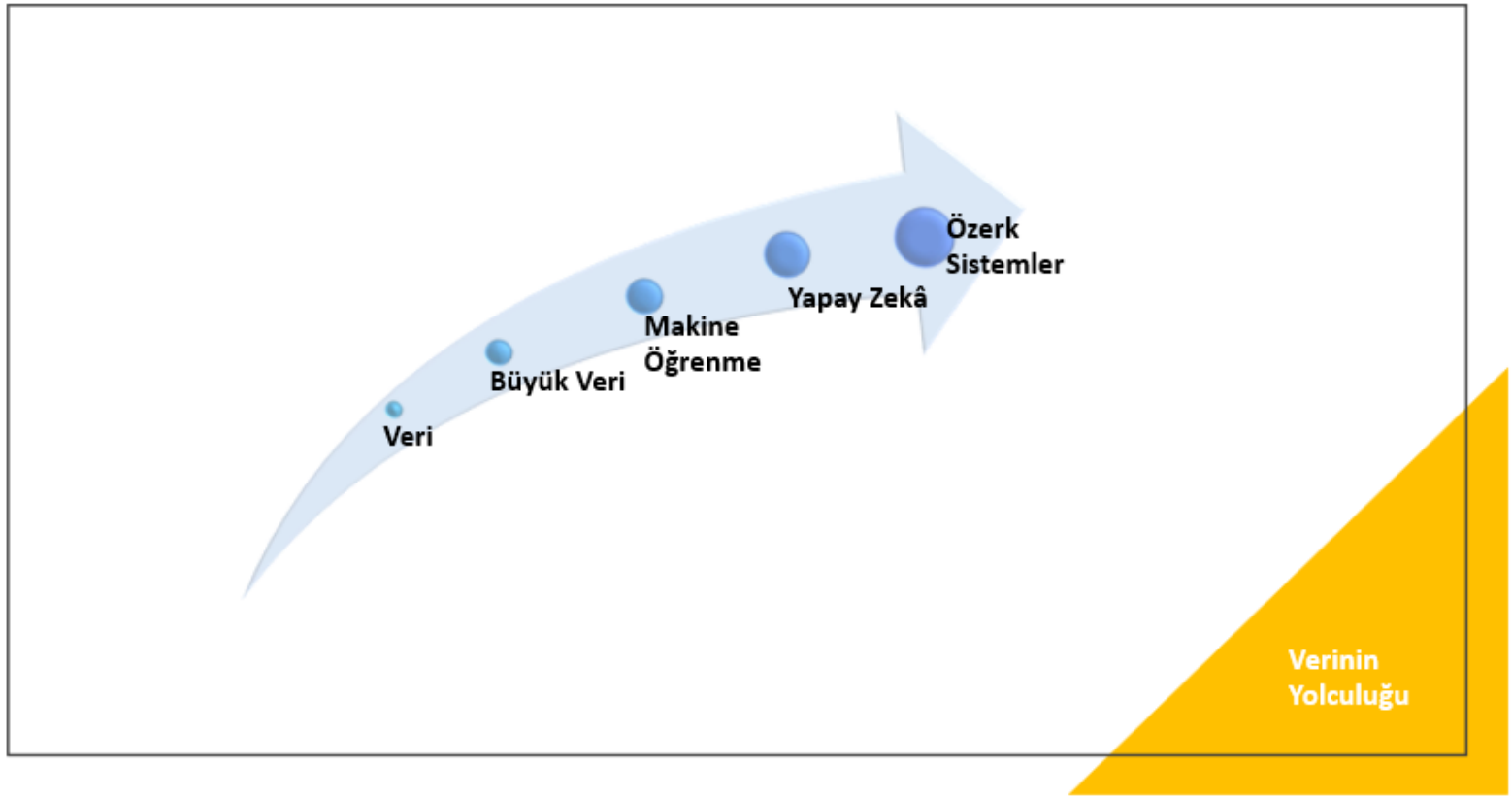
“Bir Tedarik Zinciri Saldırısı” ve Çıkarılan Dersler - Önlemler

