

SİBER GÜVENLİK

Devletlerden Bireylere ve Aileye Dijital Güvenlik Perspektifleri

Dr. Hüseyin ŞIRA

BU SUNUMDA NELER VAR?

BİLDİKLERİMİZ (SIKÇA DUYDUKLARIMIZ)

- Siber suçlarla mücadele
- Siber tehdit
- Siber güvenlik şirketleri
- Hackerlar
- Siberay
- Virüs, Trojan...

BİLMEDİKLERİMİZ (HIÇ DUYMADIĞIMIZ YA DA NADİREN DE OLSA ADI GEÇENLER)

- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
- BTK
- 5. harp sahası
- Siber savunma
- Phishing
- SOC, Log vs.
- Malware...

SİBER GÜVENLİK NEDİR?

Dijital dünyada verileri, ağları ve sistemleri koruma disiplini. Temel amacı CIA (Gizlilik, Bütünlük, Erişilebilirlik) üçlüsünü sağlamaktır.



GİZLİLİK

Verilerin sadece yetkili kişiler tarafından erişilebilir olmasını sağlar.



BÜTÜNLÜK

Verilerin yetkisiz kişilerce değiştirilmesini veya bozulmasını önler.



ERİŞİLEBİLİRLİK

Sistemlerin ve verilerin ihtiyaç duyulduğunda her zaman ulaşılabilir olmasıdır.

DEVLETLER İÇİN SİBER GÜVENLİK

ULUSAL GÜVENLİK MESELESİ

Siber uzay artık "beşinci harp sahası" olarak kabul edilmektedir. Devletler sadece fiziksel sınırlarını değil, dijital altyapılarını da korumak zorundadır.

KRİTİK ALTYAPILAR

Enerji, ulaşım, sağlık ve finans sistemleri devlet destekli siber saldırıların birincil hedefidir. Bu sistemlerin felç olması ulusal kaosa yol açabilir.

USOM VE SOME

Türkiye'de Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve kurumsal SOME'ler ile 7/24 siber vatan savunması yapılmaktadır.



TÜRKİYE'NİN SİBER GÖRÜNÜMÜ

140.000+

2023 yılında engellenen büyük ölçekli siber saldırı sayısı.

5. SIRA

Türkiye, dünya genelinde siber saldırılardan en çok etkilenen ülkeler arasında yer almaktadır.

STRATEJİK VE YASAL ADIMLAR

- ✓ **Siber Güvenlik Kanunu (2024):** Ulusal güvenlik ve ekonomik istikrar için kapsamlı yasal çerçeve.
- ✓ **Aktif Savunma:** Günlük ortalama 422 büyük saldırı ve 11 milyon zararlı erişim girişimi USOM tarafından engellenmektedir.
- ✓ **Yerli Teknoloji:** Siber güvenlikte dışa bağımlılığı azaltmak için yerli yazılım ve uzman yetiştirme teşvik edilmektedir.

Türkiye'nin siber görünümü aslında kale surlarının nöbeti gibidir.

SANAL SURLARIN NÖBETİ

Görünmez bir ağda, sonsuz bir akış,
Kablolar arasındadır her bakış.
Bir yanda fısıltılar, karanlık niyetler,
Diğer yanda kurulur, aşılmaz bentler.

Sıfırınca gün doğar, sessiz ve derinden,
Bir açık aranır, sistemin en derininden.
Şifreler birer mühür, kilitler ise demir,
Siber dünyada sabır, en büyük bir emirdir.

Ne kılıç var elde, ne kalkan ne mızrak,
Savaşın alanı hem yakın hem uzak.
Veri dediğin hazine, en kıymetli cevher,
Onu korumak için, uyanık bekler her nefer.

Güvenlik bir yolculuk, bitmeyen bir emek,
Her satır kodda, binlerce anlam demek.
Sanal surlar yükselirken, hakikat baki kalır,
Bilgiye giden yolda, en güvenli iz kalır.



