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

Veri Koruma ve Kurumsal Depolama Güvenlik Rehberi

Veri maskeleme, tokenleştirme, durağan ve aktarım halindeki veri şifreleme, çevrimdışı yedekler

VERİ KORUMA 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 veri koruma standartları ve denetimleri konusunda rehberlik eder. Tam disk şifrelemesini, güvenli erişim denetimlerini, donanım yedeklerini, bulut güvenlik duruşunu ve veri maskeleme tekniklerini 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/veri-koruma/

Veri Koruma Stratejisi Öğrenme Yol Haritan

- Veri maskeleme ile tokenleştirme tekniklerini birbirinden ayır.
- Depolama sürücüleri için bekleme sırasında şifreleme, aktarım sırasında ise TLS ile şifreleme uygula.
- Fidye yazılımı koruması için çevrimdışı, ağdan yalıtılmış yedekleme sistemleri tasarla.

VERİ KORUMA 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: veri koruması. Hızlı Düşün bonus etkinliğiyle bitir.

VERİ KORUMA VE KURUMSAL DEPOLAMA GÜVENLİĞİ (GİRİŞ)

Veri koruma, kurumsal veri varlıklarını maskeleme, tokenleştirme, durağan veri tabanı şifreleme ve güvenli aktarım protokolleriyle korur. Ağdan yalıtılmış yedekler tasarlamak, aktif bir saldırı durumunda temel veri tabanlarının geri yüklenebilmesine yardımcı olur.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. Veri maskelemenin temel amacı nedir?

- A. Gizliliği korumak için hassas tanımlayıcıları kurgusal ancak gerçekçi karakterlerle değiştirmek
- B. Fiziksel sunucu depolama alanından tasarruf etmek için büyük veritabanı dosyalarını sıkıştırmak
- C. Eski müşteri iletişim e-postalarını arşiv yedekleme sistemlerinden silmek
- D. Veritabanı sunucusunun genel IP adresini internet taramalarından gizlemek

2. Hangi mekanizma bir veri tabanı sunucusunun sabit diskinde saklanan dosyaları şifreler?

- A. Bekleme durumunda tam disk şifrelemesi
- B. Aktarım sırasında TLS oturum el sıkışma protokolleri
- C. Dinamik DNS ad sunucusu yönlendirme kuralları
- D. Donanım anahtarlarıyla çok faktörlü kimlik doğrulama

3. Aktarım halindeki veriyi ne temsil eder?

- A. Ağ yönlendiricileri ve anahtarları arasında hareket eden veri paketleri
- B. Soğuk yedek sürücüde saklanan veritabanı işlem kayıtları
- C. Yalıtılmış bir bulut kasasında saklanan arşivlenmiş kullanıcı dosyaları
- D. Yerel masaüstü depolamadaki statik sistem yapılandırma dosyaları

4. Düzenli bir çevrim dışı yedek, fidye yazılımına karşı korunmak için neden kritiktir?

- A. Fidye ödemeden dosyaları geri yüklemek için temiz, çevrimdışı bir kopya sağlar
- B. Bilgisayar korsanlarının açık port yapılandırmalarını taramasını engeller
- C. Yerel ağ iletim bant genişliği hızlarını artırır
- D. Tarayıcılarda çerez onayı kabul kayıtlarını otomatikleştirir

5. Veri belirteçleme (tokenization) ne yapar?

- A. Hassas kart numaralarını hassas olmayan rastgele belirteçlerle değiştirir
- B. Web trafiğini birden çok güvenli onion düğümü üzerinden yönlendirir
- C. Sistem dizinlerini imza tabanlı kötü amaçlı yazılımlar için tarar
- D. Veritabanı yöneticisi oturum açma sürelerini denetler

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Veri maskeleme, üretim ortamlarındaki veri tabanı kayıtlarını kalıcı olarak değiştirir.

