**Bilgisayar Güvenliği**

**1. Bilgisayar Güvenliği Nedir?**

Bilgisayar güvenliği, bilgisayar sistemleri ve ağlarını kötü niyetli saldırılara, zararlı yazılımlara, yetkisiz erişime, veri kaybına veya bozulmaya karşı korumayı amaçlayan bir alandır. Temel hedefi, verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaktır.

**2. Bilgisayar Güvenliğinin Temel İlkeleri**

Bilgisayar güvenliği üç ana ilkeye dayanır:

* **Gizlilik (Confidentiality):** Yalnızca yetkili kullanıcıların verilere erişebilmesini sağlamak.
* **Bütünlük (Integrity):** Verilerin doğruluğunu ve güvenliğini koruyarak, yetkisiz değişiklikleri engellemek.
* **Erişilebilirlik (Availability):** Yetkili kullanıcıların verilere zamanında ve kesintisiz erişebilmesini sağlamak.

**3. Bilgisayar Güvenliği Tehditleri**

Bilgisayar güvenliği, çeşitli tehditlerden korunmak zorundadır. En yaygın tehditler şunlardır:

* **Virüsler:** Bilgisayarları enfekte eden ve genellikle veri kaybına veya sistem bozulmasına yol açan zararlı yazılımlar.
* **Truva Atları (Trojan Horses):** Kullanıcıyı kandırarak sisteme zararlı yazılım yükleyen programlar.
* **Casus Yazılımlar (Spyware):** Kullanıcıların kişisel bilgilerini toplamak amacıyla sisteme giren yazılımlar.
* **Fidye Yazılımları (Ransomware):** Bilgileri şifreleyip fidye talep eden yazılımlar.
* **Phishing (Oltalama) Saldırıları:** Kullanıcıyı kandırarak kişisel bilgilerini çalmaya yönelik saldırılar.
* **Denial of Service (DoS) ve Distributed Denial of Service (DDoS) Saldırıları:** Sistemi aşırı yükleyerek erişilemez hale getirme saldırıları.

<https://www.youtube.com/watch?v=VJFaO2-zsCU&t=23s>

**4. Güvenlik Önlemleri**

Bilgisayar güvenliğini sağlamak için birçok yöntem ve strateji bulunmaktadır. Bunlar arasında:

* **Antivirüs Yazılımları:** Virüsleri, casus yazılımları ve diğer zararlı yazılımları tespit eden ve temizleyen yazılımlar.
* **Güçlü Parolalar:** Sisteme giriş için kullanılan parolaların karmaşık, tahmin edilmesi zor ve düzenli olarak değiştirilen parolalar olması.
* **Güvenlik Duvarları (Firewalls):** Bilgisayarın dış dünyadan gelen kötü amaçlı veri akışına karşı koruma sağlayan sistemler.
* **Veri Şifreleme:** Verilerin güvenliğini artırmak için verinin okunabilirliğini engelleyen şifreleme teknikleri kullanmak.
* **İki Faktörlü Kimlik Doğrulama (2FA):** Sisteme girişte sadece parolaya değil, aynı zamanda ikinci bir güvenlik katmanına da ihtiyaç duymak (örneğin, telefon üzerinden gönderilen doğrulama kodu).
* **Yedekleme (Backup):** Verilerin düzenli olarak yedeklenmesi, veri kaybı durumunda geri yükleme imkanı sağlar.

**5. Güvenlik Politikaları**

Bir organizasyonun bilgisayar güvenliğini sağlamak için belirli güvenlik politikaları oluşturulmalıdır. Bu politikalar şunları içerebilir:

* **Erişim Kontrolü:** Kullanıcıların sisteme hangi verilere erişebileceği belirlenmeli ve sadece yetkili kişilere gerekli erişim sağlanmalıdır.
* **Düzenli Yazılım Güncellemeleri:** Yazılımlar ve işletim sistemleri, güvenlik açıklarını kapatmak için düzenli olarak güncellenmelidir.
* **Eğitim ve Farkındalık:** Kullanıcılara bilgisayar güvenliği konusunda eğitim verilmeli, şüpheli e-posta ve bağlantılardan nasıl korunacakları öğretilmelidir.

