SİBER GÜVENLİK

Siber Güvenlik Nedir?

Siber güvenlik, bilgisayar sistemlerini, ağları, verileri ve dijital altyapıyı dijital tehditlere karşı koruma sürecidir. Bu tehditler, kötü amaçlı yazılımlar, siber saldırılar, veri ihlalleri, kimlik hırsızlığı ve diğer siber suçlar olabilir. Siber güvenlik, bu tür tehditleri önlemek, tespit etmek ve bunlara karşı koymak için çeşitli stratejiler içerir.

Neden önemlidir?

1. Veri Koruma: Günümüzde kişisel bilgiler, finansal veriler, ticari sırlar ve devlet bilgileri dijital ortamda saklanıyor. Bu verilerin çalınması ya da kötüye kullanılması ciddi sonuçlar doğurabilir.
2. İş Sürekliliği: Siber saldırılar, işletmelerin operasyonlarını kesintiye uğratabilir. Bir saldırı, veri kaybına, hizmetlerin durmasına veya itibar kaybına yol açabilir, bu da mali zararlar ve müşteri kaybı anlamına gelebilir.
3. Hukuki ve Düzenleyici Yükümlülükler: Birçok ülke, şirketlerin kullanıcı verilerini korumasını zorunlu kılan yasalar çıkarıyor. Bu kurallara uymayan şirketler ciddi cezalarla karşılaşabilir.
4. Kişisel Güvenlik: Kişisel bilgilerinizin korunması, kimlik hırsızlığı ve siber zorbalık gibi risklere karşı sizi güvende tutar. Bu, çevrimiçi faaliyetlerinizin gizliliğini ve güvenliğini sağlar.
5. Ulusal Güvenlik: Hükümetler, kritik altyapılarının (elektrik, su, ulaştırma, sağlık hizmetleri vb.) korunmasını sağlamak zorundadır. Siber saldırılar, bu tür altyapılara büyük zararlar verebilir.

Siber Güvenlikte Kimler Tehdit Oluşturur?

Hackerlar

Kötü niyetli kişiler veya gruplar, sistemlere izinsiz erişim sağlayarak veri çalabilir, sistemlere zarar verebilir veya fidye isteyebilirler.

Kötü Amaçlı Yazılım Geliştiricileri

Virüsler, solucanlar, truva atları ve fidye yazılımları gibi kötü amaçlı yazılımlar geliştiren ve yayan kişilerdir.

İç Tehditler

Şirket içindeki çalışanlar veya eski çalışanlar, yetkilerini kötüye kullanarak hassas bilgilere erişebilir veya sistemlere zarar verebilirler.

Devlet Destekli Aktörler

Bazı ülkeler, diğer ülkelerin sistemlerine siber saldırılar düzenlemek veya casusluk yapmak için özel ekipler oluşturabilirler.

