Emri: _____ Data: _____ Pikët: _____

Sulmet ransomware dhe biznesi Rimëkëmbja

Ekzekutimi i ngarkesës, enkriptimi kriptografik i skedarëve, kopjet rezervë offline, procedurat e përmbajtjes dhe rikuperimi nga fatkeqësitë.

PËRMBLEDHJE MËSIMORE PËR SULMET RANSOMWARE

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 sulmeve ransomware dhe rimëkëmbjes së biznesit. Do të eksplorosh ekzekutimin e ngarkesës, enkriptimin e skedarëve, kopjet rezervë jashtë linje, përmbajtjen e kërcënimeve, pagesat me kriptomonedha dhe planet e rimëkëmbjes pas fatkeqësive.

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/sulm-ransomware/

Udhërrëfyesi yt mësimor për rimëkëmbjen nga ransomware

- Dallo mes ngarkesave të tipit Trojan, ransomware dhe spyware.
- Analizo skedarët keqdashës brenda mjediseve të sigurta sandbox.
- Formuloni procedura të shpejta izolimi dhe përmbajtjeje të rrjetit.

UDHËZIME PËR UDHËZUESIN E SULMEVE RANSOMWARE

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 rimëkëmbjen nga ransomware. Përfundo me aktivitetin bonus Mendo shpejt.

SULMET RANSOMWARE DHE RIKUPERIMI NGA FATKEQËSITË (HYRJE)

Ngarkesat e ransomware e bllokojnë në mënyrë kriptografike ruajtjen e sistemit, duke kërkuar pagesa me kriptovalutë për çelësat e dekriptimit. Zbutja e këtij kërcënimi përfshin rregulla izolimi të rrjetit, analizë malware-i në sandbox dhe kopjeruajtje të ftohta të fuqishme të izoluara nga rrjeti.

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 mekanizmi kryesor i një sulmi ransomware?

- A. Enkriptim kriptografik i skedarëve të përdoruesit për të mohuar qasjen në sistem
- B. Injektimi i komandave keqdashëse SQL në fushat e formularëve
- C. Përgjimi i paketave të rrjetit në një lidhje Wi-Fi publike
- D. Falsifikimi i kokave të email-it për të anashkaluar validimin SPF

2. Çfarë është një kopje rezervë offline (e ftohtë)?

- A. Një kopje ruajtjeje e shkëputur nga rrjeti për ta mbrojtur nga përhapja e malware-it
- B. Një kopje rezervë e ruajtur në hard diskun e serverit kryesor të uebit
- C. Një cache e përkohshme e logjeve të regjistrit të sistemit
- D. Një mjet administrativ i përdorur për të rivendosur fjalëkalimet e përdoruesve

3. Si duhet t'i izolojnë ekipet e sigurisë sistemet e infektuara gjatë një sulmi ransomware?

- A. Shkëput menjëherë kabllot e rrjetit dhe çaktivizo ndërfaqet wireless
- B. Përditëso bazën e të dhënave të nënshkrimeve të antivirusit
- C. Fikja e serverit parësor DNS
- D. Riemërtimi i shtesave të skedarëve të kompromentuar

4. Pse i këshillojnë agjencitë e sigurisë të mos paguhen kërkesat e ransomware-it?

- A. Pagesa e fondeve i inkurajon sulmuesit dhe nuk garanton dorëzimin e çelësit të deshifrimit
- B. Anulon automatikisht të gjitha policat e sigurimit të korporatës
- C. Njofton automatikisht çdo klient me email
- D. Korrupton skedarët e mbetur të kopjeve rezervë të sistemit

5. Çfarë është një plan rikuperimi pas fatkeqësisë (DRP)?

- A. Një proces i strukturuar për rikthimin e operacioneve dhe të dhënave pas kompromentimit të sistemit
- B. Një konfigurim firewall-i që harton portat hyrëse të rrjetit
- C. Një skemë e bazës së të dhënave që liston privilegjet administrative të përdoruesve
- D. Një protokoll autentikimi i email-it që refuzon domenet e falsifikuara