○ Doğru ○ Yanlış

7 Soru 7

7. Fidye yazılımının yayılmasını önlemek için yedeklemeler ana kurumsal ağdan yalıtılmış olmalıdır.

○ Doğru ○ Yanlış

8 Soru 8

8. SSL/TLS sertifikaları, fiziksel ortamda bekleyen verileri şifreleyerek veritabanlarını güvenceye alır.

○ Doğru ○ Yanlış

9 Soru 9

9. Sıfır Güvenli ağ erişimi (ZTNA), veri tabanı erişimi vermeden önce her kullanıcının kimliğini doğrular.

○ Doğru ○ Yanlış

10 Soru 10

10. Kasa tabanlı belirteçleme (tokenization), orijinal kart değerlerini güvenli, merkezî bir belirteç kasasında saklar.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Kişisel adları gerçekçi yer tutucularla değiştirmeye veri _____ denir.

2. Fiziksel depolama bloklarını şifrelemek, veritabanı varlıklarını _____ korur.

3. TLS protokolleri, _____ olan etkin veri paketlerini şifreler.

4. Role dayalı izinler, hangi kullanıcıların veritabanına _____ elde edebileceğini sınırlar.

5. Bir ihlalden sonra temiz kurumsal dosyaları geri yüklemek, güvenli ve çevrimdışı bir _____ gerektirir.

6. Bulut yapılandırmalarını denetlemek, bir kuruluşun güvenlik _____ değerlendirmesini sağlar.

KELİME BANKASI

AKTARIM HALİNDE · DURAĞAN HALDE · DURUŞ · ERİŞİM · İHLAL · MASKELEME · MİNİMİZASYON · YEDEK

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

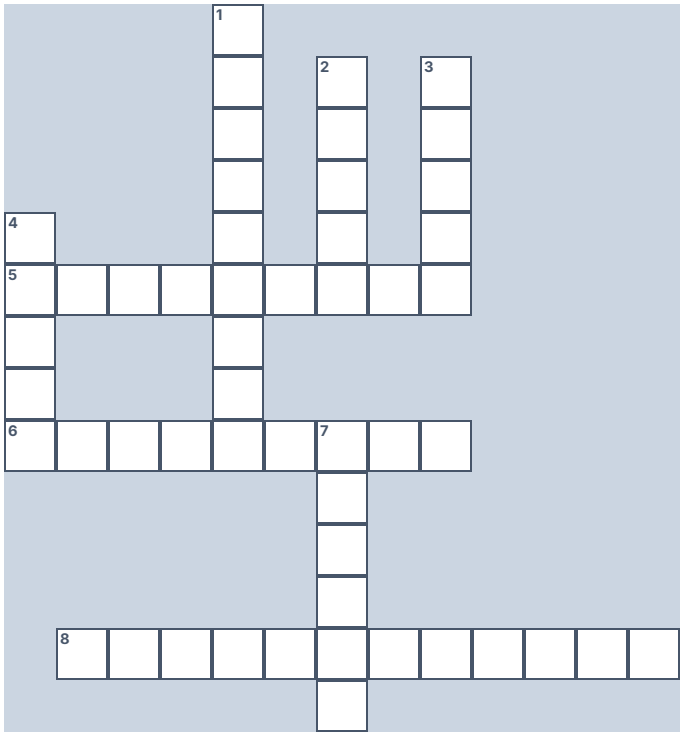
TANIM EŞLEŞTİRME

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

☐	1. ŞİFRELEME	A	Sistem arızaları durumunda geri yüklemek için verilerin güvenli, harici kopyalarını oluşturma.
☐	2. YEDEK	B	Düz metni okunamaz şifreli metne dönüştürerek ele geçirilen verilerin gizli kalmasını sağlamak.
☐	3. MİNİMİZASYON	C	Bir kuruluşun bulutunun toplu güvenlik durumu ve savunma hazırlığı.
☐	4. ERİŞİM	D	Özel kullanıcı bilgilerini yönetmek için GDPR veya CCPA gibi düzenleyici standartları karşılamak.
☐	5. DURUŞ	E	Korunan verilere yetkisiz erişildiği veya verilerin yetkisiz ifşa edildiği güvenlik olayı.
☐	6. İHLAL	F	Veritabanı okuma ve yazma izinlerini kimliği doğrulanmış kullanıcı rolleriyle kısıtlamak.
☐	7. UYUMLULUK	G	Kişisel kimlikleri korumak için veritabanı alanlarındaki hassas karakterleri değiştirmek.
☐	8. GİZLEME	H	Kişisel veri toplamayı işlemler için gereken mutlak asgari düzeyle sınırlamak.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

