Emri: _____ Data: _____ Pikët: _____

Mbrojtja e të dhënave dhe ruajtja e të dhënave në ndërmarrje Udhëzues sigurie

Maskimi i të dhënave, tokenizimi, enkriptimi në pushim kundër atij në tranzit, kopjet rezervë offline

PËRMBLEDHJE MËSIMORE PËR MBROJTJEN E TË DHËNAVE

I SIGURUAR
ENKRIPTIMI I TË DHËNAVE
Standardi AES 256-bit

I PËRPUTHSHËM
STANDARDET GLOBALE
Kornizat GDPR dhe CCPA

ZERO-TRUST
POLITIKA E QASJES
Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes standardeve dhe kontrolleve të mbrojtjes së të dhënave. Do të eksplorosh enkriptimin e plotë të diskut, kontrollet e sigurta të qasjes, kopjet rezervë harduerike, qëndrimin e sigurisë në cloud dhe teknikat e maskimit të të dhënave.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/mbrojtja-e-te-dhenave/

Udhërrëfyesi yt mësimor për strategjinë e mbrojtjes së të dhënave

- Dallo mes teknikave të maskimit të të dhënave dhe të tokenizimit.
- Zbato enkriptim në qëndrim për disqet e ruajtjes dhe enkriptim në tranzit duke përdorur TLS.
- Harto sisteme kopjesh rezervë offline, të izoluara nga rrjeti, për mbrojtje nga ransomware-i.

UDHËZIME PËR UDHËZUESIN E MBROJTJES SË TË DHËNAVE

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për mbrojtjen e të dhënave. Përfundo me aktivitetin bonus Mendo shpejt.

MBROJTJA E TË DHËNAVE DHE SIGURIA E RUAJTJES SË NDËRMARRJES (HYRJE)

Mbrojtja e të dhënave i ruan pasuritë e të dhënave të korporatës përmes maskimit, tokenizimit, enkriptimit të bazave të të dhënave në pushim dhe protokolleve të sigurta të tranzitit. Hartimi i kopjeve rezervë të izoluara nga rrjeti ndihmon të sigurohet që bazat kryesore të të dhënave të mund të rikthehen në rast ndërhyrjeje aktive.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Cili është qëllimi kryesor i maskimit të të dhënave?

- A. Zëvendësimi i identifikuesve të ndjeshëm me karaktere fiktive por realiste për të mbrojtur privatësinë
- B. Kompresimi i skedarëve të mëdhenj të bazës së të dhënave për të kursyer hapësirën e ruajtjes fizike të serverit
- C. Fshirja e emaileve të vjetra të kontaktit të klientëve nga sistemet rezervë arkivore
- D. Fshehja e IP-së publike të serverit të bazës së të dhënave nga skanimet e internetit

2. Cili mekanizëm enkripton skedarët e ruajtur në hard diskun e një serveri baze të dhënash?

- A. Enkriptim i plotë i diskut në qetësi (at rest)
- B. Protokollet e handshake-ut të sesionit TLS gjatë transitit
- C. Rregullat e përcjelljes së serverit të emrave Dynamic DNS
- D. Autentikim me shumë faktorë duke përdorur çelësa harduerikë

3. Çfarë përfaqëson të dhënat në tranzit?

- A. Paketa të dhënash që lëvizin nëpër router-ë dhe switch-e rrjeti
- B. Logjet e transaksioneve të bazës së të dhënave të ruajtura në një disk rezervë të ftohtë
- C. Skedarë të arkivuar të përdoruesve të ruajtur në një kasafortë cloud të izoluar
- D. Skedarë statikë të konfigurimit të sistemit në ruajtje lokale të desktop-it

4. Pse është kritike një kopje rezervë offline e rregullt për mbrojtjen nga ransomware?

- A. Ofron një kopje të pastër offline për rikthimin e skedarëve pa paguar shpërblim
- B. Parandalon hakerët të skanojnë konfigurimet e porteve të hapura
- C. Rrit shpejtësitë e transmetimit në rrjetin lokal
- D. Automatizon regjistrat e pranimit të cookie-ve në shfletues

5. Çfarë bën tokenizimi i të dhënave?