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

6 Pyetja 6

6. Ngarkesat e ransomware mund të përhapen lehtësisht te kopjeruajtjet online të lidhura me rrjetin.

- E vërtetë
- E gabuar

7 Pyetja 7

7. Pagesa e shpërblesës në kriptovalutë garanton që skedarët do të deshifrohen me sukses.

- E vërtetë
- E gabuar

8 Pyetja 8

8. Shkëputja e sistemeve të infektuara nga rrjeti ndihmon të ndalohet përhapja e ransomware-it në sistemet fqinje.

- E vërtetë
- E gabuar

9 Pyetja 9

9. Kriptografia simetrike nuk përdoret kurrë nga ransomware për të enkriptuar ruajtjen e sistemit.

- E vërtetë
- E gabuar

10 Pyetja 10

10. Testimi i rregullt i procedurave të rikthimit të të dhënave është një pjesë kritike e rimëkëmbjes nga katastrofa.

- 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. Mohimi i qasjes në skedarët lokalë përdor _____ kriptografik.
2. Kodi aktiv keqdashës i ekzekutuar në një sistem është _____ .
3. Kopjet e shkëputura të ruajtjes jashtë vendit përfaqësojnë një _____ të sigurt.
4. Ndalimi i përhapjes së malware-it kërkon _____ të rrjetit të pikave fundore.
5. Pagesa me kriptomonedhë e kërkuar nga kriminelët kibernetikë është _____ .
6. Rikthimi i skedarëve operativë të të dhënave përfaqëson _____ pas katastrofës.

BANKA E FJALËVE TË LEKSIKUT

ENKRIPTIM IZOLIM KATASTROFË KOPJE OFFLINE NGARKESË RIKUPERIM SHPËRBLIM TROJAN

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

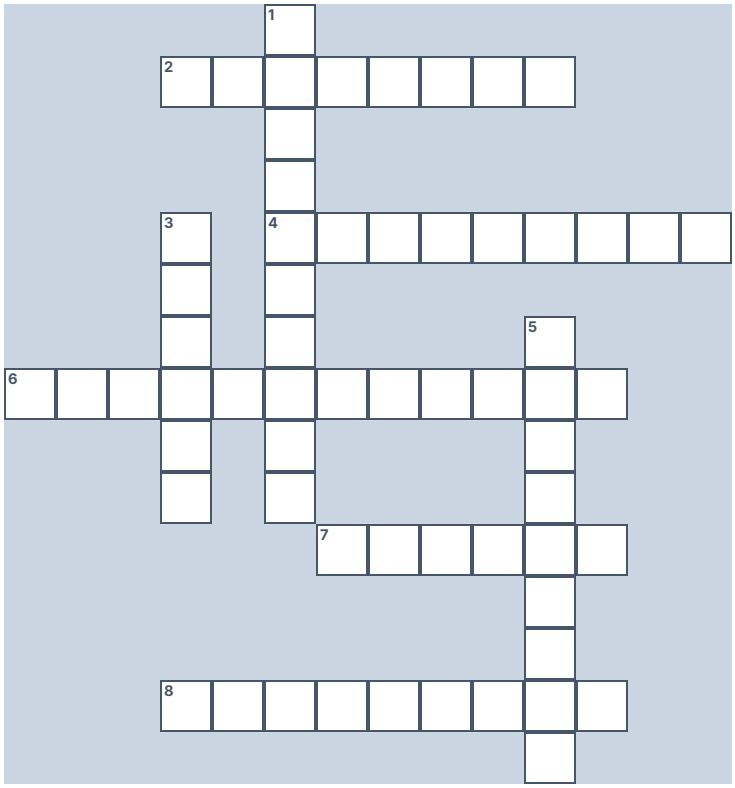
PËRPUTHJA E PËRKUFIZIMEVE

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	Shkëputja e sistemeve të rrjetit të infektuara.
☐	2. PËRMBAJTJE E PAKETËS	B	Skedar keqdashës i maskuar si i pastër.
☐	3. KOPJE REZERVË E FTOHTË	C	Kyçja e skedarëve në mënyrë kriptografike.
☐	4. IZOLIMI	D	Ngjarje e madhe ndërprerjeje të sistemit.
☐	5. SHPËRBLIM	E	Ekzekutimi i softuerit keqdashës.
☐	6. RIKUPERIM	F	Kopje offline e shkëputur.
☐	7. FATKEQËSI	G	Rikthimi i bazës së të dhënave nga kopja rezervë.
☐	8. KALI I TROJËS	H	Kërkesë pagese e çelësit kriptografik.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

