

GRUP-1

Bilgi Güvenliğinde Teknolojinin Rolü

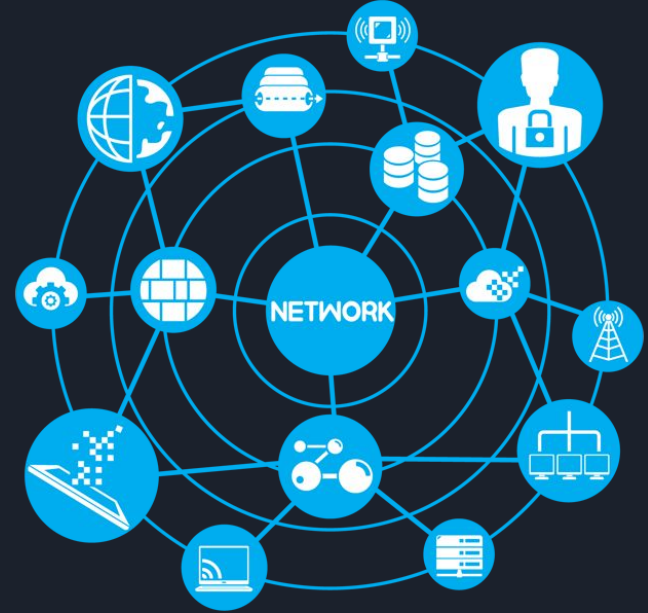


Grup #1

Bilgi güvenliği, bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma, veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemi.



Ağ ve Ağ Güvenliği



Şirket Güvenlik Politikası ve Farkındalık

- Tanımlama ve doğrulama politikası
- Şifre politikaları
- Uzaktan erişim politikası
- Farkındalık Eğitimleri



Antivirüs Programları

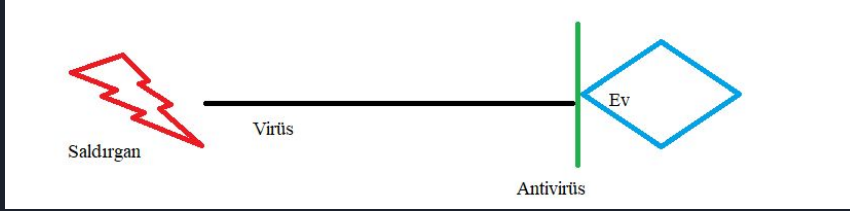
Virüs, genellikle zararsız gibi görünen bir dosyanın içine gizlenmiş ve dosya çalıştırıldığında bilgisayarda beklenmeyen ve istenmeyen olaylara neden olan programlardır.