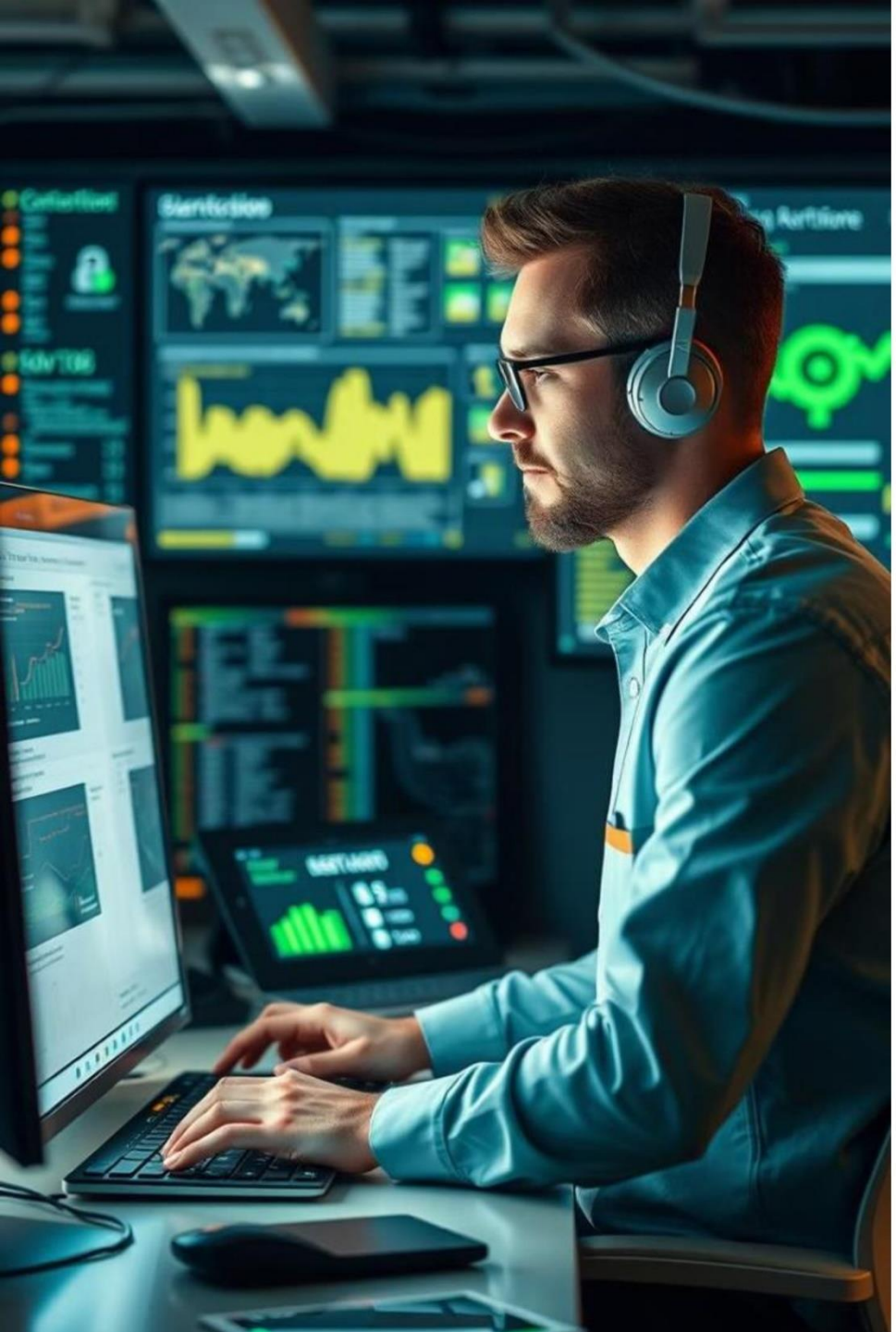
Yaygın Siber Saldırı Türleri ve Yöntemleri

1. **Kötü Amaçlı Yazılımlar (Malware)**, bilgisayar sistemlerine zarar vermek veya bilgileri çalmak için tasarlanmıştır.

2. **Kimlik Avı (Phishing)**, kullanıcılardan hassas bilgiler çalmak için aldatıcı yöntemler kullanan bir tür sosyal mühendislik saldırısıdır.

3. **Fidye Yazılımlar (Trojen, Truva Atı)** , bilgisayar sistemlerini kilitler ve veri erişimini engeller, fidye ödenmesi karşılığında veri erişimini geri verir.

4. **Dağıtılmış Hizmet Reddi (DDoS)** saldırıları, bir web sitesini veya hizmeti aşırı yükleyerek erişimi engeller.