2. Ekzekutimi i softuerit keqdashës. (8)

4. Kërkesë pagese për çelësin kriptografik. (9)

6. Kopje e shkëputur jashtë linje. (12)

7. Shkëputja e sistemeve të infektuara të rrjetit. (6)

8. Rikthimi i bazës së të dhënave nga kopja rezervë. (9)

VERTIKALISHT

1. Ngjarje e madhe ndërprerjeje e sistemit. (10)

3. Skedar keqdashës i maskuar si i pastër. (6)

5. Kyçja e skedarëve në mënyrë kriptografike. (9)

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

2 horizontalisht: Ekzekutimi i softuerit keqdashës. (8 shkronja):

4 horizontalisht: Kërkesë pagese për çelësin kriptografik. (9 shkronja):

6 horizontalisht: Kopje e shkëputur jashtë linje. (12 shkronja):

7 horizontalisht: Shkëputja e sistemeve të infektuara të rrjetit. (6 shkronja):

8 horizontalisht: Rikthimi i bazës së të dhënave nga kopja rezervë. (9 shkronja):

VERTIKALISHT

1 vertikalisht: Ngjarje e madhe ndërprerjeje e sistemit. (10 shkronja):

3 vertikalisht: Skedar keqdashës i maskuar si i pastër. (6 shkronja):

5 vertikalisht: Kyçja e skedarëve në mënyrë kriptografike. (9 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.

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

LISTA E FJALËVE TË LEKSIKUT

ENKRIPTIM, NGARKESË, KOPJEOFFLINE, IZOLIM, SHPËRBLIM, RIKUPERIM, KATASTROFË, TROJAN

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. NGARKESË

C. KOPJEOFFLINE

D. IZOLIM

E. SHPËRBLIM

F. RIKUPERIM

G. KATASTROFË

H. TROJAN

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Kopje e shkëputur jashtë linje.
2. Skedar keqdashës i maskuar si i pastër.
3. Kyçja e skedarëve në mënyrë kriptografike.
4. Kërkesë pagese për çelësin kriptografik.
5. Shkëputja e sistemeve të infektuara të rrjetit.
6. Ngjarje e madhe ndërprerjeje e sistemit.
7. Ekzekutimi i softuerit keqdashës.
8. Rikthimi i bazës së të dhënave nga kopja rezervë.

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. **EOEOKINPFLFJ** _____

3. **SBRHLMËIP** _____

4. **TFSËAORKAT** _____

5. **KEGËRNSA** _____

6. **ILIOMZ** _____

7. **ERIMRUIPK** _____

8. **ONTAJR** _____

Aktivitet bonus: Mendo shpejt

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

1	Informacione që nuk duhet t'i ndash kurrë			
2	Pajisje që mund të hakohen			
3	Arsye për të mos paguar një shpërblim			
4	Zakone të sigurta që mund t'i fillosh sot			
5	Mjete sigurie që njeh			
6	Mënyra për të mbrojtur llogaritë e tua			
7	Shenja që një kompjuter është i infektuar			
8	Vende ku mund të mbash një kopje rezervë			
9	Skedarë që nuk dëshiron t'i humbasësh kurrë			
10	Mënyra si përhapet ransomware-i			
11	Gjëra që bëhen në orën e parë të një sulmi			
12	Njerëz që duhen kontaktuar gjatë një sulmi			
13	Gjëra që mund t'i kyçë ransomware-i			
14	Fjalë që lidhen me sigurinë kibernetike			
15	Organizata që shpesh bëhen objektiv			

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: PËRMBAJTJA E NGARKESËS RANSOMWARE NË NDËRMARRJE

👷

Skenari: Një rrjet lokal korporativ është shkelur nga ransomware aktiv. Serverët kryesorë të skedarëve kanë filluar të shfaqin shtesa skedarësh me .locked.

Pyetje për diskutim: Përshkruaj në detaje hapat e izolimit dhe përshkruaj protokollin e rikuperimit të të dhënave.

STUDIMI I RASTIT 2: VLERËSIMI I ARKITEKTURAVE TË KOPJEVE REZERVË JASHTË LINJE

👷

Skenari: Një ndërmarrje dëshiron të hartojë një strategji kopjesh rezervë të të dhënave që e zvogëlon rrezikun e kompromentimit të kopjeve rezervë, edhe nëse rrjeti kryesor lokal rrëmbehet plotësisht nga ransomware.

Pyetje për diskutim: Harto një sistem të sigurt kasafortë offline për ruajtjen e kopjeve rezervë.

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

20 11 13 22 10 6 21 11 21 22 6 15 11 16 6

6 16 13 20 11 18 22 23 1 20 16 9 1 13 17 18 12 1

17 8 8 14 11 16 6

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 ransomware-i?

