Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Siber Güvenlik Temelleri ve Çevrimiçi Tehdit Önleme

Siber güvenlik tehditleri, ağ güvenlik duvarları, çok faktörlü kimlik doğrulama, güvenlik çerçeveleri

SİBER GÜVENLİK TEMELLERİ ÖĞRENME GENEL BAKIŞI

GÜVENCEDE
VERİ ŞİFRELEME
256 bit AES Standardı

UYUMLU
KÜRESEL STANDARTLAR
GDPR ve CCPA çerçeveleri

SIFIR GÜVEN
ERİŞİM POLİTİKASI
Çok Faktörlü Kimlik Doğrulama

Hoş geldin! Bu etkinlik paketi sana Siber Güvenlik Temelleri ve Çevrimiçi Tehdit Önleme'nin temel ilkeleri konusunda rehberlik eder. Kötü amaçlı yazılım tehditlerini, çok faktörlü kimlik doğrulamayı, ağ güvenlik duvarlarını ve olay müdahale çerçevelerini keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: Siber güvenlikte ve tehdit önlemede ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com siber güvenlik rehberini aç

URL: https://www.vpn.com/tr/siber-guvenlik/

Siber Güvenlik Temelleri Öğrenme Yol Haritan

- Kötü amaçlı yazılımın, kimlik avının ve kurumsal ağa sızmanın yaygın yollarını belirle.
- MFA, güvenlik duvarları ve uç nokta savunması dahil standart siber güvenlik denetimleri uygula.
- Veri ihlali etkilerini azaltmaya yönelik olay müdahale prosedürlerini değerlendir.
- NIST yönergeleri kapsamında kurumsal risk etkenlerini ve güvenlik uyumunu analiz et.
- Otomatik kimlik bilgisi doldurma saldırılarını azaltmak için güvenlik hijyeni uygulamalarını yapılandır.

SİBER GÜVENLİK REHBERİ TALİMATLARI

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: tehdit önleme. Hızlı Düşün bonus etkinliğiyle bitir.

SİBER GÜVENLİK TEMELLERİ VE TEHDİT ÖNLEME (GİRİŞ)

Siber güvenlik; ağları, sistemleri ve verileri yetkisiz dijital saldırılardan korur. Sağlam güvenlik alışkanlıkları geliştirmek, güvenlik duvarlarını yapılandırmak, çok faktörlü kimlik doğrulamayı zorunlu kılmak ve personeli tehdit tanıma konusunda eğitmek, kurumsal ağ savunmasının temel bileşenleridir.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ.

Kontrol Noktası 1: Çoktan seçmeli görev

1. Kimlik avı saldırısının temel amacı nedir?

- A. Kimlik bilgilerini ve hassas kullanıcı verilerini çalmak
- B. Web sitesinin arama motorlarındaki görünürlüğünü artırmak
- C. Ağ bant genişliği kapasitesini artırmak
- D. Yedek veri merkezi çoğaltmasını yönetmek

2. Hangi mekanizma en güçlü hesap korumasını sağlar?

- A. Donanım anahtarları kullanan çok faktörlü kimlik doğrulama
- B. Otuz günde bir güncellenen karmaşık parolalar
- C. Hesap girişini mesai saatleriyle sınırlamak
- D. Hesap kullanıcı adını herkese açık dizinlerden gizlemek

3. Fidye yazılımı bulaşmasının yükünü ne tanımlar?

- A. Sistem dosyalarını şifrelemek ve ödeme talep etmek
- B. Tuş vuruşlarını uzak sunuculara sessizce kaydetmek
- C. Tarayıcılara yetkisiz reklam enjekte etmek
- D. Kripto para madenciliği için yerel CPU kaynaklarını kullanmak

4. Sıfırıncı gün (zero-day) açığı güvenlik savunmalarını nasıl etkiler?

- A. Yama uygulanmamış, bilinmeyen güvenlik açıklarını hedefler
- B. Kurumsal güvenlik duvarını otomatik olarak devre dışı bırakır
- C. Sistemi sert yeniden başlatmaya zorlar
- D. Giderilmesi için sıfır bütçe gerekir

5. Kurumsal güvenlik kontrollerini hangi çerçeve yönetir?

- A. NIST Siber Güvenlik Çerçevesi yönergeleri
- B. W3C HTML5 belge şeması özellikleri
- C. Yazıcı sürücüsü kurulum kılavuzları
- D. IETF yönlendirme protokolü tanımları

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru D/Y 6

6. Kimlik avı saldırıları yalnızca kişisel e-posta hesaplarını hedef alır.

○ Doğru ○ Yanlış

7 Soru D/Y 7

7. Çok faktörlü kimlik doğrulama, kimlik bilgisi doldurma saldırılarını engellemeye yardımcı olur.