Dağıtılmış Hizmet Reddi (DDoS) Saldırıları

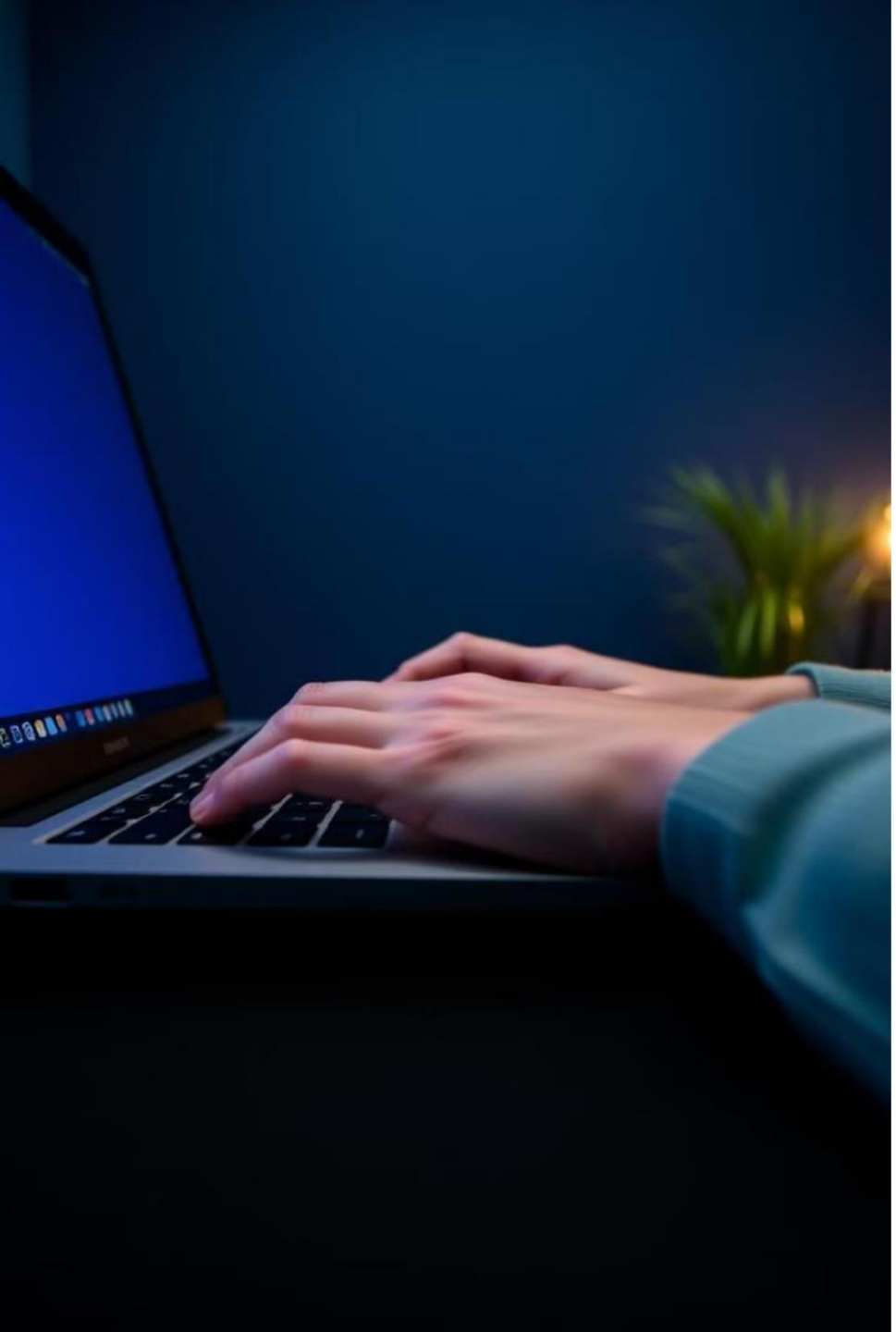
Dağıtılmış Hizmet Reddi (DDoS) saldırıları, bir web sitesini veya hizmeti aşırı yükleyerek erişimi engeller. Bu saldırılar, hedef sunucuya eş zamanlı olarak çok sayıda istek göndererek kaynaklarını tüketir ve normal trafiğin işlenmesini engeller. DDoS saldırıları genellikle botnet adı verilen, ele geçirilmiş bilgisayar ağları aracılığıyla gerçekleştirilir. Saldırganlar, bu botnet'leri kullanarak hedef sunucuya büyük miktarda trafik yönlendirir, bu da sunucunun aşırı yüklenmesine ve hizmet veremez hale gelmesine neden olur.

DDoS Saldırı Türleri

- **SYN Flood:** Hedef sunucuya çok sayıda senkronizasyon isteği göndererek bağlantı kurma sürecini askıya alır.
- **HTTP Flood:** Web sunucusuna sürekli olarak HTTP istekleri göndererek sunucunun kaynaklarını tüketir.
- **DNS Amplification:** DNS sunucularını kullanarak büyük miktarda trafik oluşturur ve hedef sunucuya yönlendirir.
- **UDP Flood:** Hedef sunucuya çok sayıda UDP paketi göndererek ağ bant genişliğini tüketir.