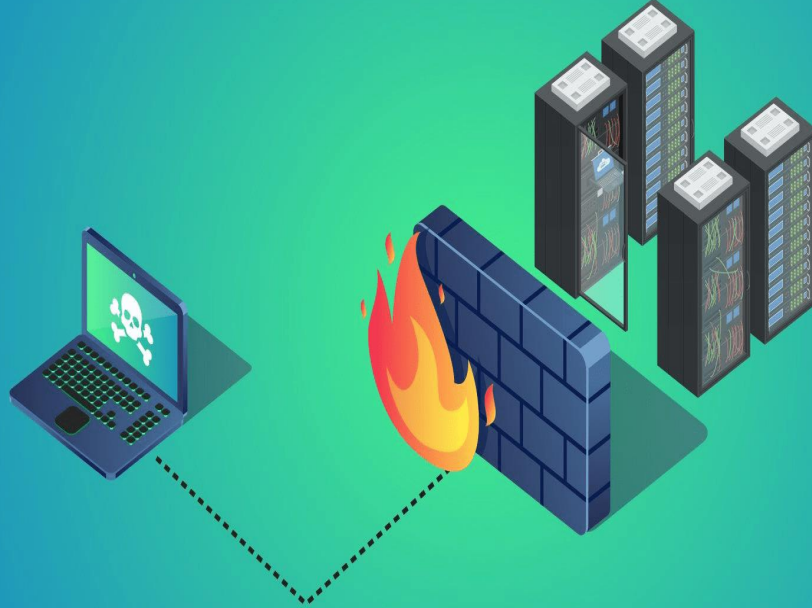
 VATAN SAVUNMASI DİJİTAL SINIRLARDA BAŞLAR

"Görünmez ordularımız, her satır kodda ve her veri paketinde ülkemizin geleceğini koruyor. USOM ve SOME birimlerimize minnetle."

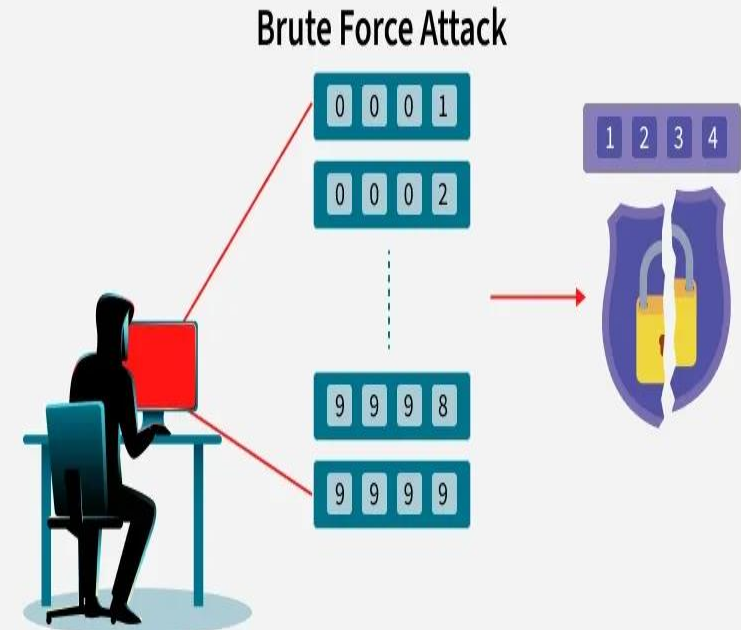
BAZI TEKNİK KAVRAMLAR



phishing



firewall



Brute force attack

BAZI TEKNİK KAVRAMLAR

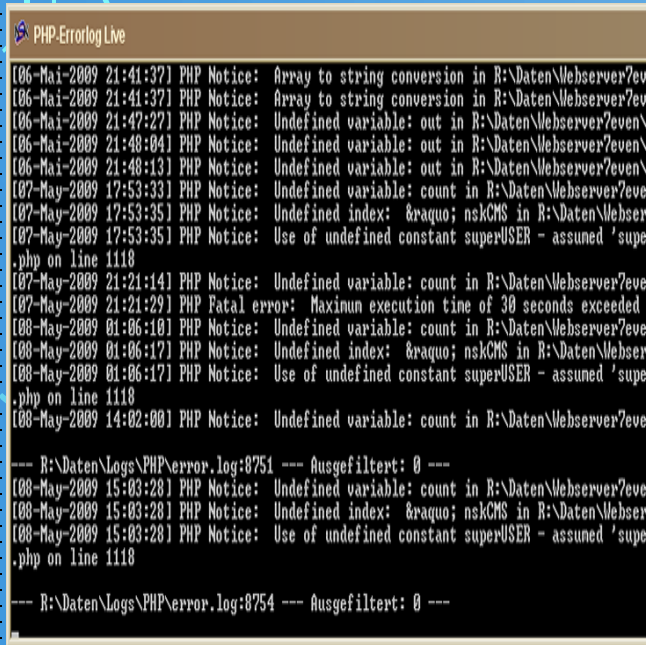


İki aşamalı doğrulama

trojan

Encryption

BAZI TEKNİK KAVRAMLAR



Log

SOC

Sandbox

Malware

Kodların Gölgesinde Savaş



Karanlık bir **phishing** oltası atılır suya,
Dikkatsiz bir tıkla dalar sistem uykuya.
Ama bizde **firewall** geçit vermez bir duvar,
Her paketi inceler, arkasında nöbet var.

