Ad Soyad: _____ Tarih: _____ Puan: _____

Fidye yazılımı saldırıları ve iş Kurtarma

Yük çalıştırma, kriptografik dosya şifreleme, çevrimdışı yedekler, sınırlandırma prosedürleri ve felaket kurtarma.

FİDYE YAZILIMI SALDIRILARI ÖĞRENME ÖZETİ

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 fidye yazılımı saldırıları ve işletmenin toparlanması konusunda rehberlik eder. Yük çalıştırmayı, dosya şifrelemeyi, çevrimdışı yedekleri, tehdit sınırlamayı, kripto para ödemelerini ve felaket kurtarma planlarını 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/fidye-yazilimi-saldirisi/

Fidye Yazılımı Kurtarma Öğrenme Yol Haritan

- Truva atı, fidye yazılımı ve casus yazılım yüklerini birbirinden ayır.
- Kötü amaçlı dosyaları güvenli korumalı alan ortamlarında analiz et.
- Hızlı ağ yalıtımı ve sınırlama prosedürleri oluştur.

FİDYE YAZILIMI SALDIRILARI 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: fidye yazılımından kurtarma. Hızlı Düşün bonus etkinliğiyle bitir.

FİDYE YAZILIMI SALDIRILARI VE FELAKET KURTARMA (GİRİŞ)

Fidye yazılımı yükleri sistem depolamasını kriptografik olarak kilitler ve şifre çözme anahtarları için kripto para ödemesi talep eder. Bu tehdidi azaltmak ağ yalıtım kurallarını, korumalı alanda kötü amaçlı yazılım analizini ve sağlam, hava boşluklu soğuk yedekleri gerektirir.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. Fidye yazılımı saldırısının temel mekanizması nedir?

- A. Sistem erişimini engellemek için kullanıcı dosyalarının kriptografik şifrelenmesi
- B. Form alanlarına kötü amaçlı SQL komutları enjekte etmek
- C. Herkese açık bir Wi-Fi bağlantısında ağ paketlerini dinlemek
- D. SPF doğrulamasını aşmak için e-posta başlıklarını taklit etmek

2. Çevrim dışı (soğuk) yedek nedir?

- A. Kötü amaçlı yazılımın yayılmasından korumak için ağdan bağlantısı kesilmiş depolama kopyası
- B. Ana web sunucusunun sabit diskinde saklanan yedek
- C. Sistem kayıt defteri kayıtlarının geçici önbelleği
- D. Kullanıcı parolalarını sıfırlamak için kullanılan bir yönetim aracı

3. Güvenlik ekipleri bir fidye yazılımı saldırısı sırasında enfekte sistemleri nasıl yalıtmalıdır?

- A. Ağ kablolarını çıkarmak ve kablosuz arayüzleri hemen devre dışı bırakmak
- B. Antivirüs imza veritabanını yükseltmek
- C. Birincil DNS sunucusunu kapat
- D. Ele geçirilen dosya uzantılarını yeniden adlandır

4. Güvenlik kurumları neden fidye yazılımı taleplerini ödememeyi önerir?

- A. Ödeme yapmak saldırganları cesaretlendirir ve şifre çözme anahtarının teslim edileceğini garanti etmez
- B. Tüm kurumsal sigorta poliçelerini otomatik olarak geçersiz kılar
- C. Her müşteriyi otomatik olarak e-postayla bilgilendirir
- D. Kalan sistem yedek dosyalarını bozar

5. Felaket kurtarma planı (DRP) nedir?

- A. Sistem ele geçirildikten sonra işleyişi ve verileri geri yüklemeye yönelik yapılandırılmış süreç
- B. Gelen ağ portlarını eşleyen bir güvenlik duvarı yapılandırması
- C. Kullanıcı yönetici ayrıcalıklarını listeleyen bir veritabanı şeması
- D. Sahte alan adlarını reddeden bir e-posta kimlik doğrulama protokolü

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Fidye yazılımı yükleri, ağa bağlı çevrimiçi yedeklere kolayca yayılabilir.