- A. Zëvendëson numrat e ndjeshëm të kartave me token-ë të rastësishëm jo të ndjeshëm
- B. E rrugëzon trafikun e uebit përmes disa nyjeve të sigurta onion
- C. Skanon drejtoritë e sistemit për malware të bazuar në nënshkrime
- D. Auditon kohët e sesioneve të hyrjes së administratorëve të bazës së të dhënave

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Maskimi i të dhënave i ndryshon përgjithmonë regjistrimet e bazës së të dhënave në mjediset e prodhimit.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. Kopjet rezervë jashtë vendit duhet të izolohen nga rrjeti kryesor korporativ për të parandaluar përhapjen e ransomware-it.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Certifikatat SSL/TLS sigurojnë bazat e të dhënave duke enkriptuar të dhënat e ruajtura në qetësi në media fizike.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. Zero-trust network access (ZTNA) verifikon identitetin e çdo përdoruesi para se t'i japë qasje në bazën e të dhënave.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Tokenizimi i bazuar në vault i ruan vlerat origjinale të kartës në një vault qendror të sigurt tokenësh.

- ○ E vërtetë
- ○ E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Zëvendësimi i emrave personalë me zëvendësues realistë quhet _____ i të dhënave.

2. Enkriptimi i blloqeve fizike të ruajtjes mbron asetet e bazës së të dhënave kur ato janë _____ .

3. Protokollet TLS enkriptojnë paketat aktive të të dhënave që lëvizin në _____ .

4. Lejet e bazuara në role kufizojnë cilët përdorues mund të marrin _____ në bazën e të dhënave.

5. Rikthimi i skedarëve të pastër të kompanisë pas një kompromentimi kërkon një _____ të sigurt jashtë linje.

6. Auditimi i konfigurimeve të cloud-it vlerëson këtë tregues të organizatës: _____ .

BANKA E FJALËVE TË LEKSIKUT

KOPJE SIGURIE | MASKIM | MINIMIZIM | NË PUSHIM | POSTURË SIGURIE | QASJE | SHKELJE | TRANZIT

Shkruaj përgjigjet e tua këtu:

1. | **2.**

3. | **4.**

5. | **6.**

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

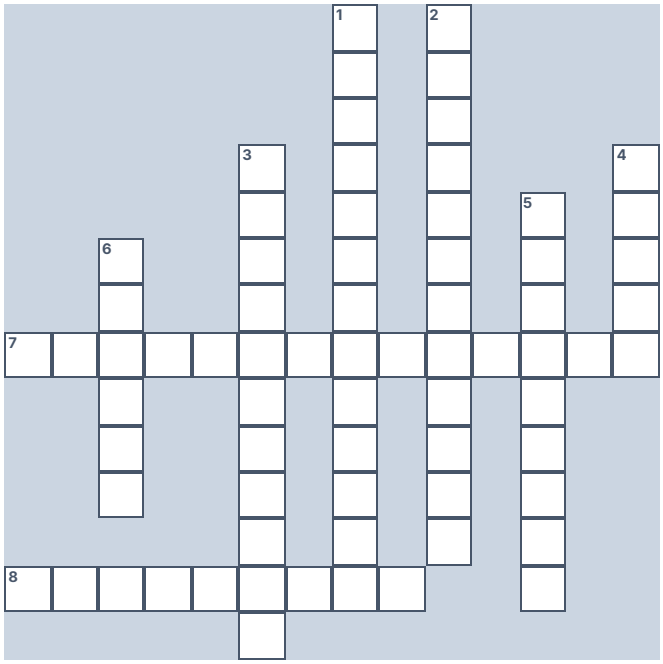
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. ENKRIPTIM	A	Krijimi i kopjeve të sigurta jashtë vendndodhjes të të dhënave për t'i rikthyer në rast dështimesh të sistemit.
☐	2. KOPJE REZERVË	B	Shndërrimi i tekstit të thjeshtë në tekst të shifruar të palexueshëm, që të dhënat e përgjuara të mbeten private.
☐	3. MINIMIZIM	C	Gjendja kolektive e sigurisë dhe gatishmëria mbrojtëse e cloud-it të një organizate.
☐	4. QASJE	D	Përmbushja e standardeve rregullatore si GDPR ose CCPA për menaxhimin e informacionit privat të përdoruesve.
☐	5. QËNDRIM	E	Incident sigurie ku të dhënat e mbrojtura aksesohen ose zbulohen pa autorizim.
☐	6. SHKELJE	F	Kufizimi i lejeve të leximit dhe shkrimit të bazës së të dhënave te rolet e përdoruesve të vërtetuar.
☐	7. PËRPUTHSHMËRI	G	Zëvendësimi i karaktereve të ndjeshme në fushat e bazës së të dhënave për të mbrojtur identitetet personale.
☐	8. MASKIM	H	Kufizimi i mbledhjes së të dhënave personale në minimumin absolut të nevojshëm për operimet.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