○ Doğru ○ Yanlış

8 Soru D/Y 8

8. Güvenlik duvarları, yetkisiz bağlantı noktası erişimini engellemek için ağ trafiğini inceler.

○ Doğru ○ Yanlış

9 Soru D/Y 9

9. Sıfırıncı gün istismarlarının giderilmesi standart antivirüs tanım güncellemelerini gerektirir.

○ Doğru ○ Yanlış

10 Soru D/Y 10

10. Honeypot, siber suçluları cezbetmek için kullanılan tuzak sunucudur.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Ağ yöneticileri gelen trafiği filtrelemek için bir _____ kurar.

2. Bir saldırgan, sistem yamalarını aşmak için bir _____ kullanır.

3. Saldırganlar çalışanlara karşı _____ kampanyaları yürütmek için sahte e-postalar gönderir.

4. Fidye yazılımı, kullanıcı verilerini kilitleyen yıkıcı bir _____ türüdür.

5. Güçlü parola _____ sağlamak, kimlik bilgisi hırsızlığı risklerini azaltır.

6. Hassas iletişimi korumak için kullanıcılar _____ protokolleri uygular.

KELİME BANKASI

BAL KÜPÜ · ÇOK FAKTÖRLÜ · GÜVENLİK DUVARI · HİJYEN · KİMLİK AVI · KÖTÜ AMAÇLI YAZILIM · SIFIR GÜN AÇIĞI · ŞİFRELEME

Cevaplarını buraya yaz:

1.
2.
3.
4.
5.
6.

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

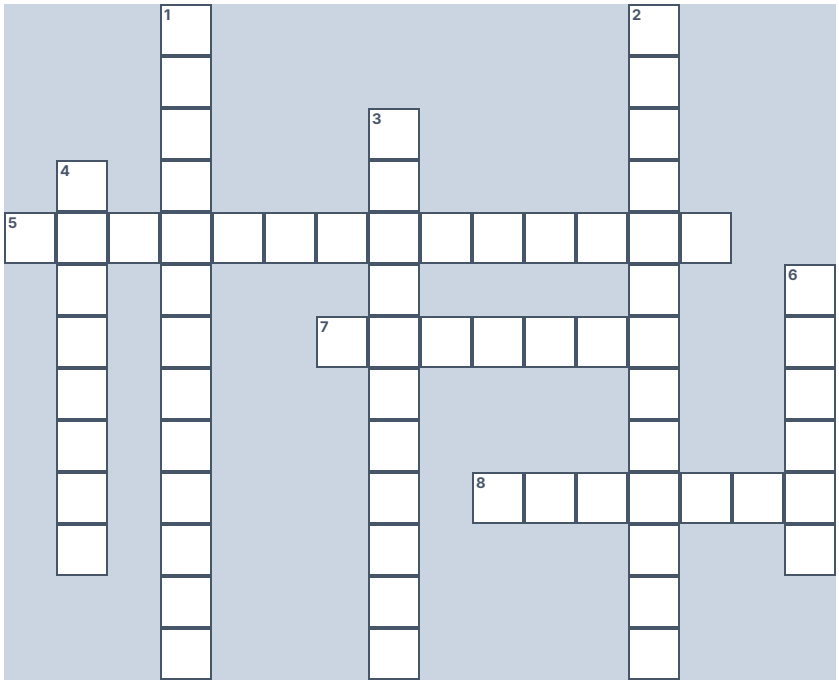
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