- ( ) Doğru
- ( ) Yanlış

7 Soru 7

7. Kripto para fidyesini ödemek, dosyaların başarıyla çözüleceğini garanti eder.

- ( ) Doğru
- ( ) Yanlış

8 Soru 8

8. Enfekte sistemleri ağdan ayırmak, fidye yazılımının bitişik sistemlere yayılmasını durdurmaya yardımcı olur.

- ( ) Doğru
- ( ) Yanlış

9 Soru 9

9. Simetrik kriptografi, fidye yazılımları tarafından sistem depolamasını şifrelemek için asla kullanılmaz.

- ( ) Doğru
- ( ) Yanlış

10 Soru 10

10. Veri geri yükleme prosedürlerini düzenli olarak test etmek, felaket kurtarmanın kritik bir parçasıdır.

- ( ) Doğru
- ( ) Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Yerel dosyalara erişimi engellemek kriptografik _____ kullanır.
2. Bir sistemde yürütülen etkin kötü amaçlı kod, _____ olarak adlandırılır.
3. Bağlantısı kesilmiş, sahadışı depolama kopyaları güvenli bir _____ oluşturur.
4. Kötü amaçlı yazılımın yayılmasını durdurmak, uç nokta ağ _____ gerektirir.
5. Siber suçluların talep ettiği kripto para ödemesi _____ olarak adlandırılır.
6. Operasyonel veri dosyalarını geri yüklemek, felaket sonrası _____ anlamına gelir.

KELİME BANKASI

FELAKET FİDYE İZOLASYON KURTARMA SOĞUK YEDEK ŞİFRELEME TROJAN ZARARLI YÜK

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

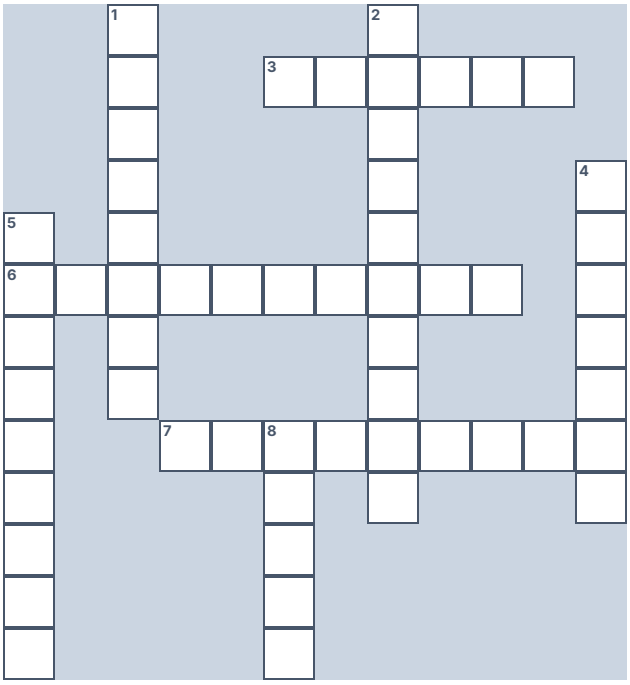
TANIM EŞLEŞTİRME

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

☐	1. ŞİFRELEME	A	Enfekte ağ sistemlerinin bağlantısını kesme.
☐	2. VERİ YÜKÜ	B	Temiz gibi görünen kötü amaçlı dosya.
☐	3. SOĞUK YEDEK	C	Dosyaları kriptografik olarak kilitlemek.
☐	4. YALITIM	D	Büyük sistem kesintisi olayı.
☐	5. FİDYE	E	Kötü amaçlı yazılımı çalıştırma.
☐	6. KURTARMA	F	Bağlantısı kesilmiş çevrimdışı kopya.
☐	7. FELAKET	G	Veritabanını yedekten geri yükleme.
☐	8. TROYA ATI	H	Şifreleme anahtarı ödeme talebi.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

3. Temiz görünen kötü amaçlı dosya. (6)

6. Kötü amaçlı yazılımı çalıştırma. (10)

7. Dosyaları kriptografik olarak kilitleme. (9)

YUKARIDAN AŞAĞI

1. Veritabanını yedekten geri yükleme. (8)

2. Bağlantısı kesilmiş çevrimdışı kopya. (10)

4. Büyük sistem aksaklığı olayı. (7)

5. Enfekte ağ sistemlerinin bağlantısını kesme. (9)

8. Kriptografik anahtar için ödeme talebi. (5)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

3 soldan sağa: Temiz görünen kötü amaçlı dosya. (6 harf):