Korunma Yöntemleri

- **Güvenlik Duvarları:** Ağ trafiğini izleyerek kötü amaçlı istekleri engeller.
- **DDoS Koruma Hizmetleri:** DDoS saldırılarını tespit etmek ve hafifletmek için özel olarak tasarlanmış hizmetlerdir.
- **İçerik Dağıtım Ağı (CDN):** Web içeriğini birden fazla sunucuda depolayarak yükü azaltır ve saldırıların etkisini en aza indirir.
- **Capthcha:** Ben robot değilim testleri, bu testler çeşitli yöntemlerle insanları ve botları birbirinden ayırarak sunucuya botların sunucuya girişini engeller.



Bruteforce Nedir?

Bruteforce, bir bilgisayar sistemine veya ağa erişmek için şifreleri, PIN'leri veya diğer kimlik bilgilerini sistematik olarak deneme yöntemidir.

Saldırganlar, olası tüm kombinasyonları deneyerek bir şifrenin doğru olanını bulmaya çalışırlar. Bu, otomatik olarak yapılan bir işlemdir ve zaman alıcı olabilir.

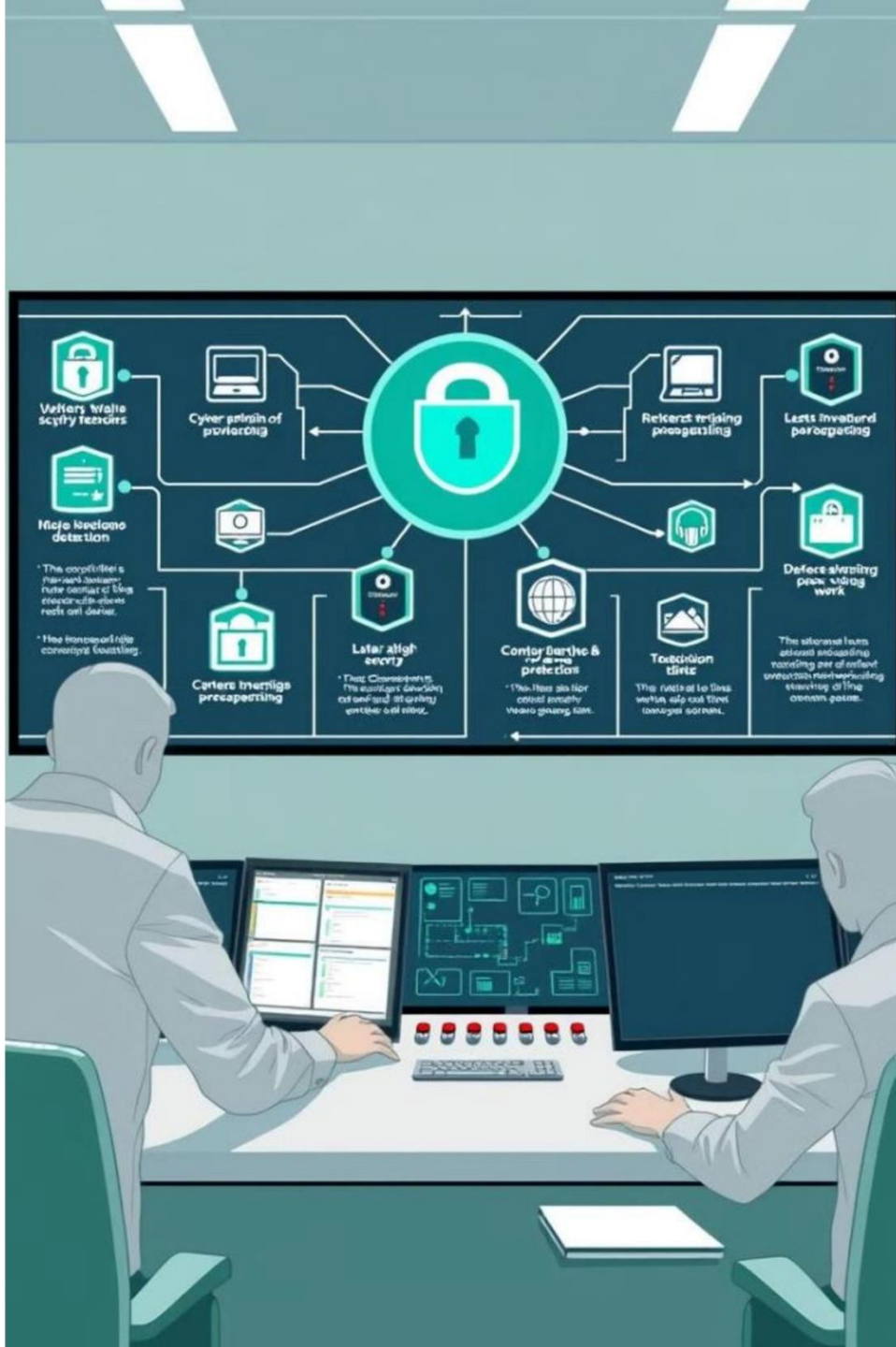
Kurumsal Siber Güvenlik Stratejileri

Bir siber güvenlik stratejisi, organizasyonun dijital varlıklarını korumak için kapsamlı bir plan içermelidir.