☐	1. Fidye Yazılımı Tehdidi	A	Siber riskleri yönetmek için kullanılan NIST gibi yapılandırılmış yönergeler.
☐	2. Çok Faktörlü Kimlik Doğrulama	B	Güvenlik ihlallerini ele alma ve hafifletme için yapılandırılmış plan.
☐	3. Sıfırıncı Gün Açığı İstismarı	C	Trafiği güvenlik kurallarına göre filtreleyen ağ bariyeri.
☐	4. Tuzak Bal Küpü	D	Verileri şifreleyip çözmek için maddi ödeme talep eden kötü amaçlı yazılım.
☐	5. Saldırı Güvenlik Duvarı	E	Satıcı yama yayımlamadan önce hedeflenen güvenlik açığı istismarı.
☐	6. Olay Müdahalesi	F	Kimlik bilgilerini ve kimlik doğrulama anahtarlarını yönetmeye yönelik en iyi uygulamalar.
☐	7. Parola Hijyeni	G	İki veya daha fazla kimlik doğrulama faktörü gerektiren güvenlik doğrulaması.
☐	8. Güvenlik Çerçevesi	H	Kötü niyetli kişileri çekip analiz etmek için kurulan tuzak sistem.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

5. Trafiği güvenlik kurallarına göre filtreleyen ağ bariyeri (14)

7. Kötü niyetli kişileri çekip analiz etmek için kurulan yem sistem (7)

8. Siber riskleri yönetmek için kullanılan NIST gibi yapılandırılmış yönergeler (7)

YUKARIDAN AŞAĞI

1. Verileri şifreleyip şifre çözme karşılığında ödeme talep eden kötü amaçlı yazılım (13)

2. Satıcı yama yayımlamadan önce hedeflenen güvenlik açığı istismarı (13)

3. İki veya daha fazla kimlik doğrulama faktörü gerektiren güvenlik doğrulaması (11)

4. Güvenlik ihlallerini ele almak ve azaltmak için yapılandırılmış plan (8)

6. Kimlik bilgilerini ve kimlik doğrulama anahtarlarını yönetmeye yönelik en iyi uygulamalar (6)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

5 soldan sağa: Trafiği güvenlik kurallarına göre filtreleyen ağ bariyeri (14 harf):

7 soldan sağa: Kötü niyetli kişileri çekip analiz etmek için kurulan yem sistem (7 harf):

8 soldan sağa: Siber riskleri yönetmek için kullanılan NIST gibi yapılandırılmış yönergeler (7 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Verileri şifreleyip şifre çözme karşılığında ödeme talep eden kötü amaçlı yazılım (13 harf):

2 yukarıdan aşağı: Satıcı yama yayımlamadan önce hedeflenen güvenlik açığı istismarı (13 harf):

3 yukarıdan aşağı: İki veya daha fazla kimlik doğrulama faktörü gerektiren güvenlik doğrulaması (11 harf):

4 yukarıdan aşağı: Güvenlik ihlallerini ele almak ve azaltmak için yapılandırılmış plan (8 harf):

6 yukarıdan aşağı: Kimlik bilgilerini ve kimlik doğrulama anahtarlarını yönetmeye yönelik en iyi uygulamalar (6 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

I	T	İ	P	B	Ü	Z	V	K	P	Ö	V	H	N	D
M	Ü	L	R	Ö	T	K	A	F	K	O	Ç	A	H	Ç
I	Ç	İ	Ö	U	Ü	Ü	J	I	Ğ	Ş	Ğ	İ	E	F
L	B	E	H	M	İ	S	R	U	P	Z	J	R	E	Ğ
I	E	R	C	Ü	A	J	O	C	Z	Y	Ç	K	İ	U
Z	P	Ş	A	D	R	Ü	I	K	E	E	K	G	Ğ	L
A	Ğ	P	F	A	J	S	J	N	V	P	Ü	Ğ	B	Ş
Y	F	Y	M	H	Y	Ü	R	E	Ğ	S	V	A	O	T
E	M	M	Z	A	N	H	O	S	Ğ	O	T	Ş	N	Ş
Y	Ş	İ	A	L	E	N	L	B	A	L	K	Ü	P	Ü
D	G	Ü	V	E	N	L	İ	K	D	U	V	A	R	I
İ	J	B	M	T	F	G	O	Ö	Ü	Y	I	İ	T	I
F	Y	S	I	F	I	R	G	Ü	N	A	Ç	I	Ğ	I
U	V	O	İ	H	Z	H	I	L	A	E	H	B	S	A
I	E	U	E	İ	Z	İ	D	J	Ö	L	I	A	F	N