5. Özel kullanıcı bilgilerini yönetmek için GDPR veya CCPA gibi düzenleyici standartları karşılama (9)

6. Düz metni okunamaz şifreli metne dönüştürerek yakalanan verilerin gizli kalmasını sağlama (9)

8. Kişisel veri toplamayı operasyonlar için gereken mutlak asgari düzeyle sınırlama (12)

YUKARIDAN AŞAĞI

1. Kişisel kimlikleri korumak için veritabanı alanlarındaki hassas karakterleri değiştirme (9)

2. Korunan verilere yetkisiz erişildiği veya verilerin yetkisiz ifşa edildiği güvenlik olayı (5)

3. Sistem arızalarında geri yüklemek üzere verilerin güvenli, uzak kopyalarını oluşturma (5)

4. Bir kuruluşun bulutunun toplu güvenlik durumu ve savunma hazırlığı (5)

7. Veritabanı okuma ve yazma izinlerini kimliği doğrulanmış kullanıcı rolleriyle kısıtlama (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: Özel kullanıcı bilgilerini yönetmek için GDPR veya CCPA gibi düzenleyici standartları karşılama (9 harf):

6 soldan sağa: Düz metni okunamaz şifreli metne dönüştürerek yakalanan verilerin gizli kalmasını sağlama (9 harf):

8 soldan sağa: Kişisel veri toplamayı operasyonlar için gereken mutlak asgari düzeyle sınırlama (12 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Kişisel kimlikleri korumak için veritabanı alanlarındaki hassas karakterleri değiştirme (9 harf):

2 yukarıdan aşağı: Korunan verilere yetkisiz erişildiği veya verilerin yetkisiz ifşa edildiği güvenlik olayı (5 harf):

3 yukarıdan aşağı: Sistem arızalarında geri yüklemek üzere verilerin güvenli, uzak kopyalarını oluşturma (5 harf):

4 yukarıdan aşağı: Bir kuruluşun bulutunun toplu güvenlik durumu ve savunma hazırlığı (5 harf):

7 yukarıdan aşağı: Veritabanı okuma ve yazma izinlerini kimliği doğrulanmış kullanıcı rolleriyle kısıtlama (6 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

ŞİFRELEME, YEDEK, MİNİMİZASYON, ERİŞİM, DURUŞ, İHLAL, UYUMLULUK, MASKELEME

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. YEDEK**
- **C. MİNİMİZASYON**
- **D. ERİŞİM**
- **E. DURUŞ**
- **F. İHLAL**
- **G. UYUMLULUK**
- **H. MASKELEME**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Korunan verilere yetkisiz erişildiği veya verilerin yetkisiz ifşa edildiği güvenlik olayı.
2. Kişisel kimlikleri korumak için veritabanı alanlarındaki hassas karakterleri değiştirme.
3. Veritabanı okuma ve yazma izinlerini kimliği doğrulanmış kullanıcı rolleriyle kısıtlama.
4. Bir kuruluşun bulutunun toplu güvenlik durumu ve savunma hazırlığı.
5. Özel kullanıcı bilgilerini yönetmek için GDPR veya CCPA gibi düzenleyici standartları karşılama.
6. Kişisel veri toplamayı operasyonlar için gereken mutlak asgari düzeyle sınırlama.
7. Düz metni okunamaz şifreli metne dönüştürerek yakalanan verilerin gizli kalmasını sağlama.
8. Sistem arızalarında geri yüklemek üzere verilerin güvenli, uzak kopyalarını oluşturma.