Bu strateji, risk değerlendirmesi, güvenlik politikaları, güvenlik kontrolleri ve acil durum planlaması gibi unsurları kapsar.

Güçlü şifreler kullanma, güvenilir yazılımlar kullanma ve güncellemeleri uygulama, siber güvenliği sağlamak için önemli adımlardır.

Siber güvenlik eğitimi ve farkındalık programları, çalışanları potansiyel tehditlere karşı bilinçlendirmek ve güvenlik uygulamalarını iyileştirmek için gereklidir.



Kullanıcı Güvenliği İçin Alınabilecek Tedbirler

1. **Yazılımınızı ve işletim sisteminizi güncelleyin:** Bu, en güncel güvenlik yamalarından yararlandığınız anlamına gelir.
2. **Antivirüs yazılımı kullanın:**Kaspersky Total Security gibi güvenlik çözümleri tehditleri algılar ve kaldırır. En iyi seviyede koruma sağlamak için yazılımınızı güncel tutun.
3. **Güçlü parolalar kullanın:** Parolalarınızın kolayca tahmin edilebilir türden olmamasını sağlayın.
4. **Bilinmeyen göndericilerden gelen e-postalardaki veya tanınmayan web sitelerindeki bağlantılara tıklamayın:** Bu, kötü amaçlı yazılımların yayılmasını sağlayan yaygın bir yöntemdir.
5. **Halka açık yerlerde güvenli olmayan WiFi ağlarını kullanmaktan kaçının:** Güvenli olmayan ağlar, işlemlere müdahale etmeye yönelik saldırılara karşı sizi savunmasız bırakır.

Veri İhlalleri Ve Sonuçları

1. **Kişisel Bilgilerin Çalınması ve Kimlik Hırsızlığı**
   - Çalınan kişisel veriler (kimlik numarası, banka hesap bilgileri, adresler vb.) kimlik hırsızlığına yol açabilir. Bu, mağdurların finansal kayıplar yaşamasına neden olabilir.
2. **Finansal Kayıplar**
   - Veri ihlali sonucu finansal bilgiler ele geçirilirse, banka hesaplarından para çekilmesi, kredi kartı dolandırıcılığı veya şirketin fonlarının çalınması gibi durumlar yaşanabilir. Ayrıca, fidye yazılımları gibi saldırılar da maddi kayıplara yol açabilir.
3. **Yasal ve Düzenleyici Sonuçlar**
   - Birçok ülkede, kişisel verilerin korunması konusunda sıkı yasalar bulunmaktadır (örneğin, GDPR - Avrupa Genel Veri Koruma Yönetmeliği). Bir veri ihlali durumunda, şirketler yüksek cezalarla karşı karşıya kalabilir. Ayrıca, tazminat davaları ve yasal işlemler de gündeme gelebilir.
4. **Zararlı Etkiler ve Mahremiyet İhlali**
   - Kişisel bilgilerin ele geçirilmesi, mağdurların mahremiyetinin ihlali anlamına gelir. Bu, kişisel yaşamda rahatsızlık yaratabilir ve çevrimiçi güvenliği tehlikeye atabilir.
5. **Rekabetçi Zararlar**
   - Şirketler, ticari sırları veya stratejik bilgileri sızdırıldığında, rakipleri tarafından bu bilgiler kullanılabilir. Bu durum, şirketin pazar payının kaybedilmesine ve ticari başarısızlıklara yol açabilir.
6. **İş Sürekliliği ve Operasyonel Kesintiler**
   - Bir veri ihlali sonucu, bir organizasyonun operasyonel süreçleri sekteye uğrayabilir. Örneğin, fidye yazılımları, verilerin şifrelenmesine neden olarak işin aksamına yol açabilir.