KELİME LİSTESİ

FİDYEYAZILIMI ÇOKFAKTÖRLÜ SIFIRGÜNAÇIĞI BALKÜPÜ GÜVENLİKDUVARI
MÜDAHALE HİJYEN ÇERÇEVE

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. FİDYEYAZILIMI**
- **B. ÇOKFAKTÖRLÜ**
- **C. SIFIRGÜNAÇIĞI**
- **D. BALKÜPÜ**
- **E. GÜVENLİKDUVARI**
- **F. MÜDAHALE**
- **G. HİJYEN**
- **H. ÇERÇEVE**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Trafiği güvenlik kurallarına göre filtreleyen ağ bariyeri.
2. Güvenlik ihlallerini ele almak ve azaltmak için yapılandırılmış plan.
3. Verileri şifreleyip şifre çözme karşılığında ödeme talep eden kötü amaçlı yazılım.
4. İki veya daha fazla kimlik doğrulama faktörü gerektiren güvenlik doğrulaması.
5. Kimlik bilgilerini ve kimlik doğrulama anahtarlarını yönetmeye yönelik en iyi uygulamalar.
6. Siber riskleri yönetmek için kullanılan NIST gibi yapılandırılmış yönergeler.
7. Satıcı yama yayımlamadan önce hedeflenen güvenlik açığı istismarı.
8. Kötü niyetli kişileri çekip analiz etmek için kurulan yem sistem.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel siber güvenlik kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. A D I M Y İ Z L F I I E Y
2. Ğ R I G F S I Ü I A Ç N I
3. G D Ü R K I U V V İ N L A E
4. N Y J E H İ
5. R O Ö T K Ü A K Ç L F
6. P L Ü B K Ü A
7. M E H A L Ü A D
8. E Ç E Ç V E R

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Siber güvenlikteki meslekler			
2	Yazılımı güncelleme nedenleri			
3	Bir güvenlik duvarının engelleyebileceği şeyler			
4	E-postadaki uyarı işaretleri			
5	Yedeklediğin şeyler			
6	Bilinen siber saldırı türleri			
7	Bir bal küpünün (honeypot) çekebileceği şeyler			
8	Asla paylaşmaman gereken bilgiler			
9	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
10	Hackerlar hakkında filmler veya diziler			
11	Oluşturabileceğin güvenlik katmanları			
12	Güvenlik tatbikatında çalışılacak şeyler			
13	Bildiğin güvenlik araçları			
14	BT yardımı için sorabileceğin kişiler			
15	'Siber' ile başlayan sözcükler			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: FİDYE YAZILIMI KURTARMA STRATEJİSİ



Senaryo: Kurumsal bir ağ fidye yazılımıyla enfekte oluyor ve kritik veritabanlarını kilitliyor. Saldırganlar 100.000 $ tutarında kripto para ödemesi talep ediyor. Şirketin 24 saat öncesine ait çevrimdışı yedekleri var.

Tartışma sorusu: Ödeme yapmanın risklerini analiz et ve kurtarma stratejisini değerlendir.

VAKA ÇALIŞMASI 2: KİMLİK BİLGİSİ DOLDURMA SAVUNMALARI



Senaryo: Çevrimiçi bir hizmet, saldırganların diğer sitelerden çalınan milyonlarca kullanıcı adı/parola çiftini denediği bir kimlik bilgisi doldurma (credential stuffing) saldırısıyla karşılaşıyor.

Tartışma sorusu: Bu saldırının mekanizmasını ayrıntılı anlat ve iki savunma sistemini özetle.

Kontrol Noktası 9: Şifreyi Çöz

Bir siber güvenlik uzmanı, ağ varlıklarını çevrimiçi tehdit aktörlerine karşı korur. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10

I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20

R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

22	12	22	24	6	16	12	17	12	4	18	14

7	1	14	24	19	21	15	26

5	18	9	21	25	15	1	16	1	28	15	1	14	18	21	25

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm A)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q1: Siber güvenliğin temel amacı nedir?

Temel amaç; ağları, cihazları ve verileri yetkisiz erişimden, saldırılardan ve kazara hasardan korumaktır.

Q2: Kimlik avı, hedefli kimlik avından nasıl farklıdır?