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. NİMİMYONASZİ
3. RDŞUU
4. LKUMLUUYU
5. DKYEE
6. İŞEİMR
7. ALİLH
8. EEMMKALES

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Yedeklediğin şeyler			
2	Siber güvenlikle ilgili sözcükler			
3	Hassas verileri görmesine izin verilen kişiler			
4	Verileri güvenli şekilde silme yolları			
5	Verilerin saklandığı yerler			
6	Şifrelenmesi gereken şeyler			
7	Bir hastanenin korumak zorunda olduğu veriler			
8	Yedekleme türleri			
9	Asla paylaşmaman gereken bilgiler			
10	E-postadaki uyarı işaretleri			
11	Bugün başlayabileceğin güvenli alışkanlıklar			
12	BT yardımı için sorabileceğin kişiler			
13	Hacklenebilecek cihazlar			
14	Verileri koruma yolları			
15	Verileri yok edebilecek şeyler			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KURUMSAL VERİTABANI DURAĞAN VERİ ŞİFRELEME YÜKSELTMESİ

👷

Senaryo: Çevrimiçi bir perakendeci, işlem veritabanlarını tam disk şifrelemesi olmadan bulut depolamada saklıyor. Yakın zamanda yapılan bir uyumluluk denetimi bunu ciddi bir CCPA veri güvenliği riski olarak işaretledi. Bir kurtarma mimarisi tasarla.

Tartışma sorusu: CCPA uyumluluk risklerini analiz et ve bekleme durumundaki (at-rest) veriler için bir şifreleme stratejisi öner.

VAKA ÇALIŞMASI 2: FİDYE YAZILIMINI KONTROL ALTINA ALMA VE VERİ GERİ YÜKLEME

👷

Senaryo: Kurumsal bir yerel ağda etkin bir fidye yazılımı saldırısı ağ sürücülerini şifreliyor. Yönetici enfeksiyonu erken fark etti. Sınırlandırma ve kurtarma adımlarını planla.

Tartışma sorusu: Acil sınırlandırma eylemlerini ayrıntılı anlat ve güvenli bir geri yükleme süreci planla.

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

19	29	6	15	27	6	21	12	15	6	21	12	17	12

8	26	27	6	17	15	12	14	18	17	24	21	18	15	15	6	21	15	6

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: Veri koruma nedir?

Kişisel ve iş verilerini teknik denetimlerle yetkisiz erişime, kayba veya bozulmaya karşı koruma sürecidir.

Q2: Tam disk şifrelemesi neden önemlidir?

Fiziksel sürücülerdeki depolanmış veri bloklarını korur; sabit disk fiziksel olarak çalınsa bile kimsenin verileri okumasını önler.

Q3: Beklemedeki (at rest) ve aktarım sırasındaki (in transit) şifreleme arasındaki fark nedir?

Durağan veri şifreleme, sürücülerdeki depolanmış dosyaları korurken, aktarım halindeki veri şifreleme yönlendiriciler üzerinden hareket eden etkin ağ paketlerini korur.

Q4: Veri maskeleme nedir?

Gerçek kayıtları açığa çıkarmadan test için hassas ayrıntıları (kredi kartı numaraları gibi) kurgusal ama gerçekçi verilerle değiştirir.

Q5: Çevrimdışı yedekleme neden önemlidir?

Dosyalarının temiz bir kopyasını ağdan yalıtılmış tutar; bu da yedeklerinin fidye yazılımıyla şifrelenmesine karşı korumaya yardımcı olur.

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

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Veri belirteçleme (tokenization) kasası nedir?

Rastgele belirteçleri özgün hassas değerleriyle (birincil kredi kartı numaraları gibi) eşleyen güvenli, yalıtılmış veritabanı.

Q7: Sıfır güvenli veritabanı erişimi ne demektir?

Ağ içindeki hiç kimseye güvenmek yerine her girişte her kullanıcının kimliğini ve cihaz durumunu doğrulamak anlamına gelir.

Q8: TLS aktarım sırasındaki verileri nasıl korur?