7. Gjendja kolektive e sigurisë dhe gatishmëria mbrojtëse e cloud-it të një organizate (14)

8. Kufizimi i mbledhjes së të dhënave personale në minimumin e nevojshëm për operacionet (9)

VERTIKALISHT

1. Përmbushja e standardeve rregullatore si GDPR ose CCPA për menaxhimin e informacionit privat të përdoruesve (13)

2. Krijimi i kopjeve të sigurta jashtë vendit për rikthim në rast dështimi të sistemit (12)

3. Incident sigurie ku të dhënat e mbrojtura aksesohen ose zbulohen pa autorizim (11)

4. Kufizimi i lejeve të leximit dhe shkrimit në bazën e të dhënave për rolet e autentikuara të përdoruesve (5)

5. Shndërrimi i tekstit të qartë në tekst të shifruar të palexueshëm, që të dhënat e përgjuara të mbeten private (9)

6. Zëvendësimi i karaktereve të ndjeshme në fushat e bazës së të dhënave për të mbrojtur identitetet personale (6)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

7 horizontalisht: Gjendja kolektive e sigurisë dhe gatishmëria mbrojtëse e cloud-it të një organizate (14 shkronja):

8 horizontalisht: Kufizimi i mbledhjes së të dhënave personale në minimumin e nevojshëm për operacionet (9 shkronja):

VERTIKALISHT

1 vertikalisht: Përmbushja e standardeve rregullatore si GDPR ose CCPA për menaxhimin e informacionit privat të përdoruesve (13 shkronja):

2 vertikalisht: Krijimi i kopjeve të sigurta jashtë vendit për rikthim në rast dështimi të sistemit (12 shkronja):

3 vertikalisht: Incident sigurie ku të dhënat e mbrojtura aksesohen ose zbulohen pa autorizim (11 shkronja):

4 vertikalisht: Kufizimi i lejeve të leximit dhe shkrimit në bazën e të dhënave për rolet e autentikuara të përdoruesve (5 shkronja):

5 vertikalisht: Shndërrimi i tekstit të qartë në tekst të shifruar të palexueshëm, që të dhënat e përgjuara të mbeten private (9 shkronja):

6 vertikalisht: Zëvendësimi i karaktereve të ndjeshme në fushat e bazës së të dhënave për të mbrojtur identitetet personale (6 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