**6. Bilgisayar Güvenliği Araçları**

Bilgisayar güvenliğini sağlamak için kullanılan bazı araçlar şunlardır:

* **Antivirüs Programları:** Virüsleri ve diğer zararlı yazılımları tespit etmek ve yok etmek için kullanılır.
* **Güvenlik Duvarları (Firewalls):** Giriş ve çıkış trafiğini denetleyerek, izinsiz erişimi engeller.
* **Şifreleme Araçları:** Verilerin güvenli bir şekilde şifrelenmesini sağlar.
* **İzleme Araçları:** Bilgisayar sistemlerinde meydana gelen şüpheli faaliyetleri tespit etmek için kullanılır.

**7. Bilgisayar Güvenliği İhlalleri ve Sonuçları**

Bir güvenlik ihlali, şirketlere, kullanıcılara ve kurumlara ciddi zararlar verebilir. Bu zararlar şunları içerebilir:

* **Veri Kaybı:** Önemli verilerin kaybolması veya bozulması.
* **Mali Zararlar:** Kötü niyetli saldırılar sonucu mali kayıplar ve fidye ödemeleri.
* **İtibar Kaybı:** Güvenlik ihlali, bir organizasyonun müşteri güvenini kaybetmesine yol açabilir.
* **Yasal Sonuçlar:** Veri ihlalleri, kişisel verilerin korunması yasalarına aykırı olabilir ve yasal sonuçlara yol açabilir.

**Siber Güvenlik**

**1. Siber Güvenlik Nedir?**

Siber güvenlik, dijital sistemler, ağlar, yazılımlar ve verilerin kötü niyetli saldırılara, veri ihlallerine, zararlı yazılımlara ve diğer siber tehditlere karşı korunması amacıyla alınan önlemler bütünüdür. Siber güvenliğin amacı, bilgi ve teknolojiyi güvende tutarak, yetkisiz erişimi engellemektir.

**2. Siber Güvenliğin Temel Bileşenleri**

Siber güvenlik, aşağıdaki temel bileşenlerden oluşur:

* **Ağ Güvenliği:** Bilgisayar ağlarını dış tehditlerden koruma amacı taşır. Bu, güvenlik duvarları (firewalls), VPN'ler (sanallaştırılmış özel ağlar), izinsiz giriş tespit sistemleri (IDS) ve izinsiz giriş engelleme sistemleri (IPS) ile sağlanır.
* **Uygulama Güvenliği:** Yazılımlar ve uygulamalardaki açıkları tespit edip gidererek, zararlı yazılımların sisteme girmesini engellemek için alınan önlemleri içerir.
* **Veri Güvenliği:** Veri şifreleme, erişim kontrolü, yedekleme ve veri bütünlüğü koruma tekniklerini içerir. Verilerin güvenliğini sağlamak, onların yetkisiz erişime, değiştirilmesine veya kaybolmasına karşı korunmasını sağlar.
* **Kimlik ve Erişim Yönetimi (IAM):** Kullanıcıların kimlik doğrulaması ve yetkilendirilmesi süreçlerini yönetir. Bu, yalnızca yetkili kişilerin verilere erişebilmesini sağlar.
* **Son Nokta Güvenliği:** Bilgisayarlar, mobil cihazlar, sunucular gibi cihazları kötü amaçlı yazılımlara karşı koruma amacını güder. Bu tür cihazlarda antivirüs yazılımları, güncellemeler ve güvenlik yazılımları kullanılır.

**3. Siber Güvenlik Tehditleri**

Siber güvenlik tehditleri, bilgi sistemlerini tehdit eden çeşitli faktörlerdir. En yaygın siber tehditler şunlardır:

* **Virüsler ve Solucanlar (Worms):** Kendi kendini kopyalayan ve diğer bilgisayarlara yayılabilen zararlı yazılımlar.
* **Truva Atları (Trojan Horses):** Kullanıcıları kandırarak sisteme gizlice sızan zararlı yazılımlar.
* **Fidye Yazılımları (Ransomware):** Bilgisayarları veya verileri şifreleyerek, şifreyi çözme karşılığında fidye talep eden zararlı yazılımlar.
* **Phishing (Oltalama) Saldırıları:** Kullanıcıları aldatmak amacıyla, sahte e-postalar veya web siteleriyle kimlik bilgilerini çalmaya yönelik saldırılar.
* **Denial of Service (DoS) ve Distributed Denial of Service (DDoS):** Bir servisi veya web sitesini aşırı trafikle boğarak erişilemez hale getiren saldırılar.
* **Keylogger:** Kullanıcıların tuşlama hareketlerini kaydederek şifre gibi hassas bilgileri çalmaya yönelik yazılımlar.