TLS, TCP oturumu yükünü şifreler ve genel ağlardaki kötü niyetli kişilerin iletilen paketleri dinlemesini veya değiştirmesini önler.

Q9: Veritabanı erişim denetimi nedir?

Yetkisiz erişim kalıplarını veya güvenlik anormalliklerini algılamak için veri tabanı sorgularının ve oturum açmaların sürekli kaydedilmesi.

Q10: Bulut güvenliği duruş denetimi nedir?

Açık bağlantı noktalarını, yanlış yapılandırılmış erişim kurallarını ve güvenlik uyumluluk açıklarını belirlemek için bulut yapılandırmalarını analiz eden süreç.

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: Zarf şifrelemesi nasıl çalışır?

Verileri bir veri anahtarıyla şifreler, ardından bu veri anahtarını bir ana anahtarla şifreler; anahtar depolamayı ve döndürmeyi basitleştirir.

Q2: Homomorfik şifreleme nedir?

Şifrelenmiş veriler üzerinde önce şifresini çözmeden doğrudan işlem yapılmasına olanak tanıyan gelişmiş şifreleme yöntemi.

Q3: Veritabanında sütun düzeyinde şifreleme neden kullanılır?

Belirli hassas sütunları (SSN gibi) tek tek şifreler ve yöneticiler genel tablo okuma erişimi elde etse bile onları korur.

Q4: Veri kaybı önleme (DLP) nedir?

Hassas dosyaların yetkisiz giden aktarımlarını algılamak ve engellemek için ağ çıkış noktalarını izleyen yazılım.

Q5: Bir kez yaz, çok kez oku (WORM) yedekleri fidye yazılımına karşı nasıl korur?

WORM yedekleri, dosyaların belirli bir süre boyunca silinmesini veya değiştirilmesini önler; fidye yazılımının mevcut yedekleri şifrelemesini engeller.

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: Anahtar yeniden kullanımının riski nedir?

Aynı şifreleme anahtarını farklı veritabanlarında tekrar kullanmak, tek bir anahtarın ele geçirilmesinin tüm veritabanlarını açığa çıkarması anlamına gelir.

Q7: Veritabanı belirteçleme (tokenization) CCPA uyumluluğunu nasıl iyileştirir?

Belirteçler üretim dışı sistemlerdeki kayıtları takma adlandırır ve ihlal riskini sınırlar, ancak belirteçlenmiş veriler yine de kişisel bilgi olabilir.

Q8: Veri sınıflandırması neden kritiktir?

Dosyaları hassasiyet düzeyine göre sınıflandırır ve kuruluşların yüksek riskli verilere en güçlü şifreleme ve erişim denetimlerini uygulamasına yardımcı olur.

Q9: Anahtar döndürmenin rolü nedir?

Şifreleme anahtarlarını düzenli olarak güncellemek, tek bir anahtar sonunda kırılırsa açığa çıkan geçmiş veri miktarını sınırlar.

Q10: Güvenli enklavlar bellekteki veritabanı sorgularını nasıl korur?

Güvenli enklavlar, sorgu işlemlerini CPU korumalı bellek bloklarında yalıtarak ana sistem yöneticilerinin RAM'deki açık metni görmesini engeller.

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

GDPR düzenlemeleri Mayıs 2018'de yürürlüğe girdi ve küresel sitelerin çerez onaylarını ve kişisel veri kayıtlarını yönetme biçimini değiştirdi.

2. GÜVENLİK İPUCU

Bir GDPR ihlali cezası 20 milyon Euro'ya veya küresel cironun %4'üne ulaşabilir; bu da önemli bir hukuki risk anlamına gelir. [4]

3. GÜVENLİK İPUCU

CCPA, Ocak 2020'de yürürlüğe girdi ve Amerika Birleşik Devletleri'nde dijital gizlilik alanında öncü tüketici haklarını oluşturdu.

4. GÜVENLİK İPUCU

Veri minimizasyonu veri tabanı depolama alanını küçülterek sunucu işletim maliyetlerini azaltır ve ihlal etkisinin ölçeğini düşürür.