Ransomware është softuer keqdashës i krijuar për të bllokuar aksesin në sistemet kompjuterike ose skedarët derisa të paguhet një shumë shpërblimi.

Q2: Si përhapet ransomware-i?

Përmes bashkëngjitjeve phishing në email, cenueshmërive të softuerit të paarnuar dhe sistemeve të kompromentuara të qasjes në distancë. [1]

Q3: Pse kërkohet pagesa në kriptovalutë?

Kriptovalutat si Bitcoin ofrojnë anonimitet relativ, duke e bërë të vështirë për zbatimin e ligjit të gjurmojë fondet.

Q4: A e bllokon antivirusi ransomware-in?

Po, por antivirusi i bazuar në nënshkrime mund të dështojë ndaj ngarkesave të reja zero-day të ransomware-it.

Q5: Çfarë është një kopjeruajtje e izoluar nga rrjeti (air-gapped)?

Një kopje rezervë që nuk ka lidhje fizike ose logjike me rrjetin kryesor, duke e mbrojtur nga përhapja.

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 shantazhi i dyfishtë (double extortion)?

Kur sulmuesit jo vetëm enkriptojnë skedarët, por vjedhin edhe të dhëna të ndjeshme për të kërcënuar me rrjedhje publike nëse nuk paguhet.

Q7: Çfarë është një dekriptues (decryptor)?

Një mjet softuerik që përmban çelësin kriptografik të nevojshëm për t'i kthyer skedarët e kyçur në tekst të thjeshtë.

Q8: Si ta zbulosh ransomware herët?

Duke monitoruar sistemet e skedarëve për modifikime të papritura e masive të skedarëve dhe aktivitet riemërtimi.

Q9: Cili është roli i sigurimit?

Sigurimi kibernetik mund të ndihmojë në mbulimin e kostove të rikuperimit, por kushtet e mbulimit dhe rregullat e pagesës së shpërblimit ndryshojnë sipas policës.

Q10: A duhet ta rinis një sistem të infektuar?

Jo, rindezja mund të shkatërrojë dëshmitë në memorien e paqëndrueshme; izoloje nga rrjeti në vend të kësaj. [1]

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 e përdor ransomware-i enkriptimin asimetrik?

Përdor një çelës publik të ngulitur në malware për të enkriptuar skedarët, duke kërkuar çelësin privat të sulmuesit për t'i dekriptuar.

Q2: Pse përdoret edhe enkriptimi simetrik?

Enkriptimi simetrik (si AES) është i shpejtë dhe mund të kyçë baza të dhënash shumë të mëdha për pak minuta, ndërsa çelësat asimetrikë e sigurojnë çelësin AES.

Q3: Çfarë është segmentimi logjik?

Ndarja e rrjeteve në zona të izoluara, që e pengon malware-in të përhapet anësisht nga nyjet e stacioneve të punës te serverët kryesorë.

Q4: Çfarë është ruajtja WORM?

Media Write-Once, Read-Many, që pengon redaktimin, mbishkrimin ose fshirjen e të dhënave të kopjeve rezervë nga ngarkesat e ransomware-it.

Q5: Çfarë janë shadow copies?

Pamje rezervë lokale të krijuara nga Windows; ransomware zakonisht i fshin këto të parat duke përdorur mjete administrative.

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: Si e mundëson vjedhja e kredencialeve ransomware-in?

Sulmuesit blejnë kredenciale të rrjedhura të administratorit për t'u kyçur përmes desktopëve në distancë, duke ekzekutuar manualisht ransomware në të gjithë rrjetin.

Q7: Çfarë është testimi i restaurimit me provë (dry-run)?

Rikthimi i rregullt i bazave të të dhënave rezervë në mjedise testimi të izoluara për të verifikuar që shpejtësia e rikthimit dhe integriteti i të dhënave plotësojnë metrikat e rimëkëmbjes nga katastrofa.

Q8: Si e ndalon ransomware zbulimi dhe reagimi në pikën fundore (EDR)?

Duke analizuar sjelljen e proceseve (p.sh. enkriptimin e shpejtë) dhe duke pezulluar shpejt aplikacionin e dyshimtë.

Q9: Çfarë është modeli ransomware-as-a-service (RaaS)?

Një model franshize ku zhvilluesit e malware-it u japin me qira ndërtuesit e ransomware-it filialeve në këmbim të një përqindjeje të pagesave.