- Proaktif
- Reaktif

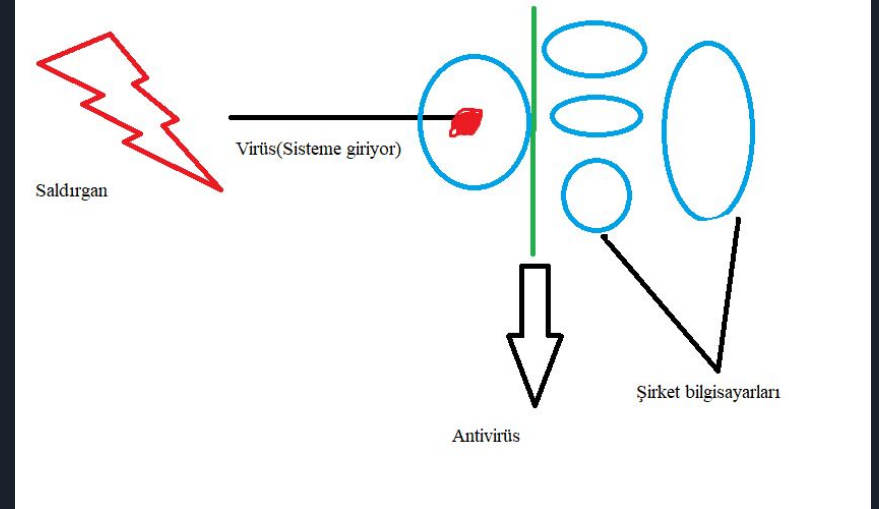


Proaktif ve Reaktif Antivirüs Programları

Proaktif

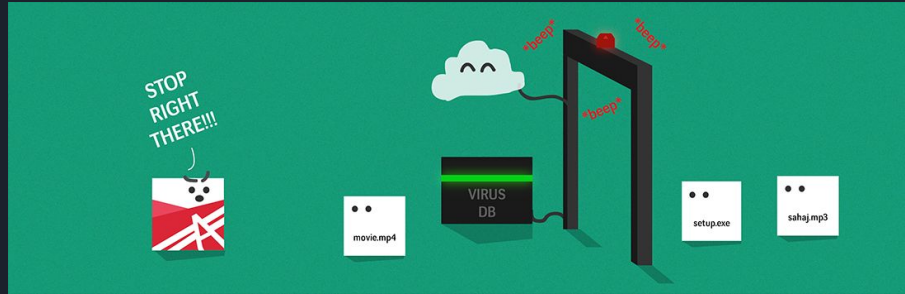


Reaktif

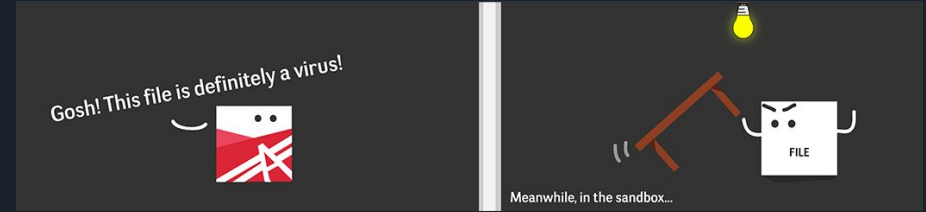


Antivirüs Programlarının Çalışma Mantığı

İmza Tabanlı Algılama



Şüpheli Davranış Algılama



Güvenlik Duvarı (Firewall) Teknolojisi

Güvenlik Duvarı (Firewall), bilgisayar ağlarında kullanılan ve ağ trafiğini denetleyerek kötü niyetli saldırılara karşı koruma sağlayan bir güvenlik önlemidir. Bir ağın içerisinde yer alan bilgisayar sistemlerini, dışarıdan gelen ağ trafiğine karşı korumak ve istenmeyen erişimlere engel olmak için kullanılır.

Güvenlik duvarının temel amacı, bilgisayar ağının güvenliğini sağlamaktır. Bunun için farklı teknolojiler ve yöntemler kullanılır. Güvenlik Duvarı, ağ trafiğini izler ve kaynak, hedef, protokol ve port gibi faktörleri değerlendirerek veri paketlerini kabul veya reddeder. Bu işlem, ağ üzerindeki iletişimin denetimini sağlar ve güvenliği artırır.

Örnek vermek gerekirse;

- Paket Filtreleme
- Durum Tabanlı İnceleme
- Uygulama Seviyesi Geçitleri
- VPN (Virtual Private Network) Erişimi Kontrolü
- İç Ağlardaki İletişimi Denetleme



Şifreleme Teknolojileri

Şifreleme teknolojileri, bilgiyi gizlemek ve korumak için kullanılan yöntemlerdir. Bu teknolojiler, veri ve iletişim güvenliğini sağlamak, gizliliği korumak ve yetkisiz erişimi engellemek amacıyla kullanılır. Şifreleme, bilgilerin yalnızca yetkili kişiler tarafından anlaşılabilir hale gelmesini sağlayan matematiksel bir süreçtir.

Şifreleme teknolojileri, günlük hayatımızda birçok alanda yaygın olarak kullanılır. İnternet üzerindeki bankacılık işlemleri, e-posta iletişimi, online alışveriş, VPN'ler ve şifreli mesajlaşma uygulamaları gibi birçok platformda şifreleme kullanılarak veri güvenliği sağlanır. Şifreleme teknolojileri, kişisel bilgilerin ve hassas verilerin yetkisiz erişimden korunmasında kritik bir rol oynar.

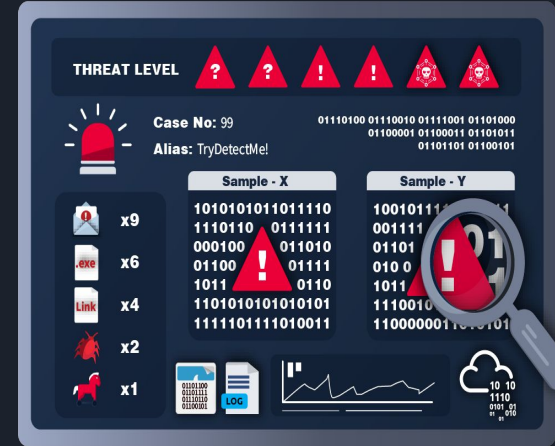
Şifreleme teknolojilerinin temel prensipleri ve farklı türleri;

- Simetrik Şifreleme
- Asimetrik Şifreleme
- Karmaşık Anahtar Şifreleme (Public Key Infrastructure - PKI)
- HMAC (Hash Message Authentication Code)
- Sayısal İmza



Saldırı Tespit Sistemi(IDS) Nedir?

Saldırıları tespit etmek için ağ veya sistem aktivitelerini izleyip bunlara bağlı olarak alarmlar üreten yazılım ya da donanımlara IDS denir. Kuruluşların verilerini, sistemlerini bulut ortamlarında koruyan bulut tabanlı IDS vardır.



Saldırı Tespit Sistemleri(IDS) Cihazı Türleri

1.Ağ tabanlı saldırı tespit sistemi (NIDS):

Saldırı türlerini tespit etmek için genel dinleme modunda ağ trafiğini analiz etmemizi sağlar.

2.Ana makine tabanlı (HIDS): Saldırı türlerini tespit etmek için sisteme yüklenen yazılımlardır. Ayrıca NIDS sisteminin tespit edemediği kötü amaçlı trafiği algılamasını sağlar.

3.İmza tabanlı (SIDS): Bir kuruluşun ağındaki tüm paketleri izler sonra bunları önceden belirlenmiş imzalara karşı eşleme yapıyor ve uyumsuzluk görünce uyarı veren bir sistemdir.





4. Anomali tabanlı izinsiz giriş tespit sistemi

(AIDS): Anomali, sistemin olağan akışı dışındaki durumlar gerçekleşip gerçekleşmediğini öğrenmek için önceden belirlenmiş bir referans modeli kullanarak tespit eden sistemlerdir.

5. Sanal makine tabanlı izinsiz giriş tespit sistemi

(VMIDS): Sanal makineleri izleyerek izinsiz girişleri algılar. Kuruluşların, cihazlarının bağlı olduğu tüm cihaz ve sistemlerdeki trafiği izlemesini sağlar.