Brute force ile zorlanır kapının kilidi,
Saniyede bin parola, bitmek bilmez ümidi.
Oysa **iki faktör** varsa, aşamaz o eşiği,
Söner siber korsanın o sahte güneş ışığı.

Bir **trojan** sızmak ister, tahta atın içinde,
Verileri kaçırmak, en sinsi bir biçimde.
Encryption devreye girer, diller birden karışır,
Şifreli o harflerle ancak makineler barışır.

Patch atılır yaraya, açıklar hemen kapanır,
Siber dünyanın kurdu, kendi ağında kapılır.
Uyanık kalmak gerek, bu bitmeyen bir maratonda,
Güvenliğin kalbinde, her zaman biz varız son!

KURUMLAR İÇİN RİSKLER



MALİYET VE İTİBAR KAYBI

Siber güvenlik artık sadece bir IT sorunu değil, bir yönetim kurulu meselesidir. Tek bir veri ihlali, yılların birikimini yok edebilir.

- ✓ **Veri ihlali Maliyeti:** Küresel ortalama ihlal başına maliyet 4 milyon dolar seviyesindedir.
- ✓ **Operasyonel Durma:** Fidyeye yazılımları (Ransomware) şirket sistemlerini kilitleyerek iş sürekliliğini bitirebilir.
- ✓ **Yasal Cezalar:** KVKK gibi düzenlemelere uyulmaması durumunda ağır idari para cezaları uygulanır.

KURUMSAL TEDBİRLER



UYUM VE STANDARTLAR

KVKK (Kişisel Verilerin Korunması Kanunu) yükümlülüklerini yerine getirmek ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi standartlarını uygulamak.



İNSAN FAKTÖRÜ

En zayıf halka insandır. Düzenli farkındalık eğitimleri, ortalama (phishing) simülasyonları ve güçlü parola politikaları şarttır.



TEKNİK SAVUNMA

Güvenlik duvarları, uç nokta koruması (EDR), düzenli sızma testleri (Pentest) ve felaket kurtarma senaryoları.

Fidye Yazılımı: Kurumsal Kalenizi Savunun

SORUN: Saldırı Adım Adım Nasıl Gerçekleşir?

1. Ortalama: Saldırı Başlıyor

Saldırıların %75'i 'Özgeçmiş pdf' gibi görünen sahte e-postalarla başlar.



2. Sızma ve Yayılma: Sistemler Kilitleniyor

Zararlı yazılım ağa yayılarak kritik verileri çifreler ve iş sürekliliğini durdurur.



3. Sonuç: Yıkıcı Etkiler



Maddi Kayıp

Bir veri ihalinin ortalama maliyeti 4 milyon dolardır



Yasal Sonuçlar

KVKK kapsamında ağır idari para cezaları uygulanır



İtibar Kaybı

Yılların birikimi olan müşteri güveni sarsılır

ÇÖZÜM: Çok Katmanlı Savunma Stratejisi



Teknik Savunma İnşa Edin

Güvenlik duvarı, EDR (uç nokta koruması), düzenli sızma testleri yapın.

İnsan Faktörünü Güçlendirin

Personele düzenli ortalama simülasyonlar ve farkındalık eğitimleri verin.

Bireysel Güvenliği Standartlaştırın

Tüm hesaplarda güçlü şifreler ve 2 Adımlı Doğrulama (ZFA) kullanımını zorunlu kılın.



“

Siber güvenlik sadece bir IT sorunu değil, doğrudan bir yönetim kurulu meselesidir.”

Şirketin en üst düzeyde sahiplenmesi gereken stratejik bir konudur.

BİREYSEL TEHDİTLER

DİJİTAL AYAK İZİ

Sosyal medya, e-ticaret ve bankacılık uygulamalarıyla bıraktığımız dijital izler, siber suçlular için birer hedef noktasıdır.

YAYGIN SALDIRI TÜRLERİ

- ✔ **Öltalama (Phishing):** Saldırıların %75'i sahte e-postalarla başlar.
- ✔ **Kimlik Hırsızlığı:** Kişisel bilgilerin çalınarak adınıza işlem yapılması.
- ✔ **Sosyal Mühendislik:** İnsanların güvenini kullanarak bilgi sızdırma teknikleri.