5. GÜVENLİK İPUCU

Şifreli imha, geçmiş yedekleme bandı dosyalarını düzenlemek yerine anahtarları silerek yedek silme zorluğunu çözer.

6. GÜVENLİK İPUCU

Dünya genelindeki çoğu ülke artık tüketicilerin gizlilik haklarını korumak için kişisel veri koruma yasaları çıkarmıştır.

7. GÜVENLİK İÇGÖRÜSÜ

Önceden işaretlenmiş kutulu açık onay formları, Avrupa veri gizliliği düzenleme tanımları uyarınca açıkça yasaklanmıştır.

8. GÜVENLİK İÇGÖRÜSÜ

GDPR, kişisel veri ihlallerinin, mümkün olduğunda, öğrenildikten sonraki 72 saat içinde denetleyici makama bildirilmesini şart koşar. [3]

9. GÜVENLİK İÇGÖRÜSÜ

Parolaları bcrypt veya Argon2 gibi yavaş algoritmalarla özetlemek (hash), çalınan özetlerin çevrimdışı kırılmasını çok daha zorlaştırır. [6]

10. GÜVENLİK İPUCU

Durağan veri kaydedilmiş veri tabanı dosyalarını temsil ederken, aktarım halindeki veri ağ yönlendiricileri arasında aktif olarak hareket eden paketleri kapsar.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Veri maskelemenin temel amacı nedir? → Gizliliği korumak için hassas tanımlayıcıları kurgusal ancak gerçekçi karakterlerle değiştirmek

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Hangi mekanizma bir veri tabanı sunucusunun sabit diskinde saklanan dosyaları şifreler? → Bekleme durumunda tam disk şifrelemesi

3 **Soru 3** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Aktarım halindeki veriyi ne temsil eder? → Ağ yönlendiricileri ve anahtarları arasında hareket eden veri paketleri

4 **Soru 4** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Düzenli bir çevrim dışı yedek, fidye yazılımına karşı korunmak için neden kritiktir? → Fidye ödemeden dosyaları geri yüklemek için temiz, çevrimdışı bir kopya sağlar

5 **Soru 5** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Veri belirteçleme (tokenization) ne yapar? → Hassas kart numaralarını hassas olmayan rastgele belirteçlerle değiştirir

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Maskeleme test kopyalarını değiştirir veya değerleri sorgu sırasında gizler; üretim kayıtları değişmeden kalır.

7 **Soru 7** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Fidye yazılımının yayılmasını önlemek için yedeklemeler ana kurumsal ağdan yalıtılmış olmalıdır.

8 **Soru 8** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

TLS sertifikaları aktarım sırasındaki verileri korur; bekleme durumundaki veriler disk, dosya veya veritabanı şifrelemesi gerektirir.

9 **Soru 9** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Sıfır Güvenli ağ erişimi (ZTNA), veri tabanı erişimi vermeden önce her kullanıcının kimliğini doğrular.

10 **Soru 10** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Kasa tabanlı belirteçleme, orijinal değerleri her belirteci verisine geri eşleyen güvenli bir belirteç kasasında tutar.

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

B 1. ŞİFRELEME	A 2. YEDEK	H 3. MİNİMİZASYON	F 4. ERİŞİM
C 5. DURUŞ	E 6. İHLAL	D 7. UYUMLULUK	G 8. GİZLEME

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 MASKELEME	2 DURAĞAN HALDE	3 AKTARIM HALİNDE	4 ERİŞİM
5 YEDEK	6 DURUŞ		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 F – İHLAL	2 H – MASKELEME	3 D – ERİŞİM	4 E – DURUŞ
5 G – UYUMLULUK	6 C – MİNİMİZASYON	7 A – ŞİFRELEME	8 B – YEDEK