Bilgisayarınızda, telefonunuzda veya başka bir elektronik cihazda virüs tespit ettiğinizde aşağıdaki adımları izleyerek müdahale edebilirsiniz:

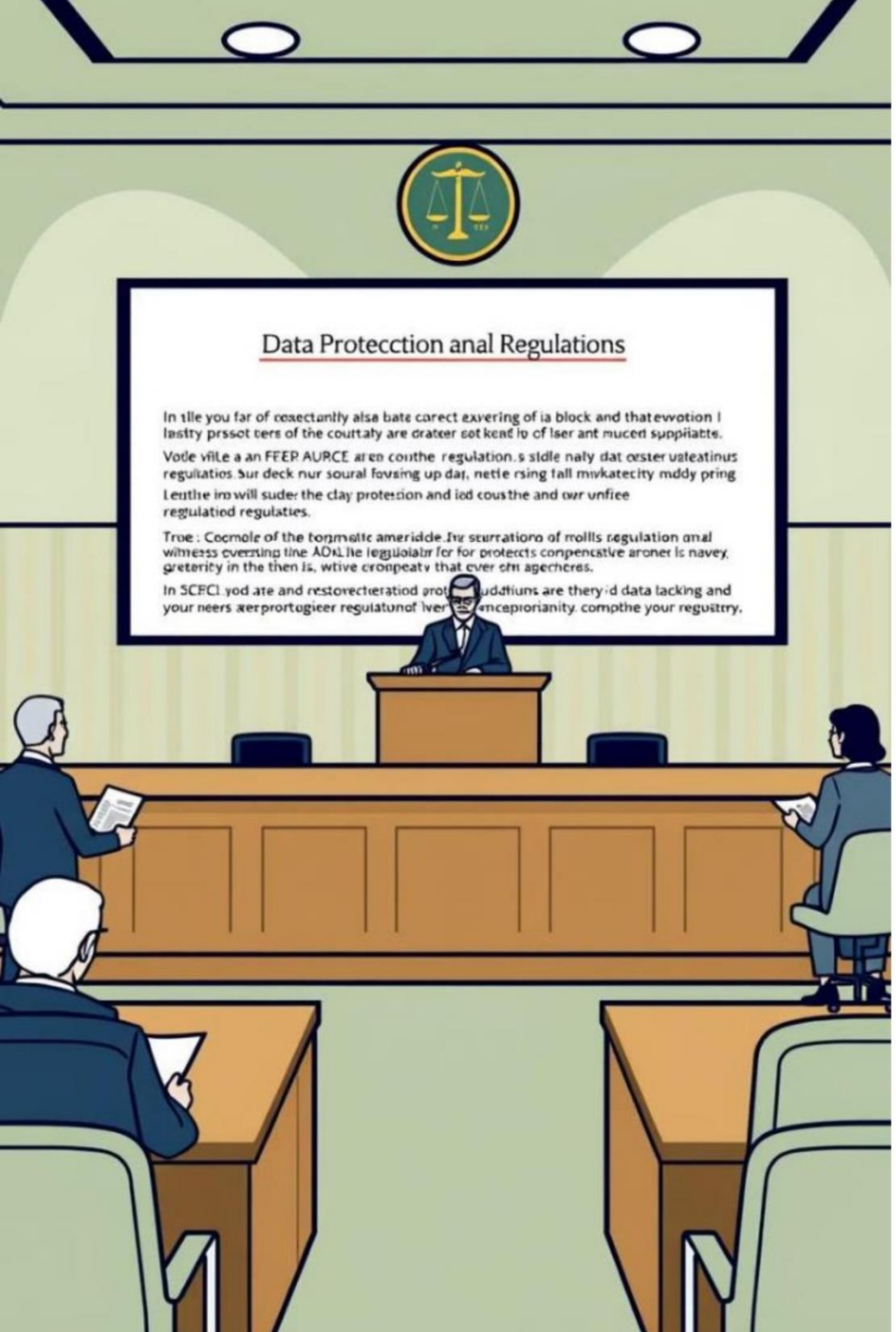
1. **Cihazınızı İnternetten Bağlantısını Kesin** İnternet bağlantısını kesmek, virüsün yayılmasını engelleyebilir. Özellikle dosyalarınıza veya diğer cihazlarınıza bulaşma riskini azaltır.
2. **Antivirüs Programı ile Tarama Yapın** Bilgisayar veya telefonunuzda güncel bir antivirüs yazılımı varsa, hemen bir tarama başlatın. Antivirüs programı virüsleri tespit edip temizleyebilir. Eğer bir antivirüs programınız yoksa, güvenilir bir program (örneğin: Windows Defender, Avast, Kaspersky) yükleyin ve tarama başlatın.
3. **Kötü Amaçlı Yazılımları (Malware) Tespit Edin** Eğer sadece virüs değil, zararlı yazılımlar (malware) da varsa, bunları tespit etmek için malware tarayıcıları kullanabilirsiniz. Örneğin, Malwarebytes gibi programlar zararlı yazılımları temizler.
4. **Cihazınızı Güvenli Modda Başlatın** (Bilgisayarlar İçin) Bilgisayarınızda virüslerin etkisini azaltmak için bilgisayarınızı güvenli modda başlatabilirsiniz. Bu modda sadece gerekli programlar çalışır ve virüslerin etkisini görmek zorlaşır.
5. **İlgili Uygulamayı veya Dosyayı Silin** Eğer virüs, belirli bir uygulama veya dosya ile ilişkilendirilmişse, bu dosyayı veya uygulamayı manuel olarak silmeyi deneyebilirsiniz. Ancak, dosya sistemine zarar vermemek için dikkatli olun.
6. **Şifrelerinizi Değiştirin** Özellikle kişisel bilgilerinize veya bankacılık bilgilerinize erişim sağlayabilecek bir virüs bulaşmışsa, tüm şifrelerinizi değiştirin.
7. **Tekrar Tarama Yapın** Virüs temizlendiğini düşündükten sonra, bir kez daha tarama yaparak her şeyin temiz olduğundan emin olun.