6. Çevre saldırı tespit sistemi (PIDS):

Kuruluşların kritik altyapılarının çevresinde gerçekleşen saldırı girişimlerini tespit etmek için bir ağı bir PIDS çözümü yerleştirilerek yapılır.

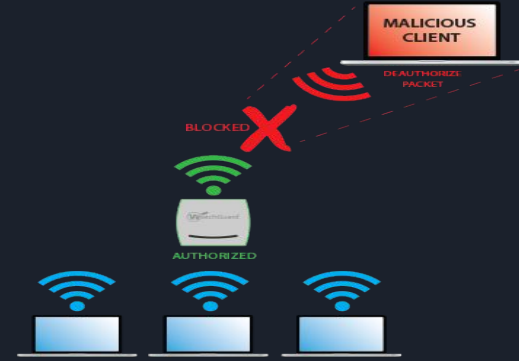
7. Yığın tabanlı izinsiz giriş tespit sistemi

(SBIDS): IDS'nin paketleri kuruluşun ağında hareket ederken izlemesini ve uygulamalar veya işletim sistemi tarafından işlenmeden önce kötü amaçlı paketleri çekmesini sağlar.



(İzinsiz Giriş Önleme Sistemi)IPS nedir?

IPS bir çeşit siber saldırı önleme sistemidir. Trafik üzerindeki paketleri analiz eder, kaynak ve hedef arasındaki iletişimi sürekli olarak kontrol eder. Anormal durumlar tespit etmesi halinde iletişimi ve veri akışını keser, bağlantıyı sıfırlar ve ağ yöneticisine saldırı hakkında uyarı gönderir.



(İzinsiz Giriş Önleme Sistemi)IPS Cihazları

1.Network Based Intrusion Prevention (NIPS): Network bazlı saldırı önleme sistemi NIPS tüm ağ üzerinde meydana gelen şüpheli hareketleri tespit edip önlemek üzerine kullanılan saldırı önleme sistemidir.

2.Wireless Intrusion Prevention Systems (WIPS): Kablosuz ağa saldırı önleme sistemi WIPS, kablosuz ağ protokolü izlenerek şüpheli hareketleri tespit etmek üzere kurulmuş saldırı önleme sistemidir.

3.Host Based Intrusion Prevention (HIPS): Ana makine üzerine yoğunlaşan saldırıları önlemek için kurulmuş bir sistemdir. Temel olarak ana makine koruma altına alınır.

4.Network Behavior Analysis (NBA): Normalde ağlar standart bazı davranışlar ile kullanılır. Bu standartların dışındaki hareketler şüphe ile yaklaşılmaması gereken hareketlerdir. Ağ üzerindeki hareketleri izleyerek, anormal durumların analiz edilmesi ve bu sayede saldırıların önceden tespit edilmesi için kurulmuş bir sistemdir.



GÜVENLİK YAZILIMLARI VE ARAÇLARI

Güvenlik yazılımları, bilgisayar sistemleri, ağlar, cihazlar ve verilerin güvenliğini sağlamak için geliştirilmiş yazılım programlarıdır. Bu yazılımlar, çeşitli güvenlik tehditlerine karşı korunmak ve hassas bilgilerin yetkisiz erişime karşı korunması için kullanılır.

Güvenlik araçları, bilgisayar sistemlerinin, ağların ve diğer dijital varlıkların güvenliğini sağlamak için kullanılan çeşitli araçlar ve programlardır.



En yaygın kullanılan güvenlik yazılımları

1.Antivirüs Yazılımları: Bilgisayar sistemlerini ve cihazlarını zararlı yazılımlara karşı korur. Zararlı yazılımları tespit edip karantinaya alıp sistemi temizler.

2. Güvenlik Duvarı (Firewall): Güvenlik duvarları, ağ trafiğini izleyerek izin verilen veya engellenen bağlantıları belirler ve güvenli bir ağ ortamı sağlar.

3.Kimlik Doğrulama Yazılımları: Kullanıcıların kimliklerini doğrulayarak yetkilendirme yapmamızı sağlar. Kimlik doğrulama yazılımları sosyal medyadan akıllı ev sistemlerine kadar bir çok alanda kullanılmaktadır.



4. Veri Şifreleme Yazılımları: Verileri şifreleyerek okunamaz hale getirir ve sadece doğru anahtara sahip olanların erişebileceği hale getirir.

5. Güvenli Bilgi ve Olay Yönetimi (SIEM) Yazılımları: Kuruluşlarda bulunan anlamlı veri getirecek, en güncel ve doğru verileri verecek kaynaklardan log almaktır.

6. Kötü Amaçlı Yazılım Koruma Yazılımları: Zararlı yazılımları tespit ederek engellememizi ve temizlememizi sağlayan yazılımlardır.