Kimlik avı rastgele kullanıcıları hedef alan geniş bir e-posta kampanyasıdır; hedefli kimlik avı (spear phishing) ise kişiselleştirilmiş verilerle belirli bireyleri hedef alır.

Q3: Ağ güvenlik duvarı nedir?

Güvenlik duvarı, gelen ve giden trafiği önceden tanımlanmış güvenlik kurallarına göre izleyen ve filtreleyen bir ağ güvenlik sistemidir.

Q4: Çok faktörlü kimlik doğrulama (MFA) neden gereklidir?

MFA, saldırganlar asıl parola bilgilerini çalsa veya kırsa bile erişimi engelleyen kritik bir savunma katmanı ekler.

Q5: Bilgisayar virüsünü ne tanımlar?

Virüs, temiz dosyalara yapışan ve çalıştırıldığında sistemler arasında yayılan, kendini çoğaltan kötü amaçlı yazılımdır.

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm B)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Fidye yazılımı yerel verileri nasıl kilitler?

Fidye yazılımı, kullanıcı dosyalarını şifrelemek için kriptografik algoritmalar kullanır ve bir şifre çözme anahtarı uygulanana kadar bunları okunamaz hâle getirir.

Q7: Sıfır gün (zero-day) açığı nedir?

Sıfırıncı gün (zero-day), yazılımda satıcının bilmediği bir güvenlik açığıdır ve istismardan önce yama geliştirmeye zaman bırakmaz.

Q8: NIST çerçevesinin rolü nedir?

NIST çerçevesi, kuruluşların siber güvenlik risklerini yönetmesine ve azaltmasına yardımcı olan gönüllü yönergeler ve standartlar sunar.

Q9: Güvenlik olayı müdahale planı nedir?

Güvenlik ihlallerini ve ağ ele geçirilmesini algılama, sınırlama ve bunlardan kurtarma prosedürlerinden oluşan belgelenmiş bir settir.

Q10: Sosyal mühendislik kullanıcıları nasıl istismar eder?

Sosyal mühendislik, çalışanları parolalarını ifşa etmeye veya kötü amaçlı dosyalar indirmeye kandırmak için psikolojik manipülasyon kullanır.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q1: DDoS saldırısı web sunucularını nasıl bunaltır?

Bir DDoS saldırısı, bant genişliği ve CPU sınırlarını tüketmek için bir sunucuyu trafikle doldurmak üzere ele geçirilmiş milyonlarca botnet cihazını koordine eder.

Q2: Simetrik ve asimetrik şifreleme arasındaki fark nedir?

Simetrik şifreleme şifreleme ve çözme için tek bir anahtar kullanır; asimetrik şifreleme ise bir açık ve özel anahtar çifti kullanır.

Q3: Bilgisayar korsanları SQL enjeksiyonu saldırılarını nasıl gerçekleştirir?

Saldırganlar form alanlarına kötü amaçlı SQL komutları girerek arka uç veritabanını yetkisiz kullanıcı kayıtlarını vermesi için kandırır.

Q4: Ağ saldırılarında yanal hareket nedir?

Saldırganların ilk sunucu erişimini, iç ağdaki diğer birbirine bağlı sistemleri ele geçirmek için kullandığı tekniktir.

Q5: DNS sahteciliği web trafiğini nasıl başka yere yönlendirir?

DNS sahteciliği, ad sunucusu önbellek kayıtlarını değiştirerek meşru kullanıcıları hedef alan adları yerine kötü amaçlı benzer web sitelerine yönlendirir.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q6: Donanım güvenlik anahtarı nedir?

Kriptografik kimlik doğrulama kanıtları üreten, uzaktan kimlik avına karşı azami savunma sunan fiziksel bir cihazdır (YubiKey gibi).

Q7: Güvenlik ekipleri tuzak bal küplerini (honeypot) nasıl kullanır?

Ekipler, izinsiz girişleri erken tespit etmek ve yetkisiz kişilerin saldırı kalıplarını analiz etmek için üretim dışı tuzak sunucular kurar.

Q8: En az ayrıcalık ilkesi nedir?

Kullanıcı erişim haklarını iş rollerini yerine getirmek için gereken mutlak asgariyle kısıtlayan güvenlik standardıdır.

Q9: Ortadaki Adam saldırısı bağlantıları nasıl istismar eder?