Q10: Si e shkakton ransomware-in një RDP i papaçuar?

Portat hyrëse të ekspozuara të Remote Desktop Protocol, pa përditësime, u lejojnë sulmuesve të marrin me forcë të ashpër hyrjet dhe të nisin manualisht malware.

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

Aktorët e ransomware shpesh përdorin mjete si vssadmin.exe për të fshirë shadow copies të Windows dhe për të bllokuar rikthimet lokale. [1]

2. PERSPEKTIVË PËR SIGURINË

Çelësat simetrikë AES-256 zakonisht përdoren për të enkriptuar ngarkesat e skedarëve, të cilat më pas kyçen me çelësa publikë RSA.

3. PERSPEKTIVË PËR SIGURINË

Rimëkëmbja nga një sulm i suksesshëm ransomware mund të zgjasë javë, prandaj kopjet rezervë offline të testuara kanë rëndësi.

4. PERSPEKTIVË PËR SIGURINË

FBI nuk mbështet pagimin e shpërblesës dhe paralajmëron se pagesa nuk garanton që do t'i marrësh të dhënat mbrapsht. [2]

5. PERSPEKTIVË PËR SIGURINË

Planet e rimëkëmbjes pas fatkeqësive (DRP) duhet të përcaktojnë një Objektiv të Kohës së Rimëkëmbjes (RTO) dhe një Objektiv të Pikës së Rimëkëmbjes (RPO).

6. PERSPEKTIVË PËR SIGURINË

FBI rekomandon kopje rezervë të enkriptuara dhe të pandryshueshme, domethënë që nuk mund të ndryshohen ose fshihen. [3]

7. NJOHURI PËR SIGURINË

Zhvilluesit e ransomware përdorin teknika të avancuara errësimi për të anashkaluar skanerët tradicionalë të antivirusit të bazuar në nënshkrime.

8. NJOHURI PËR SIGURINË

Segmentimi i rrjetit e kufizon lëvizjen anësore, duke ndihmuar ndalimin e përhapjes së ransomware-it përtej hostit të parë të infektuar. [3]

9. NJOHURI PËR SIGURINË

Shërbimet në distancë të ekspozuara dhe të mbrojtura dobët, si Remote Desktop Protocol (RDP), janë një pikë e zakonshme hyrjeje për ransomware. [1]

10. PERSPEKTIVË PËR SIGURINË

CISA rekomandon mbajtjen e kopjeve rezervë të enkriptuara jashtë linje, pasi shumë variante të ransomware-it kërkojnë dhe fshijnë kopjet rezervë të arritshme. [1]

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] 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

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

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

SHËNIM PËR MËSUESIN

Cili është mekanizmi kryesor i një sulmi ransomware? → Enkriptim kriptografik i skedarëve të përdoruesit për të mohuar qasjen në sistem

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

SHËNIM PËR MËSUESIN

Çfarë është një kopje rezervë offline (e ftohtë)? → Një kopje ruajtjeje e shkëputur nga rrjeti për ta mbrojtur nga përhapja e malware-it

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

SHËNIM PËR MËSUESIN

Si duhet t'i izolojnë ekipet e sigurisë sistemet e infektuara gjatë një sulmi ransomware? → Shkëput menjëherë kabllot e rrjetit dhe çaktivizo ndërfaqet wireless

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

SHËNIM PËR MËSUESIN

Pse i këshillojnë agjencitë e sigurisë të mos paguhen kërkesat e ransomware-it? → Pagesa e fondeve i inkurajon sulmuesit dhe nuk garanton dorëzimin e çelësit të deshifrimit

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

SHËNIM PËR MËSUESIN

Çfarë është një plan rikuperimi pas fatkeqësisë (DRP)? → Një proces i strukturuar për rikthimin e operacioneve dhe të dhënave pas kompromentimit të sistemit

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

6 **Pyetja 6** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Ngarkesat e ransomware mund të përhapen lehtësisht te kopjeruajtjet online të lidhura me rrjetin.

7 **Pyetja 7** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: FBI paralajmëron se pagesa nuk garanton që do t'i marrësh ndonjëherë të dhënat prapa.

8 **Pyetja 8** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

E vërtetë: CISA këshillon shkëputjen e hosteve të infektuar ose nxjerrjen e rrjetit jashtë linje për të frenuar përhapjen.