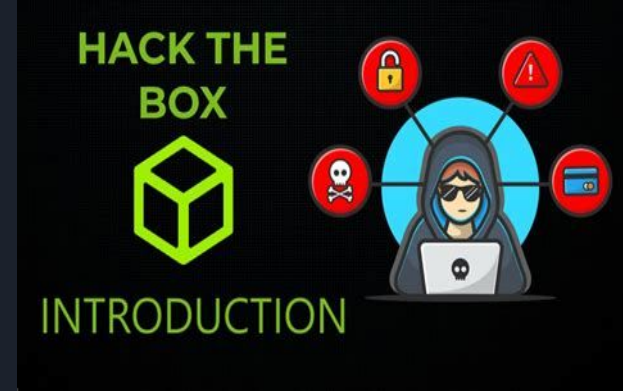


En yaygın kullanılan güvenlik araçları

1. Zafiyet Tarama Araçları: Bilgisayar sistemlerinde ve ağlarda güvenlik açıklarını taramak ve tespit etmek için kullanılan araçlardır. (Nessus, OpenVAS)

2. Sızma Testi Araçları: Bilgisayar sistemlerinin güvenlik zayıflıklarını ve açıklarını istismar etmek ve siber saldırıların nasıl gerçekleştirilebileceğini test etmek için kullanılan araçlardır. (Metasploit, Burp Suite)

3. Günlük İzleme Araçları: Bilgisayar sistemlerinin, ağların anormallikleri tespit etmek ve güvenlik olaylarını analiz etmek için kullanılan araçlardır. (Splunk, Graylog)





4. Güvenlik Bilgi ve Olay Yönetimi (SIEM) Araçları: Bir ağda meydana gelen olayları izlemek, güvenlik günlüklerini toplamak, analiz etmek ve güvenlik ihlallerini tespit etmek için kullanılan araçlardır.

5. Ağ İzleme ve Paket Analiz Araçları: Bilgisayar ağlarındaki trafiği izlemek, ağdaki bağlantıları analiz etmek ve ağ tabanlı saldırıları tespit etmek için kullanılan araçlardır.

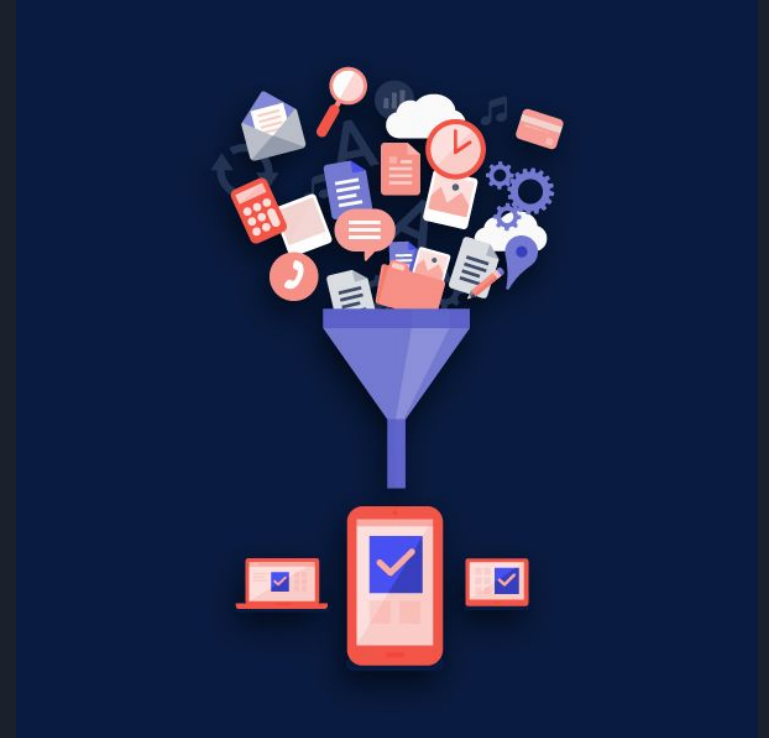
6. Saldırı Tespit Sistemleri (IDS) ve Saldırı Önleme Sistemleri (IPS): Ağ trafiğini izleyerek siber saldırıları tespit etmek ve engellemek için kullanılan araçlardır.

7. Web Uygulama Güvenlik Test Araçları: Web uygulamalarının güvenlik açıklarını taramak ve test etmek için kullanılan araçlardır.



İçerik Filtreleme

- İçerik filtreleme, istenmeyen e-postalara, internet sayfalarına veya çalıştırılabilir dosyalara ve diğer şüpheli öğelere erişimin taranması ve engellenmesidir. Başka bir deyişle içerik filtreleme internet kullanıcıları için risk oluşturabilecek içeriklere erişimin engellenmesidir.



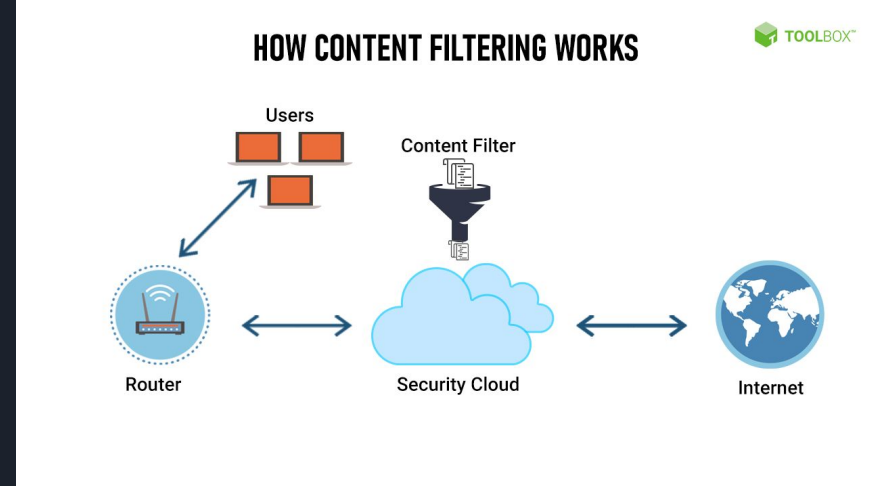
İçerik Filtreleme Neden Önemlidir ?