KİŞİSEL KORUNMA YOLLARI



GÜÇLÜ ŞİFRELEME

Tahmin edilmesi zor, karmaşık şifreler kullanın ve her hesap için farklı şifre belirleyin. 2 Adımlı Doğrulamayı (2FA) mutlaka açın.



CİHAZ GÜVENLİĞİ

İşletim sisteminizi ve uygulamalarınızı güncel tutun. Kaynağı bilinmeyen linklere tıklamayın ve dosyaları indirmeyin.

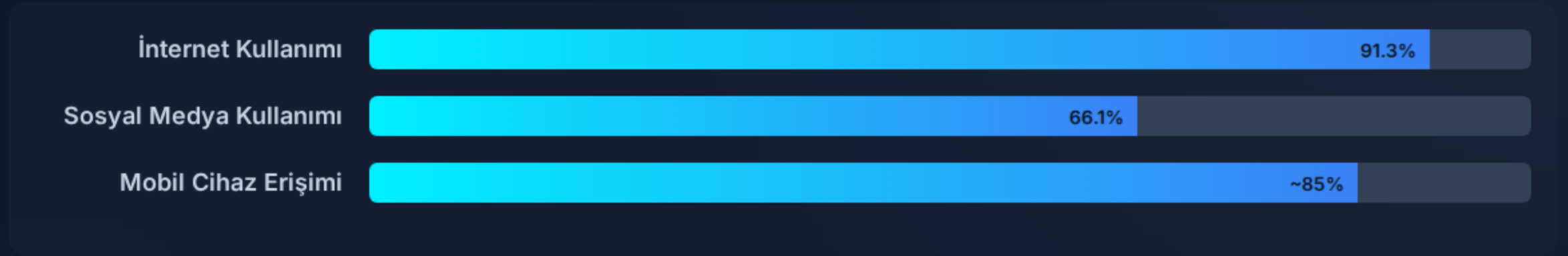


AĞ GÜVENLİĞİ

Ortak Wi-Fi ağlarında bankacılık işlemi yapmayın. Ev ağınızın şifresini güçlü tutun ve "https" protokolüne dikkat edin.

AİLELER VE İNTERNET: GÜNCEL DURUM

Türkiye'de çocukların dijital dünyaya erişimi oldukça yüksektir. Bu durum, aile içi denetimi zorunlu kılar. (TÜİK Verileri, 6-15 Yaş)



Yüksek erişim oranları, siber zorbalık ve uygunsuz içerik riskini beraberinde getirmektedir.

BİLİNÇLİ DİJİTAL EBEVEYNLİK



İLETİŞİM VE GÜVEN

Yasaklamak çözüm değildir. Çocuklarla internetteki deneyimleri hakkında açıkça konuşulmalıdır.

Karşılaştıkları bir tehdidi korkmadan anlatabilecekleri bir güven ortamı oluşturulmalıdır.



KURALLAR VE ARAÇLAR

Yaşa uygun ekran süreleri belirlenmelidir. "Güvenli İnternet Hizmeti" ve ebeveyn kontrol yazılımları gibi teknik araçlar kullanılmalı, ancak asıl denetimin ebeveyn rehberliği olduğu unutulmamalıdır.

GELECEĞİN AİLE YAPISINDA GÜVENLİK



Teknolojiyle Dost: Teknolojiyi yasaklayan değil, onu güvenli ve üretken kullanan nesiller yetiştirmek.



Temel Değer: Dijital okuryazarlığın, dürüstlük ve saygı gibi temel bir aile değeri haline gelmesi.



Toplumsal Bilinç: Aileden başlayıp devlete uzanan bütüncül bir güvenlik kültürü oluşturmak.

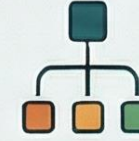
Siber Güvenlik: Devletten Aileye Ortak Sorumluluğumuz

Büyük Resim: Ulusal ve Kurumsal Tehditler



Türkiye, Küresel Siber Tehdit Altında 5. Sırada

Ülkemiz, dünya genelinde siber saldırılardan en çok etkilenen ülkelerden biridir.



Kritik Altyapılar Birincil Hedef

Enerji, sağlık ve finans gibi sistemlere yönelik saldırılar ulusal kaosa yol açabilir.



Kurumsal Maliyet: İhlal Başına 4 Milyon Dolar

Tek bir veri ihlali, şirketler için milyonlarca dolarlık maliyet ve itibar kaybı demektir.