solarwinds123

- Kolay tahmin edilebilecek parolaları kullanmamak
- Parolaları sık ve düzenli olarak değiştirmek (Bunun için parola yönetim yazılımları kullanılabilir.)
- Parolaları, süreleri hiç dolmayacak şekilde tanımlamamak
- Parolaları başkalarıyla paylaşmamak
- Yazılım ve donanımlarla gelen parolaları değiştirmek
- Bir güvenlik doğrulamasıyla yetinmeyip, iki aşamalı (/çoklu) kimlik doğrulama yöntemlerini kullanmak (Bunun için tek seferlik parola (OTP) ya da biyometrik araçlar; parmak izi, iris tarama gibi yöntemler kullanılabilir.)
- Ağdaki olağandışı hareketleri düzenli olarak gözlemlemek, raporlamak, değerlendirmek
- Kullanıcı yetkilerini düzenli olarak gözden geçirmek
- Siber istihbarat olanaklarından yararlanmak


Yeni Teknolojiler ve Siber Güvenliğe Etkisi

Verinin Yolculuğu



Yapay Zekâ ve Kuantum Bilgisayarlar Siber Güvenlikte Oyunun Kurallarını Yeniden Yazdıracak

- 2009 Bulut Bilişim
- 2013 Büyük Veri, Nesnelerin İnterneti
- 2015 Özerk Sistemler
- 2016 Makine Öğrenme
- 2017 YZ, Gelişmiş Derin Öğrenme, Blokzincir
- 2019 YZ Destekli Yazılım Geliştirme, Kuantum Bilişim
- 2021 YZ Mühendisliği, Davranışların İnterneti
- 2022 YZ Güvenliği, Üretken YZ (verilerden yeni veri üretme, insanımsı yazı, görüntü)
- 2023 Uyarlanır YZ, YZ Risk ve Güvenlik Yönetimi
- 2024 YZ Risk ve Güvenlik Yönetimi
- 2025 Kuantum Sonrası Kriptografi

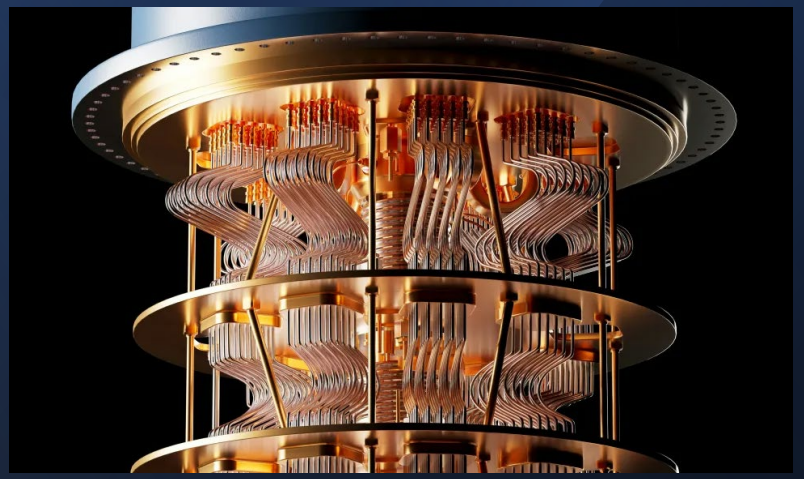
Yapay Zekâ ve Siber Güvenlik

YZ;
İnsan hatalarını azaltmada,
Doğru karar ve sonuç almada,
Benzetim – simülasyon yapmada,
Örnek senaryoların uygulanmasında daha etkili duruma gelecek.