6 soldan sağa: Kötü amaçlı yazılımı çalıştırma. (10 harf):

7 soldan sağa: Dosyaları kriptografik olarak kilitleme. (9 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Veritabanını yedekten geri yükleme. (8 harf):

2 yukarıdan aşağı: Bağlantısı kesilmiş çevrimdışı kopya. (10 harf):

4 yukarıdan aşağı: Büyük sistem aksaklığı olayı. (7 harf):

5 yukarıdan aşağı: Enfekte ağ sistemlerinin bağlantısını kesme. (9 harf):

8 yukarıdan aşağı: Kriptografik anahtar için ödeme talebi. (5 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

ŞİFRELEME ZARARLIYÜK SOĞUKYEDEK İZOLASYON FİDYE KURTARMA FELAKET TROJAN

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. ŞİFRELEME**
- **B. ZARARLIYÜK**
- **C. SOĞUKYEDEK**
- **D. İZOLASYON**
- **E. FİDYE**
- **F. KURTARMA**
- **G. FELAKET**
- **H. TROJAN**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Bağlantısı kesilmiş çevrimdışı kopya.
2. Temiz görünen kötü amaçlı dosya.
3. Dosyaları kriptografik olarak kilitleme.
4. Kriptografik anahtar için ödeme talebi.
5. Enfekte ağ sistemlerinin bağlantısını kesme.
6. Büyük sistem aksaklığı olayı.
7. Kötü amaçlı yazılımı çalıştırma.
8. Veritabanını yedekten geri yükleme.

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. **LERİŞEMEF** _____
2. **EUSOKKEDYĞ** _____
3. **DFEYİ** _____
4. **TEKAEFL** _____
5. **YLKAAIRZÜR** _____
6. **OLZYSİANO** _____
7. **KAARMUTR** _____
8. **ONTAJR** _____

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Asla paylaşmaman gereken bilgiler			
2	Hacklenebilecek cihazlar			
3	Fidyeyi ödememe nedenleri			
4	Bugün başlayabileceğin güvenli alışkanlıklar			
5	Bildiğin güvenlik araçları			
6	Hesaplarını koruma yolları			
7	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
8	Yedek tutulacak yerler			
9	Asla kaybetmek istemediğin dosyalar			
10	Fidye yazılımının yayılma yolları			
11	Saldırının ilk saatinde yapılacaklar			
12	Saldırı sırasında iletişime geçilecek kişiler			
13	Fidye yazılımının kilitleyebileceği şeyler			
14	Siber güvenlikle ilgili sözcükler			
15	Sık hedef alınan kuruluşlar			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KURUMSAL FİDYE YAZILIMI YÜKÜNÜ KONTROL ALTINA ALMA

👷

Senaryo: Kurumsal bir yerel alan ağı, aktif bir fidye yazılımı tarafından ele geçirildi. Önemli dosya sunucuları .locked uzantılı dosyalar göstermeye başladı.

Tartışma sorusu: Sınırlandırma adımlarını ayrıntılı anlat ve veri kurtarma protokolünü özetle.

VAKA ÇALIŞMASI 2: ÇEVRİMDIŞI YEDEKLEME MİMARİLERİNİ DEĞERLENDİRME

👷

Senaryo: Bir kuruluş, birincil yerel ağın tamamen fidye yazılımı tarafından ele geçirilmesi durumunda bile yedeklerin tehlikeye girme riskini azaltan bir veri yedekleme stratejisi tasarlamak istiyor.

Tartışma sorusu: Güvenli bir çevrimdışı yedek depolama kasası sistemi tasarla.

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

23	12	7	21	6	15	12		22	12	22	24	6	16	12		22	18	9	25	14
28	6	5	6	14	24	6	17		8	6	21	12		28	26	14	15	6		

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: Fidye yazılımı nedir?

Fidye yazılımı, bir fidye tutarı ödenene kadar bilgisayar sistemlerine veya dosyalara erişimi engellemek için tasarlanmış kötü amaçlı yazılımdır.

Q2: Fidye yazılımı nasıl yayılır?

E-posta kimlik avı ekleri, yamalanmamış yazılım açıkları ve ele geçirilmiş uzaktan erişim sistemleri aracılığıyla. [1]

Q3: Ödeme neden kripto parayla isteniyor?