- İçerik filtrelemesi, şirketlerin ya da insanların genel olarak uygunsuz, yasa dışı veya sakıncalı içerikleri tespit ederek bu risklerin azaltılmasına yardımcı olur. Kötü amaçlı yazılım saldırılarını indirgeme, ağ bant genişliğini arttırma, personel verimliliğini arttırmada içerik filtrelemesi yapmak son derece önemlidir.



İçerik Filtreleme Nasıl Çalışır ?

İçerik filtreleri genellikle internet güvenlik duvarının bir parçasıdır, ancak donanım veya yazılım olarak da uygulanabilir. Bu tür içerik filtreleri genellikle içerik kaynakları ile kullanıcı arasındadır. Yapacağınız bağlanma isteği ilk olarak filtreleme işleminden geçecektir. Filtrelemede yaygın olarak SaaS kaynakları, DNS filtreleme, IDS, IPS, Proxy, ISP filtreleri, arama motoru filtreleri olabilir.



İçerik Filtreleme Nerelerde Kullanılır ?

- Şirketlerde sosyal medya erişimini kısıtlayarak, verimi arttırmaya dayalı olarak kullanılabilir.
- Okullarda internetin eğitim dışında kullanılmamasını sağlamak amacıyla kullanılabilir.
- Ev içerisinde dolandırıcılık, uygun olmayan, illegal kaynaklara erişimi kısıtlama amacıyla kullanılır.



MOBİL GÜVENLİĞİ

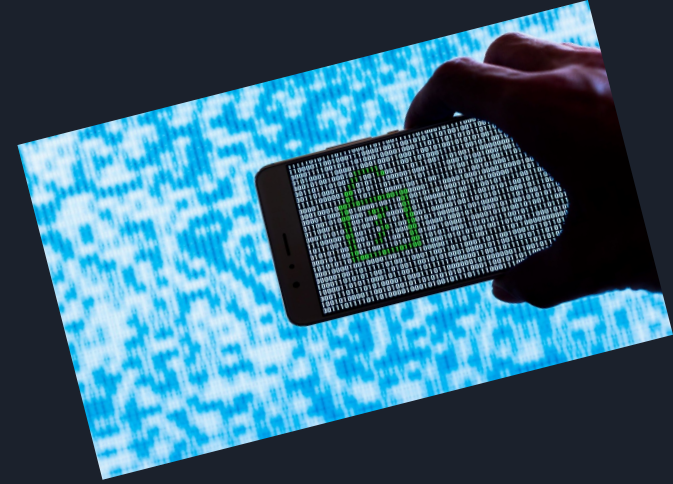
Mobil güvenlik, akıllı telefonlar ve tabletler gibi mobil cihazlarda veri güvenliğini sağlama çabalarını ifade eder. Genellikle, mobil güvenlik, işletmelerin çeşitli mobil cihazlarda kullanılması nedeniyle tehlikeye girebilecek hassas bilgileri kontrol etmek için üzerinde çalıştığı bir şeydir. Mobil cihazların kullanımı arttıkça, cihazların güvenliğinin sağlanması mobil teknolojide giderek daha önemli bir konu haline gelmiştir.

Saldırganlar mobil cihazlar üzerindeki saldırılarında üç ana başlıklı hedeflerler. Bunlar;

Veriler: Mobil cihazlar, içerilerindeki hassas olabilecek kişisel ve kurumsal verileri depolamaktadırlar. Bu veriler arasında kişinin bir sisteme girebilmesi için sahip olduğu hesap bilgileri, kredi kartı numaraları, gelen ve giden arama/mesaj bilgileri gibi cihaz üzerinde saklanan verilerdir.

Kimlik bilgileri: Mobil cihazlar genellikle kişiye özel olarak kullanılan cihazlardır. Saldırganlar, cihazı kullanmakta olan kişinin kim olduğunu, cihaz üzerindeki bilgilerden elde edip gelecekteki saldırılarında elde ettiği kullanıcı kimliğini kullanabilir.

Kullanılabilirlik: Saldırgan cihaz üzerinde yeni kısıtlar koyarak, cihazın özelliklerinden kullanıcıyı yoksun bırakabilir.



PEKİ MOBİL GÜVENLİĞİ NASIL SAĞLANIR?

- Uygulama indirirken dikkatli ve seçici olun.
- Her uygulama indirdiğinizde izin penceresini dikkatlice okuyun.
- Telefonunuzu şifreyle koruyun.
- Erişim izinlerini kaldırın.
- Halka açık WiFi ağlarına katılmayın.
- Başkalarının hesaplarınıza erişmesini engellemek için çift faktörlü doğrulama kullanın.
- Hassas bilgileri telefonunuzda saklamamaya özen gösterin.
- İhtiyaç olmadığı durumlarda Bluetooth'u kapatın.
- Cep telefonunuzu satarken ya da tamire gönderirken sim kart bilgilerinizi temizleyin.



BULUT GÜVENLİĞİ



Bulut güvenliği, bulutta çalışan sistemleri korumaya yönelik bir siber güvenlik disiplini. Bu; çevrimiçi altyapı, uygulamalar ve platformlarda verileri gizli ve güvende tutmayı içerir. Bu sistemlerin güvenliğini sağlamak, bulut sağlayıcıları ve müşterilerin birey, küçük ila orta ölçekli işletme veya kurum olup olmadığına bakılmaksızın, sistemleri kullananların çabalarını kapsar.