M I D J P L I P A E N I M Ç L

E I C Ç F G B Ë B N Q K O U S

I G K Y E Y Q R F X V G E P S

R M T S I Q Ç P S R K O J L R

U G I O A G Y U N K V T M M Y

G P P B A M J T N L B J I G Q

I E H M Y B Z H Z Y B L T U A

S X K C E N V S O P X F E D S

E Y C V K E F H F Z V C M N J

J P I V X Q J M Z A L Q O Z E

P P O S T U R Ë S I G U R I E

O Q K Ë R V Ë R J V H B P Y C

K C Y M I T P I R K N E M N T

Z N Z T S B G U O X C L O K G

M I Z I M I N I M O X Y K Z X

LISTA E FJALËVE TË LEKSIKUT

ENKRIPTIM KOPJESIGURIE MINIMIZIM QASJE POSTURËSIGURIE KOMPROMETIM PËRPUTHSHMËRI MASKIM

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. ENKRIPTIM**
- **B. KOPJESIGURIE**
- **C. MINIMIZIM**
- **D. QASJE**
- **E. POSTURËSIGURIE**
- **F. KOMPROMETIM**
- **G. PËRPUTHSHMËRI**
- **H. MASKIM**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Incident sigurie ku të dhënat e mbrojtura aksesohen ose zbulohen pa autorizim.
2. Zëvendësimi i karaktereve të ndjeshme në fushat e bazës së të dhënave për të mbrojtur identitetet personale.
3. Kufizimi i lejeve të leximit dhe shkrimit në bazën e të dhënave për rolet e autentikuara të përdoruesve.
4. Gjendja kolektive e sigurisë dhe gatishmëria mbrojtëse e cloud-it të një organizate.
5. Përmbushja e standardeve rregullatore si GDPR ose CCPA për menaxhimin e informacionit privat të përdoruesve.
6. Kufizimi i mbledhjes së të dhënave personale në minimumin e nevojshëm për operacionet.
7. Shndërrimi i tekstit të qartë në tekst të shifruar të palexueshëm, që të dhënat e përgjuara të mbeten private.
8. Krijimi i kopjeve të sigurta jashtë vendit për rikthim në rast dështimi të sistemit.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. PIRNETIMK
2. MMIIIIZMN
3. PIOISEGUSËURRT
4. TRHRSUIHËMPËP
5. ORGIEPEUSKIJ
6. JQSEA
7. ERKOMMTIMOP
8. SMMIKA

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Gjëra që ruan si kopje rezervë			
2	Fjalë që lidhen me sigurinë kibernetike			
3	Njerëz që lejohen t'i shohin të dhënat e ndjeshme			
4	Mënyra për të fshirë të dhënat në mënyrë të sigurt			
5	Vende ku ruhen të dhënat			
6	Gjëra që duhet të enkriptohen			
7	Të dhëna që një spital duhet t'i mbrojë			
8	Lloje kopjesh rezervë			
9	Informacione që nuk duhet t'i ndash kurrë			
10	Shenja paralajmëruese në një email			
11	Zakone të sigurta që mund t'i fillosh sot			
12	Njerëz që mund t'i pyesësh për ndihmë me IT-në			
13	Pajisje që mund të hakohen			
14	Mënyra për të mbrojtur të dhënat			
15	Gjëra që mund t'i shkatërrojnë të dhënat			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: PËRMIRËSIMI I ENKRIPTIMIT NË PUSHIM TË BAZËS SË TË DHËNAVE TË NDËRMARRJES

👷

Skenari: Një shitës online i ruan bazat e të dhënave të transaksioneve në hapësirë ruajtjeje cloud pa enkriptim të plotë të diskut. Një auditim i fundit i përputhshmërisë e shënoi këtë si rrezik serioz të sigurisë së të dhënave sipas CCPA. Harto një arkitekturë rimëkëmbjeje.

Pyetje për diskutim: Analizo rreziqet e përputhshmërisë me CCPA dhe propozo një strategji enkriptimi në qetësi (at rest).

STUDIMI I RASTIT 2: PËRMBAJTJA E RANSOMWARE-IT DHE RIKTHIMI I TË DHËNAVE

👷

Skenari: Një sulm aktiv ransomware po enkripton disqet e rrjetit në një rrjet lokal të kompanisë. Administratori e ka zbuluar infeksionin herët. Planifiko hapat e izolimit dhe të rimëkëmbjes.

Pyetje për diskutim: Përshkruaj në detaje veprimet e menjëhershme të izolimit dhe planifiko një proces të sigurt restaurimi.

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

15 2 20 17 12 22 7 5 10 7 16 1 22

18 20 11 24 1 22 6 15 6 13 17 16 22 20 17 14 14 6

22 7 21 11 9 23 20 22 1

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Çfarë është mbrojtja e të dhënave?