Bitcoin gibi kripto para birimleri göreli anonimlik sunar ve kolluk kuvvetlerinin fonları izlemesini zorlaştırır.

Q4: Antivirüs fidye yazılımını engeller mi?

Evet, ancak imza tabanlı antivirüs, yeni oluşturulmuş sıfırıncı gün fidye yazılımı yüklerine karşı başarısız olabilir.

Q5: Hava boşluklu (air-gapped) yedek nedir?

Yayılmasını önlemek için birincil ağla fiziksel veya mantıksal bağlantısı olmayan yedek kopya.

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

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Çifte şantaj (double extortion) nedir?

Saldırganların yalnızca dosyaları şifrelemekle kalmayıp ödeme yapılmazsa herkese açık sızıntıyla tehdit etmek için hassas verileri de çalması.

Q7: Şifre çözücü (decryptor) nedir?

Kilitli dosyaları düz metne geri döndürmek için gereken kriptografik anahtarı içeren yazılım aracı.

Q8: Fidye yazılımını erken nasıl tespit edersin?

Dosya sistemlerini ani, kitlesel dosya değişikliği ve yeniden adlandırma etkinliği için izleyerek.

Q9: Sigortanın rolü nedir?

Siber sigorta, kurtarma maliyetlerini karşılamaya yardımcı olabilir; ancak teminat koşulları ve fidye ödeme kuralları poliçeye göre değişir.

Q10: Enfekte olmuş bir sistemi yeniden başlatmalı mıyım?

Hayır, yeniden başlatma geçici bellekteki kanıtları yok edebilir; bunun yerine cihazı ağdan yalıt. [1]

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: Fidye yazılımı asimetrik şifrelemeyi nasıl kullanır?

Dosyaları şifrelemek için kötü amaçlı yazılımın içine gömülü bir genel anahtar kullanır; şifreyi çözmek için saldırganın özel anahtarı gerekir.

Q2: Simetrik şifreleme neden de kullanılır?

Simetrik şifreleme (AES gibi) hızlıdır ve çok büyük veritabanlarını dakikalar içinde kilitleyebilir; asimetrik anahtarlar ise AES anahtarını güvenceye alır.

Q3: Mantıksal bölümleme nedir?

Ağları yalıtılmış bölgelere ayırmak, kötü amaçlı yazılımın iş istasyonu düğümlerinden çekirdek sunuculara yanal olarak yayılmasını önler.

Q4: WORM depolama nedir?

Bir kez yaz, çok kez oku (Write-Once, Read-Many) ortamı; yedek verilerin fidye yazılımı yükleri tarafından düzenlenmesini, üzerine yazılmasını veya silinmesini önler.

Q5: Gölge kopyalar nedir?

Windows tarafından oluşturulan yerel yedek anlık görüntüleri; fidye yazılımı genellikle önce bunları yönetici araçlarıyla siler.

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: Kimlik bilgisi hırsızlığı fidye yazılımını nasıl mümkün kılar?

Saldırganlar, uzak masaüstleri üzerinden oturum açmak için sızdırılmış yönetici girişlerini satın alır ve fidye yazılımını ağ genelinde elle çalıştırır.

Q7: Kuru çalıştırma geri yükleme testi nedir?

Geri yükleme hızının ve veri bütünlüğünün felaket ölçütlerini karşıladığını doğrulamak için yedek veritabanlarını düzenli olarak yalıtılmış test ortamlarına geri yüklemek.

Q8: Uç nokta tespiti (EDR) fidye yazılımını nasıl durdurur?

İşlem davranışını (örneğin hızlı şifreleme) analiz ederek ve sahte uygulamayı hızla askıya alarak.

Q9: Hizmet olarak fidye yazılımı (RaaS) modeli nedir?

Kötü amaçlı yazılım geliştiricilerinin fidye yazılımı oluşturucularını, ödemelerden pay karşılığında iştiraklere kiraladığı bayilik modeli.

Q10: Yamasız RDP fidye yazılımını nasıl tetikler?

Açıkta kalmış, yamalanmamış Uzaktan Masaüstü Protokolü ağ geçitleri, saldırganların oturum açma bilgilerini kaba kuvvetle denemesine ve kötü amaçlı yazılımı elle başlatmasına olanak tanır.