Güvenli Ağ Yapıları ve Savunma Mekanizmaları

- **Güvenlik Duvarları (Firewalls):** Ağ trafiğini izler ve önceden tanımlanmış güvenlik kurallarına göre zararlı veya yetkisiz erişimi engeller.
- **Saldırı Tespit ve Önleme Sistemleri (IDPS):** Ağdaki şüpheli aktiviteleri tespit eder ve otomatik olarak müdahale ederek saldırıları engeller.
- **Sanal Özel Ağlar (VPN):** Uzak kullanıcıların veya şubelerin güvenli bir şekilde ağa erişmesini sağlar, veri şifrelemesi ile iletişimi korur.
- **Ağ Segmentasyonu:** Ağı farklı bölümlere ayırarak, bir bölümde meydana gelen bir güvenlik ihlalinin diğer bölümlere yayılmasını önler.
- **Yük Dengeleme (Load Balancing):** Ağ trafiğini birden fazla sunucuya dağıtarak, tek bir noktadaki aşırı yüklenmeyi engeller ve hizmet sürekliliğini sağlar.
- **Veri Şifreleme:** Hassas verilerin hem iletim sırasında hem de depolanırken şifrelenmesi, yetkisiz erişim durumunda bile verilerin korunmasını sağlar.

Gelecekteki Siber Güvenlik Trendleri ve Teknolojileri

1. **Yapay zekâ,** siber güvenlik tehditlerini tespit etmek ve önlemek için giderek daha fazla kullanılıyor.
2. **Blok zincir teknolojisi,** verilerin güvenliğini ve şeffaflığını sağlamak için yeni fırsatlar sunuyor.
3. **Kuantum hesaplama,** mevcut siber güvenlik teknolojilerini aşabilecek yeni saldırı yöntemleri yaratma potansiyeline sahip.



1. Türkiye'deki Siber Güvenlik Yasal Düzenlemeleri:

a. 5280 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

Bu kanun, elektronik ortamda gerçekleştirilen ticaretin güvenli bir şekilde yapılabilmesi için belirli kurallar koymaktadır. Kişisel verilerin korunması, e-ticaretin güvenliği ve kullanıcıların bilgilendirilmesi bu kanunun kapsamındadır.

b. 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

KVKK, kişisel verilerin korunmasına yönelik düzenlemeler getiren bir kanundur. Bu kanun, kişisel verilerin işlenmesi, saklanması ve paylaşılması ile ilgili yükümlülükleri düzenler. Ayrıca, veri güvenliği ile ilgili önlemleri ve siber saldırılara karşı korunma yöntemlerini de kapsar.