Yakın Plan: Birey ve Aile İçin Dijital Kalkan



En Yaygın Saldırı: Oltalama (Phishing)

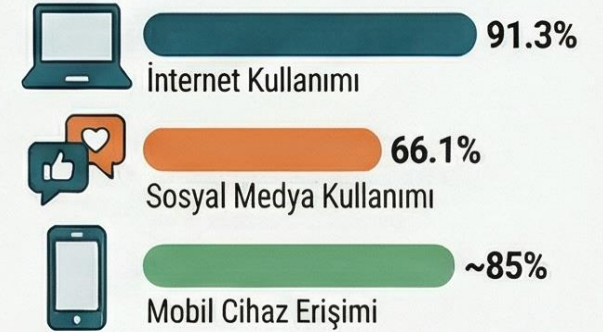
Siber saldırıların %75'i sahte e-postalar ve linklerle başlamaktadır.



Kişisel Korunmanın 3 Altın Kuralı

-  Güçlü şifreler
-  Güncel yazılımlar
-  Güvenli ağ kullanımı

Çocukların Dijital Erişimi (6-15 Yaş)



Sonuç: Güvenli Gelecek Bilinçli Kullanımla Başlar



“Siber güvenlik, devletten bireye herkesin ortak sorumluluğundadır.”

Teknik önlemler kadar toplumsal bilinç de dijital dünyamızı korur.

Dijital Savunma Hattı: Toplumsal Sorumluluk Kültürü

Siber güvenlikte bütüncül bir savunma kültürü oluşturmak, toplumun her kesiminin aktif katılımını gerektiren kolektif bir çabadır. Güvenli bir dijital gelecek, bu sorumluluğun devlet politikalarından bireysel şifre seçimine kadar her seviyede benimsenmesiyle mümkündür.

DEVLET: Büyük Barajlar ve Kanallar

Sorumluluk Katmanı

Ulusal siber savunma altyapısını kurar.

Siber uzayı “beşinci harp sahası” olarak kabul eder ve yasal çerçeveler oluşturur.

KURUMLAR VE ŞİRKETLER: Mahalle Drenaj Sistemleri

Sorumluluk Katmanı

Kendi sistemlerini ve verilerini koruma altına alır.

Güvenliği bir IT sorunu değil, “yönetim kurulu meselesi” olarak ele alır.

AİLELER VE BİREYLER: Ev Önü Su Giderleri

Sorumluluk Katmanı

Kişisel cihaz ve hesaplarının güvenliğini sağlar.

Dijital okuryazarlığı dürüstlük gibi “temel bir aile değeri” haline getirir.

Güçlü şifreleme ve 2 Adımlı Doğrulama (2FA) gibi kişisel önlemleri uygular.



SONUÇ: ORTAK SORUMLULUK

Siber güvenlik sadece teknik uzmanların işi değildir. Devletin stratejik korumasından, kurumların veri güvenliğine, bireylerin şifre seçiminden ailenin çocuk eğitimine kadar herkesin sorumluluğundadır.

"Güvenli Gelecek, Bilinçli Teknoloji Kullanımıyla Başlar."

Siber Cephenin Kalbi

Ekranlarda akar gider, binlerce satır **log**,
Bir sızıntı sezilirse, başlar hemen o diyalog.
SOC ekibi tetikte, gözler hiç kırılmıyor,
Tehditler bir bir düşerken, sistem sarsılmıyor.

Sandbox içinde hapsolür, o zehirli yazılım,
Analizler yapılırken, atılır her bir adım.

Malware dediğin sinsî, kılık değıştirse bile,
Kurtulamaz bu ağdan, yapîlsa yüz bin hîle.

Varsa eğer SORULAR?

Dinlediğiniz için teşekkürler.



Source: www.infotrust.com.au



Source: us.norton.com



https://plus.unsplash.com/premium_photo-1754980059771-3d50115cbcae?fm=jpg&q=60&w=3000&ixlib=rb-4.1.0&ixid=M3wxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8fA%3D%3D
Source: [unsplash.com](https://plus.unsplash.com/premium_photo-1754980059771-3d50115cbcae?fm=jpg&q=60&w=3000&ixlib=rb-4.1.0&ixid=M3wxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8fA%3D%3D)

IMAGE SOURCES



https://static.vecteezy.com/system/resources/thumbnails/026/384/935/small_2x/futuristic-glowing-padlock-with-plexus-lines-and-glitter-particles-a-padlock-in-the-neon-light-style-cyber-security-data-and-privacy-protection-digital-technology-background-vector.jpg

Source: www.vecteezy.com