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

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

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

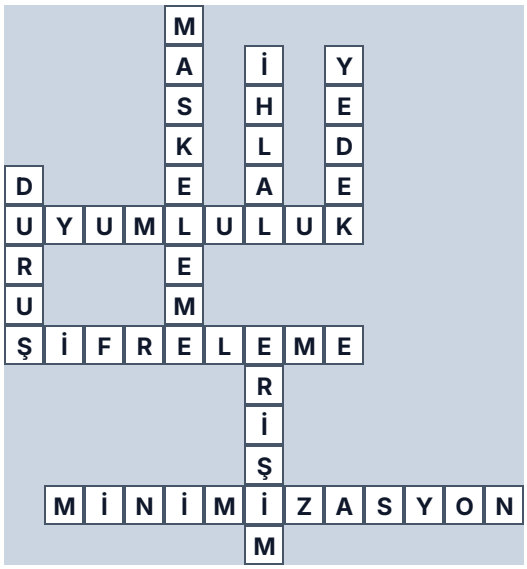
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

5 soldan sağa: UYUMLULUK Özel kullanıcı bilgilerini yönetmek için GDPR veya CCPA gibi düzenleyici standartları karşılama (9 harf)

6 soldan sağa: ŞİFRELEME Düz metni okunamaz şifreli metne dönüştürerek yakalanan verilerin gizli kalmasını sağlama (9 harf)

8 soldan sağa: MİNİMİZASYON Kişisel veri toplamayı operasyonlar için gereken mutlak asgari düzeyle sınırlama (12 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: MASKELEME Kişisel kimlikleri korumak için veritabanı alanlarındaki hassas karakterleri değiştirme (9 harf)

2 yukarıdan aşağı: İHLAL Korunan verilere yetkisiz erişildiği veya verilerin yetkisiz ifşa edildiği güvenlik olayı (5 harf)

3 yukarıdan aşağı: YEDEK Sistem arızalarında geri yüklemek üzere verilerin güvenli, uzak kopyalarını oluşturma (5 harf)

4 yukarıdan aşağı: DURUŞ Bir kuruluşun bulutunun toplu güvenlik durumu ve savunma hazırlığı (5 harf)

7 yukarıdan aşağı: ERİŞİM Veritabanı okuma ve yazma izinlerini kimliği doğrulanmış kullanıcı rolleriyle kısıtlama (6 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	LERİŞEMEF	ŞİFRELEME	5.	DKYEE	YEDEK
2.	NİMİMYONASZİ	MİNİMİZASYON	6.	İŞEİMR	ERİŞİM
3.	RDŞUU	DURUŞ	7.	ALİLH	İHLAL
4.	LKUMLUUYU	UYUMLULUK	8.	EEMMKALES	MASKELEME

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"ÖZEL VERİLERİNİ GÜVENLİ KONTROLLERLE KORU"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Kurumsal Veritabanı Durağan Veri Şifreleme Yükseltmesi

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir çevrimiçi perakendeci, işlem veritabanlarını tam disk şifrelemesi olmadan bulut depolamada saklıyor. Yakın tarihli bir uyumluluk denetimi bunu ciddi bir CCPA veri güvenliği riski olarak işaretledi. Bir kurtarma mimarisi tasarla.
- Önerilen Strateji ve Çözüm: Tüm dosya sistemlerinde bekleme durumunda AES-256 tam disk şifrelemesi uygula. Otomatik anahtar döndürmeli merkezi bir Anahtar Yönetim Hizmeti (KMS) kullan ve şifre çözme erişimini denetlemek için katı IAM politikaları uygula.

B Vaka Çalışması 2: Fidye Yazılımını Kontrol Altına Alma ve Veri Geri Yükleme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Etkin bir fidye yazılımı saldırısı, kurumsal yerel ağdaki ağ sürücülerini şifreliyor. Yönetici enfeksiyonu erken tespit etti. Sınırlama ve kurtarma adımlarını planla.
- Önerilen Strateji ve Çözüm: Ele geçirilen segmenti hemen izole et. Etkilenen uç noktaları biçimlendir ve en son çevrimdışı, bir kez yaz çok kez oku (WORM) yedekten geri yükle. Sistemleri yeniden bağlamadan önce yedeğin bütünlüğünü doğrula.