Bir saldırganın şifrelenmemiş ağlarda iki cihaz arasındaki iletişimi araya girerek değiştirmesi ve oturum belirteçlerini ile kimlik bilgilerini çalması.

Q10: Ele geçirilme göstergeleri (IOC) nelerdir?

IOC'ler, bir sistemin ihlal edildiğini gösteren olağandışı kayıt defteri değişiklikleri veya yetkisiz IP trafiği gibi adli veri ipuçlarıdır.

Bölüm 11: Siber güvenlikle ilgili 10 gerçek dünya gerçeği ve içgörüsü

Güvenlik ihlalleri, savunma mekanizmaları ve uyumluluk standartlarıyla ilgili gerçek dünya bilgilerini incele.

1. GÜVENLİK İPUCU

Saldırganlar, savunmasız sunucular için interneti sürekli tarar ve çalışanların gelen kutularına kimlik avı e-postaları gönderir.

2. GÜVENLİK İPUCU

Kimlik avı bağlantılarına tıklamak gibi insan hatası, veri ihlallerinde yaygın bir etkendir; eğitimin önemi bu yüzdendir.

3. GÜVENLİK İPUCU

Veri ihlali maliyetleri arasında yasal cezalar, müşteri kaybı, inceleme ve onarım yer alır ve milyonlarca dolara ulaşabilir.

4. GÜVENLİK İPUCU

Kimlik avına dayanıklı MFA, örneğin donanım güvenlik anahtarları, en güçlü MFA türüdür ve CISA'nın ısrarla önerdiği standarttır. [2]

5. GÜVENLİK İPUCU

Fidye yazılımı kurumsal ağlar için büyük bir tehdit olmaya devam ediyor ve CISA, temel bir savunma olarak çevrimdışı, şifrelenmiş yedekleri öneriyor. [4]

6. GÜVENLİK İPUCU

NIST Siber Güvenlik Çerçevesi 2.0'ın (2024) altı temel işlevi vardır: Yönet, Belirle, Koru, Algıla, Müdahale Et, Kurtar. [1]

7. GÜVENLİK İÇGÖRÜSÜ

Kimlik bilgisi doldurma botları, sızdırılmış kullanıcı adı ve parola çiftlerini bankacılık ve e-ticaret giriş portallarında büyük ölçekte dener.

8. GÜVENLİK İÇGÖRÜSÜ

Dünya genelinde sıfırıncı gün istismarı pazarları vardır; burada yüksek önem derecesine sahip güvenlik açıkları yama yapılmadan önce yüksek meblağlara satılabilir.

9. GÜVENLİK İÇGÖRÜSÜ

Bir honeypot tuzak sistemi, meşru kullanıcıların ona erişmek için bir nedeni olmadığından izinsiz giriş uyarılarını hemen bildirir.

10. GÜVENLİK İPUCU

Aktarım Katmanı Güvenliği (TLS), tarayıcı oturumlarını şifreler ve herkese açık Wi-Fi ağlarında paket dinlemeyi önler.

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Kimlik avı saldırıları** KİMLİK AVI — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kimlik avı kampanyaları, sahte e-postalar kullanarak kimlik bilgilerini ve hassas kullanıcı verilerini çalmaya çalışır. Kaynak: OWASP Secure Configuration.

2 **Hesap Koruması** MFA ANAHTARI — **Doğru cevap: A**

ÖĞRETMEN NOTU

Donanım belirteçleri kullanan çok faktörlü kimlik doğrulama (MFA), en güçlü hesap erişim savunmasını sağlar. Kaynak: NIST Dijital Kimlik.

3 **Fidye yazılımı tehdidi** FİDYE YAZILIMI — **Doğru cevap: A**

ÖĞRETMEN NOTU

Fidye yazılımı kritik sistemleri ve verileri şifreler ve şifre çözme anahtarları için kripto para ödemesi talep eder. Kaynak: Center for Internet Security (CIS).

4 **Sıfırıncı Gün Güvenlik Açığı** SIFIRINCI GÜN — **Doğru cevap: A**

ÖĞRETMEN NOTU

Sıfırıncı gün tehditleri, bir satıcı yaması yayımlanmadan önce yamalanmamış, bilinmeyen güvenlik kusurlarını istismar eder. Kaynak: OWASP Secure Configuration.