Bulut sağlayıcıları, her daim etkin olan internet bağlantıları aracılığıyla sunucularında hizmetler barındırır. İşleri müşterilerin güvenine bağlı olduğundan müşterilerin verilerinin gizli ve güvenli bir şekilde saklanması için bulut güvenliği yöntemleri kullanılır. Ancak bulut güvenliği kısmen müşterinin de elindedir. Bu kavramın iki tarafını da anlamak, sağlıklı bir bulut güvenliği çözümü açısından çok önemlidir.



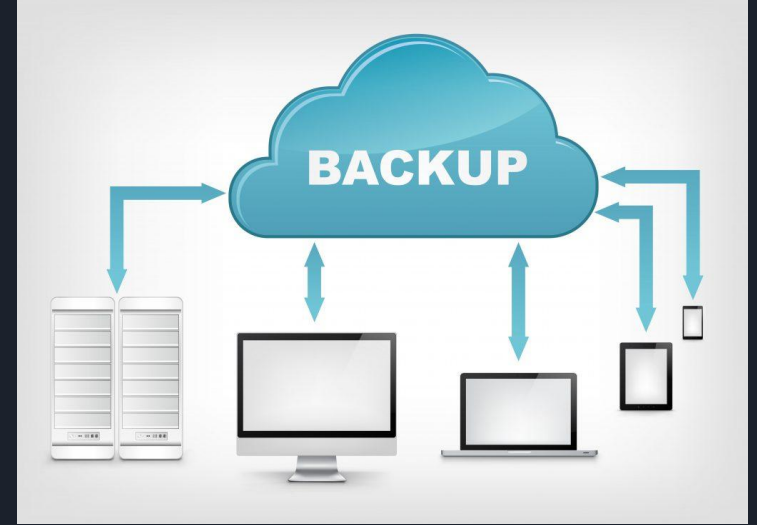
BULUT GÜVENLİĞİ, TEMELDE AŞAĞIDAKİ KATEGORİLERDEN OLUŞUR

- . Fiziksel ağlar — yönlendiriciler, elektrik gücü, kablolar, iklim kontrolleri vb.
- . Veri depolama — sabit sürücüler vb.
- . Veri sunucuları — temel ağ bilgi işlem donanımları ve yazılımları
- . Bilgisayar sanallaştırma yapıları — sanal makine yazılımları, sunu makineler ve konuk makineler
- . İşletim sistemleri (İS) — tüm bilgisayar işlevlerini destekleyen yazılım
- . Aracı yazılımlar — uygulama programlama arayüzü (API) yönetimi
- . Yürütme ortamları — çalışan bir programın yürütülmesi ve bakımı
- . Veriler — saklanan, değiştirilen ve erişilen tüm bilgiler
- . Uygulamalar — geleneksel yazılım hizmetleri (e-posta, vergi yazılımı, verimlilik programı grupları vb.)
- . Son kullanıcı donanımları — bilgisayarlar, mobil cihazlar, Nesnelerin İnterneti (IoT) cihazları



Veri yedekleme nedir ?

- Yazılımsal hata, hasar ve arıza gibi geri dönülmez durumlarda verilerin geri dönülmez bir şekilde kaybolmasını önleyen sistemdir. Düzenli yedeklemeler arıza, yazılım hataları, elektrik kesintisi, hırsızlık gibi olumsuz sonuçları en aza indirecektir. Veri yedekleme birden fazla şekilde gerçekleştirilebilir.



Veri Yedekleme Türleri

- Tam Yedekleme : Ortamda bulunan veriler olduğu gibi yedeklenmesidir. Bütün verileri yedeklendiği için en güvenilir yöntemdir. En çok vakit alan yöntemdir.
- Fark Yedeklemesi : Uygulanabilmesi için öncelikle tam yedekleme alınmış olması gerekmektedir. Tam yedek alındıktan sonra veri üzerinde değişiklik yapılırsa, değişen veri yeni bir klasöre yedeklenerek kaydedilir. Tam yedeklemeye göre zamandan ve yerden tasarruf edilir.



- Artımlı Yedekleme : Fark yedeklemesiyle neredeyse aynıdır. Yedek alma işleminde bir önceki artımlı yada tam yedekleme işlemine bakılarak sadece değişen veriyi yedekler. Yedekleme işleminden ve yerden tasarruf edilir.
- Ayna Yedeklemesi : Daha önce yedeği alınmış bir verinin başka bir ortamda veya diskte tekrar yedeğinin alınması demektir.
- Sunucu Yedeklemesi : Bilgisayarlar ve sunuculardaki verileri güven altına almak isteyenler için uygundur. Verilere, olumsuz bir durumda karşı karşıya kaldıklarında uzaktan erişebilmek veya yedeklemek isteyenler için son derece önemlidir. Bu yöntem ile veriler güvenli bir ortamda yedeklenmiş olur.





TYPES OF BACKUP: FULL, DIFFERENTIAL, AND INCREMENTAL

Full Backups: Entire data set, regardless of any previous backups or circumstances.




Differential Backups: Additions and alterations since the most recent full backup.



Incremental Backups: Additions and alterations since the most recent incremental backup.