YZ;
İzleme, tehdit saptama ve önleme süreçlerin kotarılmasında,
Güvenlik açıklarının saptanması ve yönetilmesinde,
Tehdit istibaratının toplanmasında,
Siber güvenlik otomasyonunda,
Şifre yönetiminde,
YZ destekli güvenli kod geliştirmede,
Risk çözümlemede,
Güvenlik eğitimleri düzenlenmesinde ve değerlendirilmesinde,
Sızma testlerinin, kırmızı takım simülasyonların yapılmasında,
Olay çözümlemede kullanılabilir.

Kötü taraf: sosyal mühendislik, yanıltıcı bilgi, saldırı öncesi keşif, sömürü (exploit) yazılımları geliştirme ve siber saldırılar…

Kuantum Bilgisayarlar ve Siber Güvenlik



Kuantum bilgisayarlarla;

Kriptolama / kripto çözme,

Eniyileme,

DNA dizilimi,

İlaç etkileşimleri, vb.

işlemler daha hızlı sonuçlandırılacak.

Kriptografi kırılmazlık algısına dayanır,

Kuantum bu algıyı yıkıyor!!!

RSA 2048 bit şifrelemeyi kırmak için 300 trilyon yıl gerekiyor. Kuantum bilgisayar 4096 kararlı kübitle bunu 10 sn'de yapılabiliyor.

Kuantum Bilgisayarlar ve Siber Güvenlik

Q-day/k-günü/kuantum günü:
Binlerce yıl sürecek işlemler sn'ler içinde tamamlanabilir.

2024 yılında Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) kuantum sonrası şifreleme standartları belgesini yayımladı.

- Kuantumun etkilerini azaltmayı amaçlıyor.

Kuantum farkındalığı zamanı geldi! Kuantum sonrası için güvenli şifreleme ve anahtarlama konusu önemli!

Kuantum farkındalığı:
Planlama, envanter çıkarma (şifrelenmiş veriler), şifreleme anahtarlarının döndürülmesi…

Kuantumla ilgili gelişmelerin dikkatle izlenmesi gerekiyor…

Kötü taraf: YZ ve Kuantum'un insan denetiminin önüne geçmesi öngörülemeyen sonuçlara yol açabilir.

Siber güvenli bir gelecek dileğiyle…

Basit ama etkili önlemler:

- Bilişim araçlarında ve uygulamalarda güçlü parolalar kullanmak,
- Önemli bilgileri düzenli olarak yedeklemek,
- Donanım ve yazılımları güncel tutmak,
- Şüpheli bağlantıları açmamak,
- Sanal ortam hesaplarını ve gizlilik ayarlarını dikkatli yönetmek.


https://pekelahmet.com

SORU-YANIT

1. Aşağıdaki parolalar arasında en güçlü parola hangisidir?

a) 9999 (4 karakter)
b) 123456 (6 karakter)
c) qwerty123456 (12 karakter)
d) T;3B9#tx (8 karakter)
e) temmuz2025 (10 karakter)

2. Aşağıdakilerden hangisi fiziksel güvenlik kapsamında alınan bir önlemdir?

a) Önemli veriler içeren basılı belgeler masa üzerinde bırakılmaz.
b) Hesap parolaları not kâğıtlarına yazılmaz, bilgisayar üzerine yapıştırılmaz.
c) Yazıcıya gönderilen gizli bilgiler, yazıcının başında, denetimli olarak alınır; yazıcıda bırakılmaz.
d) Önemli veri ya da bilgilerin olduğu ortamda dış bir hizmet alınacaksa, bir refakatçi eşliğinde yapılır.
e) Hepsi

3. Bir İnternet sayfasının güvenli olmadığını aşağıdaki denetimlerden hangisiyle anlayabiliriz?

a) Sayfadaki iletişim bilgilerinin doğrulanması
b) Sayfanın güvenlik damgasının olması
c) Sayfadaki gizlilik politikasının verilerinizin nasıl toplandığı, kullanıldığı ve korunduğu konusunda ayrıntılı bilgi vermesi
d) Bağlantı kuralı olarak HTTP'nin kullanılması
e) Hepsi