5 **Güvenlik Çerçeveleri** ÇERÇEVELER — **Doğru cevap: A**

ÖĞRETMEN NOTU

NIST gibi çerçeveler, kuruluşların siber riskleri yönetmesine ve azaltmasına yardımcı olan yapılandırılmış yönergeler sunar. Kaynak: NIST Digital Identity.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Hedefli Kimlik Avı** KİMLİK AVI — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Kimlik avı saldırıları, istismar vektörlerini genişletmek için hem kurumsal ağları hem kişisel hesapları hedef alır. Kaynak: OWASP Secure Configuration.

7 **Soru 7** — Doğru cevap: Doğru

ÖĞRETMEN NOTU

MFA ikinci bir faktör gerektirir, bu yüzden çalınmış bir parola tek başına genellikle oturum açmak için yeterli değildir.

8 **Trafik Güvenlik Duvarı** GÜVENLİK DUVARI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Güvenlik duvarları, yetkisiz bağlantıları ayıklamak için belirli ağ bağlantı noktalarındaki trafiği inceler ve engeller. Kaynak: Center for Internet Security (CIS).

9 **Sıfırıncı Gün Müdahalesi** SIFIRINCI GÜN — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Sıfırıncı gün açıklarını gidermek, henüz imzaları bulunmadığı için kod yamaları ve WAF filtrelemesi gerektirir. Kaynak: OWASP Secure Configuration.

10 **Tuzak Sistemler (Honeypot)** BAL KÜPÜ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Bal küpleri (honeypot), güvenlik ekiplerinin kötü niyetli kişileri çekmek, uyarı almak ve incelemek için kullandığı aldatıcı sunucudardır. Kaynak: Center for Internet Security (CIS).

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

D 1. Fidye Yazılımı Tehdidi	G 2. Çok Faktörlü Kimlik Doğrulama	E 3. Sıfırıncı Gün Açığı İstismarı	H 4. Tuzak Bal Küpü
C 5. Saldırı Güvenlik Duvarı	B 6. Olay Müdahalesi	F 7. Parola Hijyeni	A 8. Güvenlik Çerçevesi

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 GÜVENLİK DUVARI	2 SIFIR GÜN AÇIĞI	3 KİMLİK AVI	4 KÖTÜ AMAÇLI YAZILIM
5 HİJYEN	6 ŞİFRELEME		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 E – GÜVENLİKDUVARI	2 F – MÜDAHALE	3 A – FİDYEYAZILIMI	4 B – ÇOKFAKTÖRLÜ
5 G – HİJYEN	6 H – ÇERÇEVE	7 C – SIFIRGÜNAÇIĞI	8 D – BALKÜPÜ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin Fidye Yazılımı Tehdidi, Çok Faktörlü Kimlik Doğrulama ve Sıfırıncı Gün Açığı İstismarı terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

I	T	İ	P	B	Ü	Z	V	K	P	Ö	V	H	N	D
M	Ü	L	R	Ö	T	K	A	F	K	O	Ç	A	H	Ç
I	Ç	İ	Ö	U	Ü	Ü	J	I	Ğ	Ş	Ğ	İ	E	F
L	B	E	H	M	İ	S	R	U	P	Z	J	R	E	Ğ
I	E	R	C	Ü	A	J	O	C	Z	Y	Ç	K	İ	U
Z	P	Ş	A	D	R	Ü	I	K	E	E	K	G	Ğ	L
A	Ğ	P	F	A	J	S	J	N	V	P	Ü	Ğ	B	Ş
Y	F	Y	M	H	Y	Ü	R	E	Ğ	S	V	A	O	T
E	M	M	Z	A	N	H	O	S	Ğ	O	T	Ş	N	Ş
Y	Ş	İ	A	L	E	N	L	B	A	L	K	Ü	P	Ü
D	G	Ü	V	E	N	L	İ	K	D	U	V	A	R	I
İ	J	B	M	T	F	G	O	Ö	Ü	Y	I	İ	T	I
F	Y	S	I	F	I	R	G	Ü	N	A	Ç	I	Ğ	I
U	V	O	İ	H	Z	H	I	L	A	E	H	B	S	A
I	E	U	E	İ	Z	İ	D	J	Ö	L	I	A	F	N