Initial Full Backup • 1st Backup 2nd Backup 3rd Backup 4th Backup 5th Backup

 Data subject to backup

Biyometrik kimlik doğrulama sistemleri

Biyometrik doğrulama, kişinin fiziksel özelliklerini kullanarak kimlik doğrulama işlemidir. Biyometrik doğrulama sistemleri, geleneksel parola veya PIN kodlarına göre daha güvenlidir. Ancak bu sistemlerin de bazı zayıflıkları vardır. Örneğin, parmak izi kalıbı veya görüntüsü ile yanıltmak kolaydır. Yüz tanıma sistemleri ise bazen yüzün benzer özelliklere sahip başka bir kişi tarafından yanıltılabilir. Dolandırıcılık algılama için yüz tanıma teknolojisi kullanılabilir.



Kimlik doğrulama sistemi metodları

Fizyolojik Metodlar : Bir bireyin yüz detayları, parmak izi (sabıka sorgulama veya hasta kayıt/tanıma işlemlerinde), el geometrisi, avuç izi, iris desenleri, retina taraması (kan damarı seviyesi taranır), kan örneği veya ses tanıma (ses ses teli/boşluğu ve ağız hareketleri kişiye özeldir) olabilir. Kısacası, kişinin fiziksel özellikleri analiz edilir.

Davranışsal Metodlar: El yazısı (imzası) tanıma (kalem tutuş tarzı, yazı stili, yazış baskısı, yazma hızı kişiye özeldir), klavye hareketlerini algılama (klavyeye basma hızı/tarzı/baskısı kişiye özeldir) olabilir. Kısacası, kişinin neyi ve nasıl yaptığı analiz edilir.





Avantajlar ve Dezavantajları

Avantajlar

- Biyometrik teknoloji, kişiye özel ve taklit edilmesi zor olan verileri içerir.
- Biyometri bir bireyin fiziksel özellikleriyle ilişkili olduğundan, o kişinin bu erişim yeteneğini unutması, yanlış yerleştirmesi veya başka bir şekilde kontrolünü kaybetmesi daha zordur.
- Biyometrik okuyucular en güvenilir yöntemlerdendir. Kimlik bilgisi cihazlarına ek olarak veya bir PIN kodu ile de kullanılabilir.

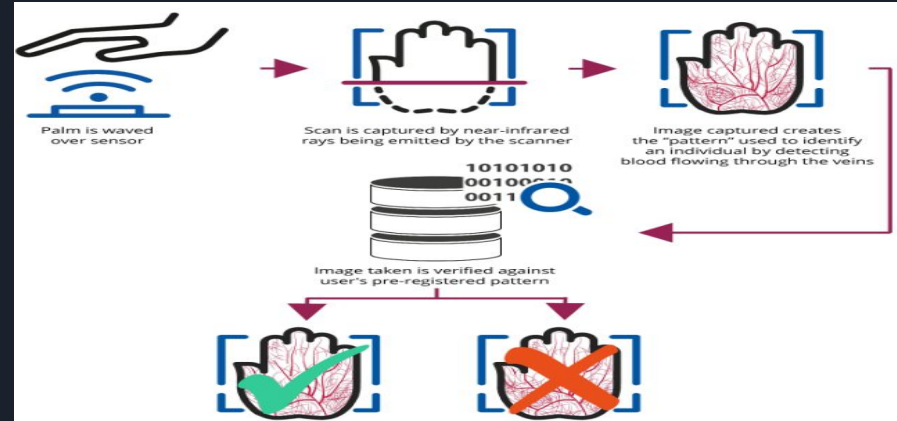
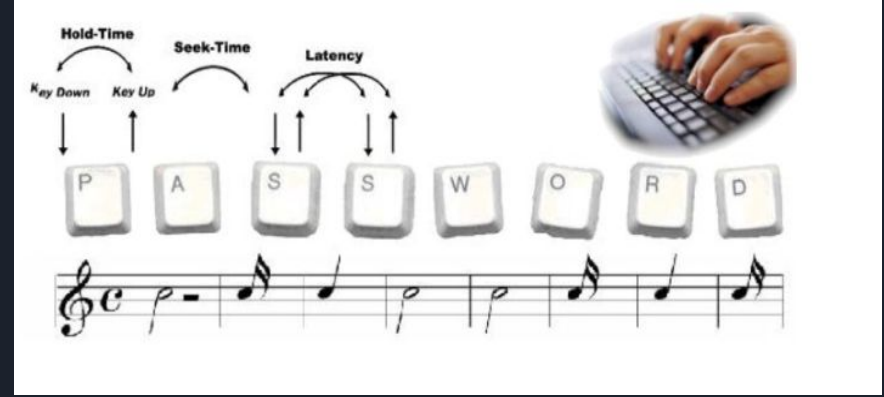
Dezavantajları

- Parmak izi gibi bir takım kimlik doğrulama yöntemlerinde kesin sonuç almak zor olabilir.
- Ses tanımlama gibi bir takım kimlik doğrulama yöntemlerinde kimlik doğrulayan sistemler kullanıcının sesi kaydedilerek kolayca atlatılabilir, taklit edilebilir.
- İris desenleri, genetik cinsiyeti ortaya çıkarabilir. Retina taramaları bir kişinin hamile veya şeker hastası olup olmadığını gösterebilir.
- Kayıt süresi (enroll) uzunsa (birkaç dakikadan fazla), biyometrik sistemin kullanıcıyı tarayabildiği / kabul edebildiği veya reddedebildiği hız çok yavaşsa, biyometrik sistemler büyük kullanılabilirlik zorluklarıyla karşılaşabilir.