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

Fidye yazılımı aktörleri, Windows gölge kopyalarını silmek ve yerel geri yüklemeleri engellemek için sıklıkla vssadmin.exe gibi araçları kullanır. [1]

2. GÜVENLİK İPUCU

Simetrik AES-256 anahtarları genellikle dosya yüklerini şifrelemek için kullanılır; bunlar daha sonra açık RSA anahtarlarıyla kilitlenir.

3. GÜVENLİK İPUCU

Başarılı bir fidye yazılımı saldırısından kurtulmak haftalar sürebilir; bu yüzden test edilmiş çevrimdışı yedekler önemlidir.

4. GÜVENLİK İPUCU

FBI, fidye ödenmesini desteklemez ve ödeme yapmanın verilerinin geri geleceğini garanti etmediği konusunda uyarır. [2]

5. GÜVENLİK İPUCU

Felaket kurtarma planları (DRP), bir Kurtarma Süresi Hedefi (RTO) ve bir Kurtarma Noktası Hedefi (RPO) tanımlamalıdır.

6. GÜVENLİK İPUCU

FBI, şifrelenmiş ve değiştirilemez, yani değiştirilemeyen veya silinemeyen yedekler önerir. [3]

7. GÜVENLİK İÇGÖRÜSÜ

Fidye yazılımı geliştiricileri, geleneksel imza tabanlı antivirüs tarayıcılarını atlatmak için gelişmiş gizleme tekniklerinden yararlanır.

8. GÜVENLİK İÇGÖRÜSÜ

Ağ bölümleme yanal hareketi kısıtlar ve fidye yazılımının ilk bulaşan ana bilgisayarın ötesine yayılmasını durdurmaya yardımcı olur. [3]

9. GÜVENLİK İÇGÖRÜSÜ

Uzaktan Masaüstü Protokolü (RDP) gibi açıkta kalmış, zayıf korunan uzak hizmetler yaygın bir fidye yazılımı giriş noktasıdır. [1]

10. GÜVENLİK İPUCU

CISA, birçok fidye yazılımı çeşidinin erişilebilir yedekleri aradığı ve sildiği için şifrelenmiş yedeklerin çevrimdışı tutulmasını önerir. [1]

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

[5] 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

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 Soru 1 — Doğru cevap: A

ÖĞRETMEN NOTU

Fidye yazılımı saldırısının temel mekanizması nedir? → Sistem erişimini engellemek için kullanıcı dosyalarının kriptografik şifrelenmesi

2 Soru 2 — Doğru cevap: A

ÖĞRETMEN NOTU

Çevrim dışı (soğuk) yedek nedir? → Kötü amaçlı yazılımın yayılmasından korumak için ağdan bağlantısı kesilmiş depolama kopyası

3 Soru 3 — Doğru cevap: A

ÖĞRETMEN NOTU

Güvenlik ekipleri bir fidye yazılımı saldırısı sırasında enfekte sistemleri nasıl yalıtmalıdır? → Ağ kablolarını çıkarmak ve kablosuz arayüzleri hemen devre dışı bırakmak

4 Soru 4 — Doğru cevap: A

ÖĞRETMEN NOTU

Güvenlik kurumları neden fidye yazılımı taleplerini ödememeyi önerir? → Ödeme yapmak saldırganları cesaretlendirir ve şifre çözme anahtarının teslim edileceğini garanti etmez

5 Soru 5 — Doğru cevap: A

ÖĞRETMEN NOTU

Felaket kurtarma planı (DRP) nedir? → Sistem ele geçirildikten sonra işleyişi ve verileri geri yüklemeye yönelik yapılandırılmış süreç

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Fidye yazılımı yükleri, ağa bağlı çevrimiçi yedeklere kolayca yayılabilir.

7 **Soru 7** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: FBI, ödeme yapmanın verilerinin herhangi bir kısmını geri alacağın anlamına gelmediği konusunda uyarıyor.

8 **Soru 8** — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Doğru: CISA, yayılmayı sınırlamak için enfekte ana bilgisayarların fişinin çekilmesini veya ağın çevrimdışına alınmasını öneriyor.

9 **Soru 9** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: fidye yazılımı genellikle dosyaları AES gibi hızlı simetrik şifrelerle şifreler.