Është procesi i sigurimit të të dhënave personale dhe të biznesit nga qasja e paautorizuar, humbja ose korruptimi përmes kontrolleve teknike.

Q2: Pse është e rëndësishme enkriptimi i plotë i diskut?

Siguron blloqet e ruajtura të të dhënave në disqet fizike, duke parandaluar që kushdo të lexojë të dhënat nëse vjedh fizikisht hard diskun.

Q3: Cili është ndryshimi mes enkriptimit në pushim dhe atij gjatë transmetimit?

Enkriptimi në pushim siguron skedarët e ruajtur në disqe, ndërsa enkriptimi në tranzit siguron paketat aktive të rrjetit që lëvizin nëpër router-ë.

Q4: Çfarë është maskimi i të dhënave?

Zëvendëson detaje të ndjeshme (si numrat e kartave të kreditit) me të dhëna fiktive por realiste për testim pa ekspozuar regjistrat realë.

Q5: Pse është e rëndësishme kopjeruajtja offline?

Ruan një kopje të pastër të skedarëve të tu të izoluar nga rrjeti, gjë që ndihmon në mbrojtjen e kopjeve rezervë nga enkriptimi nga ransomware.

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Çfarë është një kasafortë tokenizimi e të dhënave?

Një bazë e dhënash e sigurt dhe e izoluar që lidh token-ët e rastësishëm me vlerat e tyre origjinale të ndjeshme (si numrat kryesorë të kartave të kreditit).

Q7: Çfarë do të thotë aksesi zero-trust në bazën e të dhënave?

Do të thotë verifikimi i identitetit dhe i gjendjes së pajisjes së çdo përdoruesi në çdo hyrje, në vend që t'i besohet kujtdo brenda rrjetit.

Q8: Si i mbron TLS të dhënat gjatë transmetimit?

TLS enkripton ngarkesën e seancës TCP, duke parandaluar që aktorët keqdashës në rrjete publike të përgjojnë ose modifikojnë paketat në tranzit.

Q9: Çfarë është auditimi i aksesit në bazën e të dhënave?

Regjistrimi i vazhdueshëm i kërkesave dhe hyrjeve në bazën e të dhënave për të zbuluar modele të qasjes së paautorizuar ose anomali sigurie.

Q10: Çfarë është një auditim i qëndrimit të sigurisë në cloud?

Një proces që analizon konfigurimet cloud për të identifikuar portat e hapura, rregullat e gabuara të qasjes dhe boshllëqet e përputhshmërisë së sigurisë.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si funksionon enkriptimi me zarf (envelope encryption)?

Enkripton të dhënat me një çelës të dhënash, pastaj e enkripton atë çelës të dhënash me një çelës kryesor, duke thjeshtuar ruajtjen dhe rotacionin e çelësave.

Q2: Çfarë është enkriptimi homomorfik?

Një metodë e avancuar enkriptimi që lejon kryerjen e veprimeve drejtpërdrejt mbi të dhënat e enkriptuara pa i deshifruar së pari.

Q3: Pse përdoret enkriptimi në nivel kolone i bazës së të dhënave?

Enkripton veçmas kolona specifike të ndjeshme (si SSN-të), duke i mbrojtur edhe nëse administratorët fitojnë qasje të përgjithshme leximi në tabelë.

Q4: Çfarë është parandalimi i humbjes së të dhënave (DLP)?

Softuer që monitoron pikat e daljes së rrjetit për të zbuluar dhe bllokuar transferimet e paautorizuara dalëse të skedarëve të ndjeshëm.

Q5: Si mbrojnë kopjeruajtjet WORM (write-once-read-many) nga ransomware?

Kopjet rezervë WORM pengojnë fshirjen ose modifikimin e skedarëve për një kohëzgjatje të caktuar dhe e ndalojnë ransomware-in të enkriptojë kopjet rezervë ekzistuese.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Cili është rreziku i ripërdorimit të çelësave?