Biyometrik kimlik doğrulama çeşitleri

- Ses Tanıma
- Yüz Tanıma
- El Geometrisi
- Parmak izi
- İris Desenleri
- Retina Tarama
- İmza
- Tarama/Tanımlama
- Vasküler Desenler
- Tuş Vuruşu Tanımlama



Güvenlik izleme ve veri ihlali

Veri ihlalleri, bilgisayar korsanlarının güvenlik açıklarından yararlanarak bilgi güvenliği sistemlerinizi ve kontrollerinizi kıldığı durumlarda kasıtlı olabilir. Güvenlik duvarınızdaki boşlukları kapatarak bunu önleyebilirsiniz. Düzenli güvenlik açığı taramaları yapmak, tehditleri belirlemek ve güvenlik açıklarını kapatmak için faydalıdır. Ancak tüm veri ihlalleri kasıtlı değildir, bazen de veriye erişim izni ve yetkisi olanlar bilgileri istemsiz olarak açığa çıkarabilir.

1. Yanlış parola yönetimi
2. Güvenlik açıkları
3. Kötü amaçlı yazılımlar
4. İçeriden gelen tehditler ve kazalar



Veri ihlali karşısında ne yapılmalı?

Acil yanıt stratejisinin ilk adımı risk durumundaki değerli dijital varlıkları güvence altına almaktır. Bu hamle, mali açıdan felakete yol açabilecek ve itibarınıza zarar verebilecek birden fazla veri ihlali olasılığını azaltır.

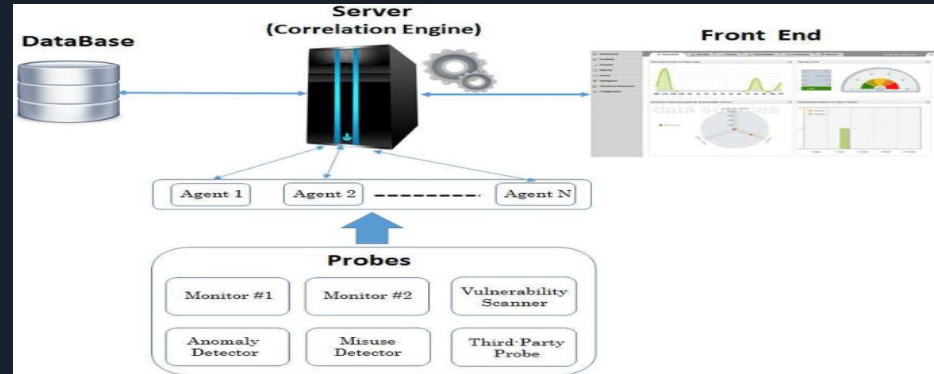
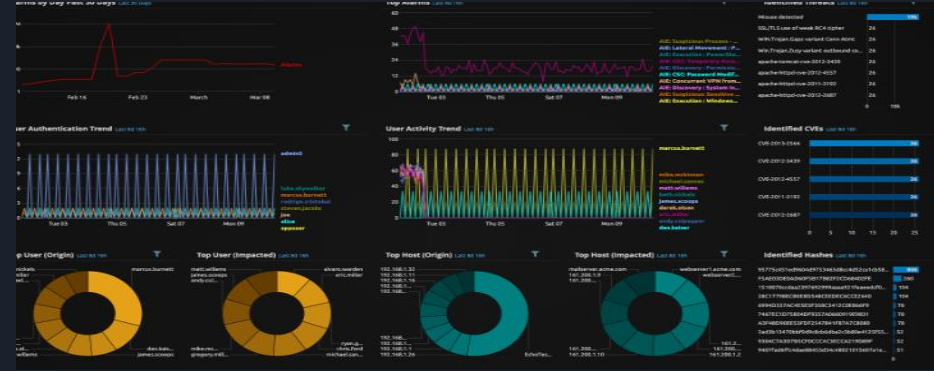
BT ortamınızı siber saldırılara karşı savunmasız bırakan güvenlik açıklarını kapatmalısınız. Güvenlik açığı değerlendirmesi yapmak, sistem koruma günlüklerini izlemek ve sızıntı testi uygulamak, güvenlik durumunuzu kontrol etmenize yardımcı olacaktır.

Veri ihlali hakkında yasal mercileri ve etkilenen tarafları bilgilendirmelisiniz. Şirketiniz için geçerli olan yasaları kontrol edin. Güvenliği ihlal edilen bilgi ve şirketinizin tabi olduğu düzenlemelere göre kamuoyunu bilgilendirmeniz gerekebilir.



SOC ve SIEM ürünleri

Siber güvenlik günümüzde artık ulusal güvenlik stratejilerinden birisi haline gelmiştir. Teknolojinin her geçen gün gelişmesiyle beraber, siber güvenlik hususunda meydana gelen gelişmeler, alınan önlemler ve yasal düzenlemeler yetersiz kalmaktadır. Olası ihtiyacın ve tehditlerin doğrultusunda alınan kararlar ileriye dönük olarak yeterli güveni sağlamamaktadır. İleriye dönük ve güven ortamının oluşması içinse, günümüzde SOC merkezleri kurulmaya başlanmıştır. SOC merkezi bir kurum ya da kuruluşun güvenliğini devamlı olarak izler ve bu merkez güvenlik olaylarında oluşan logların analizinden sorumludur. Bu merkezde çalışan kişilere ise SOC analistleri denilmektedir. Bu analistler siber saldırılara karşı teknolojik çözümler kullanarak, iyi bir süreç yönetimi yapmaktadır ve siber güvenlik olaylarının tespit edilmesini sağlayarak yapılan analizi sunmaktadır.





TEŞEKKÜRLER.