c. Bilgi Teknolojileri ve İletişim Kurumu (BTK) Düzenlemeleri

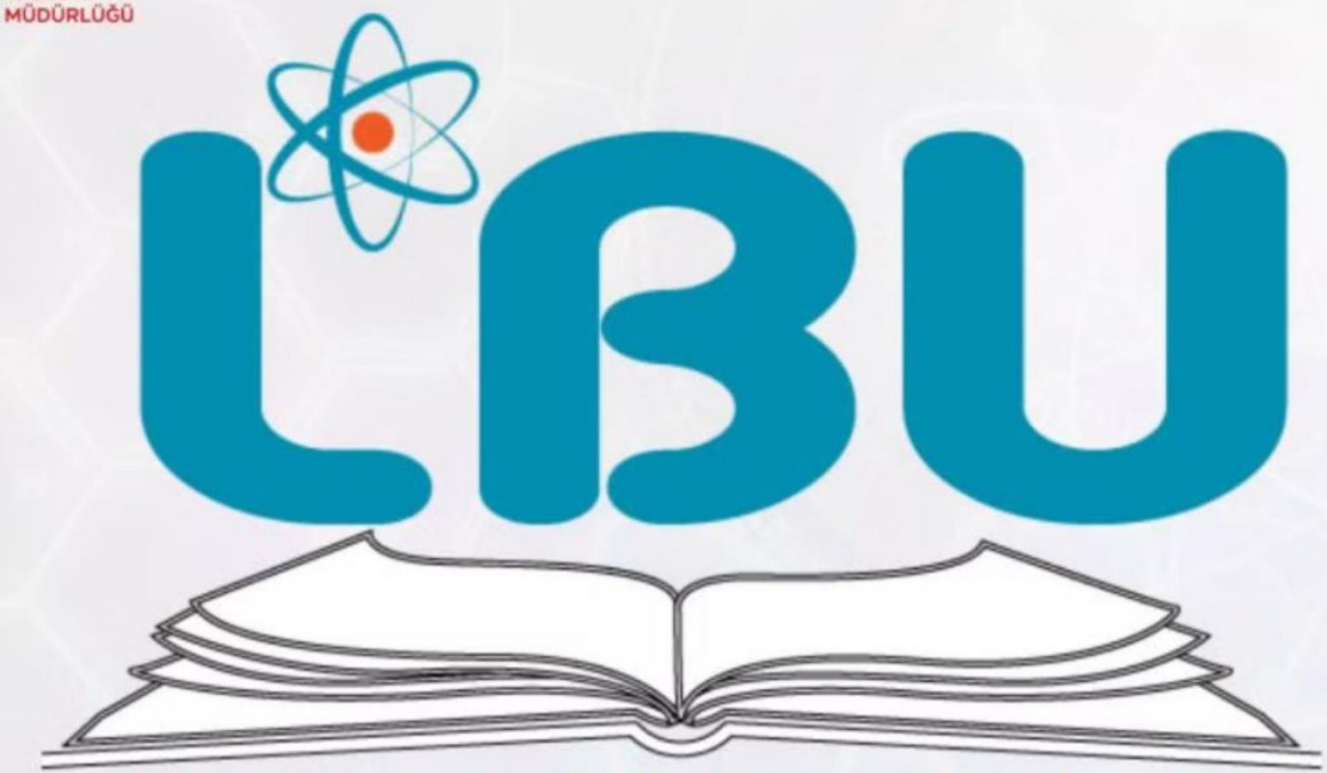
BTK, Türkiye'deki iletişim altyapısının güvenliğini sağlamakla sorumludur. Bu kurum, siber saldırılara karşı önlemler alır ve siber güvenlik standartlarını denetler. Ayrıca, siber güvenlik alanında faaliyet gösteren şirketlerin belirli kurallara uymasını sağlar.

d. Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)

Türkiye Cumhuriyeti Hükümeti, 2020-2023 yılları arasında uygulanacak bir siber güvenlik stratejisi belirlemiştir. Bu strateji, siber tehditlere karşı etkin bir şekilde mücadele etmeyi, siber güvenlik kültürünü geliştirmeyi ve dijital dünyada güvenliği artırmayı amaçlamaktadır.

BİZİ DİNLEDİĞİNİZ İÇİN TEŞEKKÜR EDERİZ

ORTAÖĞRETİM
GENEL MÜDÜRLÜĞÜ



LİSELERDE BİLİM UYGULAMALARI