Ripërdorimi i të njëjtit çelës kriptografik nëpër baza të ndryshme të dhënash do të thotë se kompromet imi i një çelësi të vetëm ekspozon të gjitha bazat e të dhënave.

Q7: Si e përmirëson tokenizimi i bazës së të dhënave pajtueshmërinë me CCPA?

Tokenat pseudonimizojnë regjistrimet në sistemet jo-prodhuese dhe kufizojnë ekspozimin ndaj shkeljeve, por të dhënat e tokenizuara mund të jenë përsëri informacion personal.

Q8: Pse është kritike klasifikimi i të dhënave?

Kategorizon skedarët sipas nivelit të ndjeshmërisë, duke ndihmuar organizatat të zbatojnë enkriptimin dhe kontrollet e qasjes më të forta për të dhënat me rrezik të lartë.

Q9: Cili është roli i rrotullimit të çelësave?

Përditësimi i rregullt i çelësave të enkriptimit kufizon sasinë e të dhënave historike të ekspozuara nëse një çelës i vetëm thyhet përfundimisht.

Q10: Si i mbrojnë enklavat e sigurta kërkesat e bazës së të dhënave në memorie?

Enklavat e sigurta izolojnë operacionet e kërkesave në blloqe memorieje të mbrojtura nga CPU-ja, duke parandaluar që administratorët e hostit të shohin tekstin e hapur në RAM.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

Rregulloret GDPR hynë në fuqi në maj 2018, duke ndryshuar mënyrën se si faqet globale menaxhojnë pëlqimet për cookie dhe regjistrat e të dhënave personale.

2. PERSPEKTIVË PËR SIGURINË

Një gjobë për shkelje të GDPR mund të arrijë 20 milionë euro ose 4% të qarkullimit global, çka përfaqëson ekspozim të konsiderueshëm ligjor. [4]

3. PERSPEKTIVË PËR SIGURINË

CCPA hyri në fuqi në janar 2020 dhe themeloi të drejta pioniere të konsumatorëve për privatësinë digjitale në Shtetet e Bashkuara.

4. PERSPEKTIVË PËR SIGURINË

Minimizimi i të dhënave zvogëlon hapësirën e zënë nga baza e të dhënave, duke ulur kostot operative të serverit dhe duke zvogëluar shkallën e ndikimit të një shkeljeje.

5. PERSPEKTIVË PËR SIGURINË

Shkatërrimi kriptografik e zgjidh sfidën e fshirjes së kopjeve rezervë duke pastruar çelësat në vend që të redaktojë skedarët historikë të shiritave të kopjeve rezervë.

6. PERSPEKTIVË PËR SIGURINË

Shumica e vendeve në botë tani kanë miratuar ligje për mbrojtjen e të dhënave personale për të mbrojtur të drejtat e privatësisë së konsumatorëve.

7. NJOHURI PËR SIGURINË

Formularët e pëlqimit me kuti të parakontrolluara ndalohen shprehimisht sipas përkufizimeve rregullatore evropiane për privatësinë e të dhënave.

8. NJOHURI PËR SIGURINË

GDPR kërkon raportimin e shkeljeve të të dhënave personale te autoriteti mbikëqyrës brenda 72 orëve nga marrja dijeni, kur është e mundur. [3]

9. NJOHURI PËR SIGURINË

Hashimi i fjalëkalimeve me algoritme të ngadalta si bcrypt ose Argon2 e bën shumë më të vështirë thyerjen offline të hash-eve të vjedhura. [6]

10. PERSPEKTIVË PËR SIGURINË

Të dhënat në pushim përfaqësojnë skedarët e ruajtur të bazave të të dhënave, ndërsa të dhënat në tranzit përfshijnë paketat që lëvizin aktivisht nëpër router-ët e rrjetit.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili është qëllimi kryesor i maskimit të të dhënave? → Zëvendësimi i identifikuesve të ndjeshëm me karaktere fiktive por realiste për të mbrojtur privatësinë

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili mekanizëm enkripton skedarët e ruajtur në hard diskun e një serveri baze të dhënash? → Enkriptim i plotë i diskut në qetësi (at rest)