10 **Soru 10** — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Veri geri yükleme prosedürlerini düzenli olarak test etmek, felaket kurtarmanın kritik bir parçasıdır.

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

C 1. ŞİFRELEME	E 2. VERİ YÜKÜ	F 3. SOĞUK YEDEK	A 4. YALITIM
H 5. FİDYE	G 6. KURTARMA	D 7. FELAKET	B 8. TROYA ATI

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 ŞİFRELEME	2 ZARARLI YÜK	3 SOĞUK YEDEK	4 İZOLASYON
5 FİDYE	6 KURTARMA		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 C – SOĞUKYEDEK	2 H – TROJAN	3 A – ŞİFRELEME	4 E – FİDYE
5 D – İZOLASYON	6 G – FELAKET	7 B – ZARARLIYÜK	8 F – KURTARMA

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin ŞİFRELEME, VERİ YÜKÜ ve SOĞUK YEDEK terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

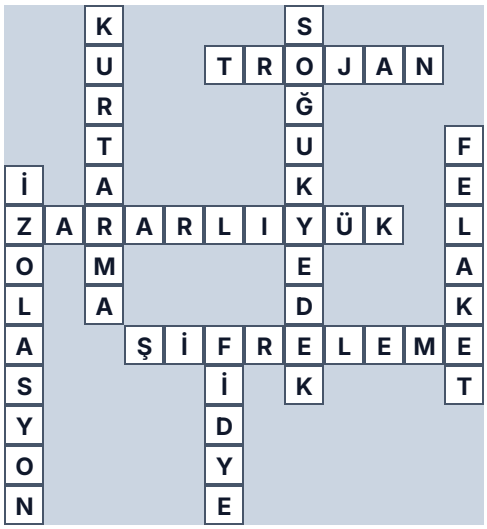
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

3 soldan sağa: TROJAN Temiz görünen kötü amaçlı dosya. (6 harf)

6 soldan sağa: ZARARLIYÜK Kötü amaçlı yazılımı çalıştırma. (10 harf)

7 soldan sağa: ŞİFRELEME Dosyaları kriptografik olarak kilitleme. (9 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: KURTARMA Veritabanını yedekten geri yükleme. (8 harf)

2 yukarıdan aşağı: SOĞUKYEDEK Bağlantısı kesilmiş çevrimdışı kopya. (10 harf)

4 yukarıdan aşağı: FELAKET Büyük sistem aksaklığı olayı. (7 harf)

5 yukarıdan aşağı: İZOLASYON Enfekte ağ sistemlerinin bağlantısını kesme. (9 harf)

8 yukarıdan aşağı: FİDYE Kriptografik anahtar için ödeme talebi. (5 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. LERİŞEMEF	ŞİFRELEME	5. YLKAAIRZÜR	ZARARLIYÜK
2. EUSOKKEDYĞ	SOĞUKYEDEK	6. OLZYSİANO	İZOLASYON
3. DFEYİ	FİDYE	7. KAARMUTR	KURTARMA
4. TEKAEFL	FELAKET	8. ONTAJR	TROJAN

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"ŞİFRELİ SİSTEMİ SOĞUK YEDEKTEN GERİ YÜKLE"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Kurumsal Fidye Yazılımı Yükünü Kontrol Altına Alma

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kurumsal yerel ağ, etkin fidye yazılımı tarafından ihlal edildi. Kilit dosya sunucuları .locked uzantılı dosyalar göstermeye başladı.
- Önerilen strateji ve çözüm: Etkilenen tüm sunucuların yerel ağ bağlantısını kes. Etkin yönetici oturumlarını sonlandır. Etkilenmemiş dosyaları, yazmaya karşı kilitli, güvenli bir çevrimdışı yedekleme sisteminden geri yükle.

B Vaka Çalışması 2: Çevrimdışı Yedekleme Mimarilerini Değerlendirme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kuruluş, birincil yerel ağ fidye yazılımı tarafından tamamen ele geçirilse bile yedeklerin ele geçirilme riskini azaltan bir veri yedekleme stratejisi tasarlamak istiyor.
- Önerilen Strateji ve Çözüm: Bir kez yaz, çok kez oku (WORM) depolama uygula. Yedekleme sistemini tüm ağlardan ayırarak mantıksal bir hava boşluğu oluştur ve günlük fiziksel ortam rotasyonunu zorunlu kıl.