**4. Siber Güvenlik Önlemleri**

Siber güvenliği sağlamak için çeşitli önlemler alınabilir. Bunlar şunları içerir:

* **Güçlü Parolalar:** Kullanıcıların karmaşık ve zor tahmin edilen parolalar kullanması, siber saldırılara karşı ilk savunma hattıdır.
* **Şifreleme (Encryption):** Verilerin, sadece yetkili kişiler tarafından okunabilir olmasını sağlayan bir güvenlik önlemidir. Hem veri iletimi hem de depolama sırasında şifreleme yapılmalıdır.
* **Güvenlik Duvarları (Firewalls):** İç ve dış ağlar arasındaki trafiği denetleyerek, kötü amaçlı trafiği engellemeye yardımcı olur.
* **Antivirüs Yazılımları ve Malware Taraması:** Bilgisayarları ve cihazları zararlı yazılımlar karşısında korumak için antivirüs yazılımları kullanılır.
* **Güncellemeler ve Yama Yönetimi (Patch Management):** Sistemlerin ve yazılımların güvenlik açıklarını kapatmak için düzenli olarak güncellenmesi gerekir.
* **Eğitim ve Farkındalık:** Kullanıcıları siber tehditler hakkında eğitmek, örneğin phishing saldırılarına karşı dikkatli olmalarını sağlamak.

**5. Siber Güvenlik Yönetişimi**

Bir organizasyonun siber güvenlik önlemlerini etkili bir şekilde yönetebilmesi için aşağıdaki stratejilere ihtiyacı vardır:

* **Politikalar ve Prosedürler:** Siber güvenlik ile ilgili organizasyonel politikalar ve prosedürler oluşturmak, çalışanların güvenlik önlemlerini anlamalarını sağlar.
* **Risk Yönetimi:** Organizasyonlar, siber güvenlik risklerini tespit etmeli, değerlendirmeli ve uygun güvenlik önlemleri ile minimize etmelidir.
* **Acil Durum Planları (Incident Response Plan):** Olası bir güvenlik ihlali durumunda, hızlı bir şekilde müdahale edebilmek için bir acil durum planı oluşturulmalıdır.

**6. Güvenlik Olayları ve Müdahale**

Siber güvenlik ihlalleri ve saldırıları, çoğu zaman öngörülemez. Bu tür durumlar için etkili bir olay müdahale süreci gereklidir. Olay müdahale süreci şu adımlardan oluşur:

1. **Tespit (Detection):** Güvenlik ihlalinin erken tespiti önemlidir. Sistem izleme araçları ve anomali tespit yöntemleri bu aşamada kullanılır.
2. **Yanıt (Response):** Güvenlik olayı tespit edildikten sonra, hızlı bir şekilde önlem alınmalı, zarar minimize edilmelidir.
3. **İyileştirme (Recovery):** Olaydan sonra, etkilenen sistemler düzeltilmeli ve normale döndürülmelidir.
4. **Analiz (Analysis):** İhlalin sebepleri ve etkileri detaylıca incelenerek gelecekte benzer saldırıların önlenmesi için dersler çıkarılmalıdır.

**7. Siber Güvenlik Araçları**

Siber güvenlikte kullanılan bazı araçlar şunlardır:

* **Güvenlik Duvarları (Firewall):** Ağ trafiğini denetleyerek, dış tehditlere karşı koruma sağlar.
* **İzleme Sistemleri (SIEM):** Güvenlik olaylarını toplar, analiz eder ve anomali tespiti yapar.
* **Antivirüs ve Antimalware Yazılımları:** Zararlı yazılımları tespit eder ve yok eder.
* **Şifreleme Araçları:** Verilerin şifrelenmesini sağlar ve güvenli bir şekilde iletilmesini sağlar.

<https://www.youtube.com/watch?v=inWWhr5tnEA&t=71s>