BULMACA ÇÖZÜMÜ

			F									S		
			İ									I		
			D			Ç						F		
	M		Y			O						I		
G	Ü	V	E	N	L	İ	K	D	U	V	A	R	I	
	D		Y			F						G		H
	A		A		B	A	L	K	Ü	P	Ü			İ
	H		Z			K						N		J
	A		I			T						A		Y
	L		L			Ö		Ç	E	R	Ç	E	V	E
	E		I			R						I		N
			M			L						Ğ		
			I			Ü						I		

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

5 soldan sağa: GÜVENLİKDUVARI Trafiği güvenlik kurallarına göre filtreleyen ağ bariyeri (14 harf)

7 soldan sağa: BALKÜPÜ Kötü niyetli kişileri çekip analiz etmek için kurulan yem sistem (7 harf)

8 soldan sağa: ÇERÇEVE Siber riskleri yönetmek için kullanılan NIST gibi yapılandırılmış yönergeler (7 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: FİDYEYAZILIMI Verileri şifreleyip şifre çözme karşılığında ödeme talep eden kötü amaçlı yazılım (13 harf)

2 yukarıdan aşağı: SIFIRGÜNAÇIĞI Satıcı yama yayımlamadan önce hedeflenen güvenlik açığı istismarı (13 harf)

3 yukarıdan aşağı: ÇOKFAKTÖRLÜ İki veya daha fazla kimlik doğrulama faktörü gerektiren güvenlik doğrulaması (11 harf)

4 yukarıdan aşağı: MÜDAHALE Güvenlik ihlallerini ele almak ve azaltmak için yapılandırılmış plan (8 harf)

6 yukarıdan aşağı: HİJYEN Kimlik bilgilerini ve kimlik doğrulama anahtarlarını yönetmeye yönelik en iyi uygulamalar (6 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	ADIMYİZLFIIEY	FİDYEYAZILIMI	5.	ROÖTKÜAKÇLF	ÇOKFAKTÖRLÜ
2.	ĞRIGFSIÜIAÇNI	SIFIRGÜNAÇIĞI	6.	PLÜBKÜA	BALKÜPÜ
3.	GDÜRKIUVVİNLAE	GÜVENLİKDUVARI	7.	MEHALÜAD	MÜDAHALE
4.	NYJEHİ	HİJYEN	8.	EÇEÇVER	ÇERÇEVE

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SİSTEMİNİ ÇOK FAKTÖRLÜ DOĞRULAMAYLA KORU"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Fidye Yazılımı Kurtarma Stratejisi

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kurumsal ağ fidye yazılımıyla enfekte olur ve kritik veritabanları kilitlenir. Saldırganlar $100,000 kripto para ödemesi talep eder. Şirketin 24 saat öncesine ait çevrimdışı yedekleri vardır.
- Önerilen Strateji ve Çözüm: Ödemenin Riskleri: Ödeme yapmak dosyaların şifresinin çözüleceğini garanti etmez, şirketi ödeme yapan bir hedef olarak etiketler ve suç faaliyetlerini finanse eder. Kurtarma Stratejisi: Ekip, enfekte olmuş ana makineleri izole etmeli, ele geçirilmiş sunucuları silmeli ve verileri çevrimdışı yedeklerden geri yüklemelidir. Anında yeniden enfeksiyonu önlemek için ilk erişim vektörünü (kimlik avı veya istismar) yamalamalıdırlar.

B Vaka Çalışması 2: Kimlik Bilgisi Doldurma Savunmaları

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir çevrimiçi hizmet, bilgisayar korsanlarının başka sitelerden çalınan milyonlarca kullanıcı adı/parola çiftini denediği bir kimlik bilgisi doldurma saldırısı yaşıyor.
- Önerilen Strateji ve Çözüm: Mekanizma: Saldırganlar, kullanıcı hesaplarına giriş yapmak için otomatik botlarla siteler arasında parola tekrar kullanımından yararlanır. Savunmalar: 1. Çok faktörlü kimlik doğrulama (MFA), parola doğru olsa bile giriş denemelerini engeller. 2. Hız sınırlaması ve CAPTCHA uygulamak, oturum açma uç noktalarını dolduran otomatik bot trafiğini engeller.