3 **Pyetja 3** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë përfaqëson të dhënat në tranzit? → Paketa të dhënash që lëvizin nëpër router-ë dhe switch-e rrjeti

4 **Pyetja 4** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Pse është kritike një kopje rezervë offline e rregullt për mbrojtjen nga ransomware? → Ofron një kopje të pastër offline për rikthimin e skedarëve pa paguar shpërblim

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë bën tokenizimi i të dhënave? → Zëvendëson numrat e ndjeshëm të kartave me token-ë të rastësishëm jo të ndjeshëm

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Pyetja 6** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Maskimi i ndryshon kopjet e testimit ose i fsheh vlerat në kohën e kërkesës; regjistrat e prodhimit mbeten të pandryshuar.

7 **Pyetja 7** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Kopjet rezervë jashtë vendit duhet të izolohen nga rrjeti kryesor korporativ për të parandaluar përhapjen e ransomware-it.

8 **Pyetja 8** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Certifikatat TLS i mbrojnë të dhënat gjatë transmetimit; të dhënat në qetësi (at rest) kanë nevojë për enkriptim të diskut, skedarit ose bazës së të dhënave.

9 **Pyetja 9** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Zero-trust network access (ZTNA) verifikon identitetin e çdo përdoruesi para se t'i japë qasje në bazën e të dhënave.

10 **Pyetja 10** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Tokenizimi i bazuar në vault i ruan vlerat origjinale në një vault të sigurt tokenësh që e lidh çdo token me të dhënat e tij.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

B 1. ENKRIPTIM	A 2. KOPJE REZERVË	H 3. MINIMIZIM	F 4. QASJE
C 5. QËNDRIM	E 6. SHKELJE	D 7. PËRPUTHSHMËRI	G 8. MASKIM

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 MASKIM	2 NË PUSHIM	3 TRANZIT	4 QASJE
5 KOPJE SIGURIE	6 POSTURË SIGURIE		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 F – KOMPROMETIM	2 H – MASKIM	3 D – QASJE	4 E – POSTURËSIGURIE
5 G – PËRPUTHSHMËRI	6 C – MINIMIZIM	7 A – ENKRIPTIM	8 B – KOPJESIGURIE

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë ENKRIPTIM, KOPJE REZERVË dhe MINIMIZIM me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

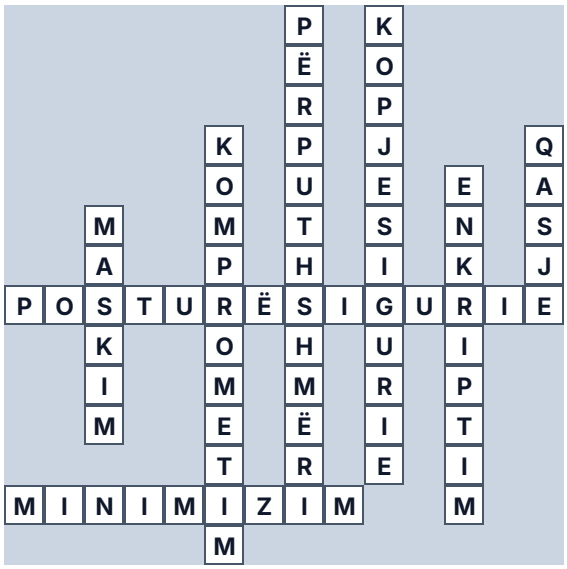
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

M	I	D	J	P	L	I	P	A	E	N	I	M	Ç	L
E	I	C	Ç	F	G	B	Ë	B	N	Q	K	O	U	S
I	G	K	Y	E	Y	Q	R	F	X	V	G	E	P	S
R	M	T	S	I	Q	Ç	P	S	R	K	O	J	L	R
U	G	I	O	A	G	Y	U	N	K	V	T	M	M	Y
G	P	P	B	A	M	J	T	N	L	B	J	I	G	Q
I	E	H	M	Y	B	Z	H	Z	Y	B	L	T	U	A
S	X	K	C	E	N	V	S	O	P	X	F	E	D	S
E	Y	C	V	K	E	F	H	F	Z	V	C	M	N	J
J	P	I	V	X	Q	J	M	Z	A	L	Q	O	Z	E
P	P	O	S	T	U	R	Ë	S	I	G	U	R	I	E
O	Q	K	Ë	R	V	Ë	R	J	V	H	B	P	Y	C
K	C	Y	M	I	T	P	I	R	K	N	E	M	N	T
Z	N	Z	T	S	B	G	U	O	X	C	L	O	K	G
M	I	Z	I	M	I	N	I	M	O	X	Y	K	Z	X

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

7 horizontalisht: POSTURËSIGURIE Gjendja kolektive e sigurisë dhe gatishmëria mbrojtëse e cloud-it të një organizate (14 shkronja)

8 horizontalisht: MINIMIZIM Kufizimi i mbledhjes së të dhënave personale në minimumin e nevojshëm për operacionet (9 shkronja)

VERTIKALISHT

1 vertikalisht: PËRPUTHSHMËRI Përmbushja e standardeve rregullatore si GDPR ose CCPA për menaxhimin e informacionit privat të përdoruesve (13 shkronja)

2 vertikalisht: KOPJESIGURIE Krijimi i kopjeve të sigurta jashtë vendit për rikthim në rast dështimi të sistemit (12 shkronja)

3 vertikalisht: KOMPROMETIM Incident sigurie ku të dhënat e mbrojtura aksesohen ose zbulohen pa autorizim (11 shkronja)

4 vertikalisht: QASJE Kufizimi i lejeve të leximit dhe shkrimit në bazën e të dhënave për rolet e autentikuara të përdoruesve (5 shkronja)

5 vertikalisht: ENKRIPTIM Shndërrimi i tekstit të qartë në tekst të shifruar të palexueshëm, që të dhënat e përgjuara të mbeten private (9 shkronja)

6 vertikalisht: MASKIM Zëvendësimi i karaktereve të ndjeshme në fushat e bazës së të dhënave për të mbrojtur identitetet personale (6 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. PIRNETIMK — **ENKRIPTIM**
2. MMIIIIZMN — **MINIMIZIM**
3. PIOISEGUSËURRT — **POSTURËSIGURIE**
4. TRHRSUIHËMPËP — **PËRPUTHSHMËRI**
5. ORGIEPEUSKIJ — **KOPJESIGURIE**
6. JQSEA — **QASJE**
7. ERKOMMTIMOP — **KOMPROMETIM**
8. SMMIKA — **MASKIM**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"MBROJ TË DHËNAT PRIVATE ME KONTROLLE TË SIGURTA"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Përmirësimi i enkriptimit në pushim të bazës së të dhënave të ndërmarrjes

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një shitës online i ruan bazat e të dhënave të transaksioneve në ruajtje cloud pa enkriptim të plotë të diskut. Një auditim i fundit i pajtueshmërisë e shënoi këtë si rrezik serioz për sigurinë e të dhënave sipas CCPA. Hartoje një arkitekturë rikuperimi.
- Strategjia dhe zgjidhja e rekomanduar: Zbato enkriptim AES-256 të plotë të diskut në qetësi në të gjitha sistemet e skedarëve. Përdor një Shërbim të centralizuar të Menaxhimit të Çelësave (KMS) me rotacion automatik dhe zbato politika të rrepta IAM për të kontrolluar qasjen në deshifrim.

B Studimi i rastit 2: Përmbajtja e ransomware-it dhe rikthimi i të dhënave

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një sulm aktiv ransomware po enkripton disqet e rrjetit në një rrjet lokal korporativ. Administratori e ka zbuluar infeksionin herët. Planifiko hapat e izolimit dhe rimëkëmbjes.
- Strategjia dhe zgjidhja e rekomanduar: Izolo menjëherë segmentin e kompromentuar. Formato pikat fundore të prekura dhe rikthe nga kopja rezervë më e fundit offline write-once-read-many (WORM). Verifiko integritetin e kopjes rezervë përpara se t'i rilidhësh sistemet.