9 **Pyetja 9** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: ransomware zakonisht i enkripton skedarët me shifra simetrike të shpejta si AES.

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

SHËNIM PËR MËSUESIN

Testimi i rregullt i procedurave të rikthimit të të dhënave është një pjesë kritike e rimëkëmbjes nga katastrofa.

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

C 1. ENKRIPTIM	E 2. PËRMBAJTJE E PAKETËS	F 3. KOPJE REZERVË E FTOHTË	A 4. IZOLIMI
H 5. SHPËRBLIM	G 6. RIKUPERIM	D 7. FATKEQËSI	B 8. KALI I TROJËS

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 ENKRIPTIM	2 NGARKESË	3 KOPJE OFFLINE	4 IZOLIM
5 SHPËRBLIM	6 RIKUPERIM		

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

1 C – KOPJEOFFLINE	2 H – TROJAN	3 A – ENKRIPTIM	4 E – SHPËRBLIM
5 D – IZOLIM	6 G – KATASTROFË	7 B – NGARKESË	8 F – RIKUPERIM

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë ENKRIPTIM, PËRMBAJTJE E PAKETËS dhe KOPJE REZERVË E FTOHTË 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.

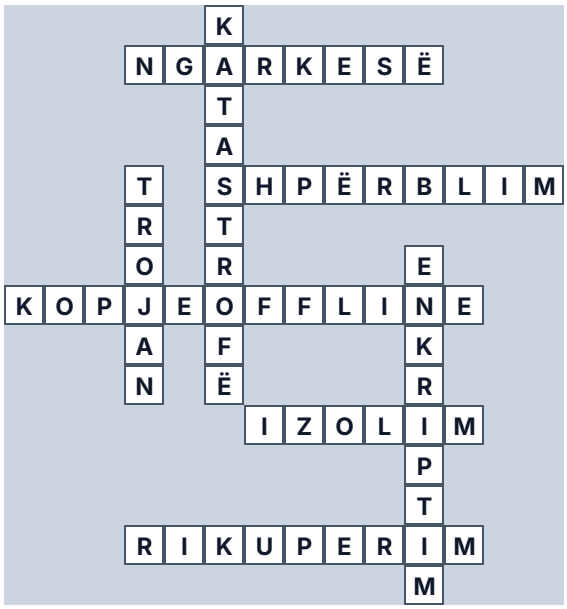
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

2 horizontalisht: NGARKESË Ekzekutimi i softuerit keqdashës. (8 shkronja)

4 horizontalisht: SHPËRBLIM Kërkesë pagese për çelësin kriptografik. (9 shkronja)

6 horizontalisht: KOPJEOFFLINE Kopje e shkëputur jashtë linje. (12 shkronja)

7 horizontalisht: IZOLIM Shkëputja e sistemeve të infektuara të rrjetit. (6 shkronja)

8 horizontalisht: RIKUPERIM Rikthimi i bazës së të dhënave nga kopja rezervë. (9 shkronja)

VERTIKALISHT

1 vertikalisht: KATASTROFË Ngjarje e madhe ndërprerjeje e sistemit. (10 shkronja)

3 vertikalisht: TROJAN Skedar keqdashës i maskuar si i pastër. (6 shkronja)

5 vertikalisht: ENKRIPTIM Kyçja e skedarëve në mënyrë kriptografike. (9 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	5.	KEGËRNSA	NGARKESË
2.	EOEOKINPFLFJ	KOPJEOFFLINE	6.	ILIOMZ	IZOLIM
3.	SBRHLMËIP	SHPËRBLIM	7.	ERIMRUIPK	RIKUPERIM
4.	TFSËAORKAT	KATASTROFË	8.	ONTAJR	TROJAN

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"RIKTHE SISTEMIN E ENKRIPTUAR NGA KOPJA OFFLINE"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Përmbajtja e ngarkesës ransomware në ndërmarrje

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një rrjet lokal korporativ është shkelur nga ransomware aktiv. Serverët kyç të skedarëve kanë nisur të shfaqin shtesa skedarësh me .locked.
- Strategjia dhe zgjidhja e rekomanduar: Shkëput të gjithë serverët e prekur nga rrjeti lokal. Mbyll seancat aktive administrative. Rikthe skedarët e pakompromentuar nga një sistem i sigurt kopjeruajtjeje offline, i mbyllur për shkrim.

B Studimi i rastit 2: Vlerësimi i arkitekturave të kopjeve rezervë jashtë linje

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një ndërmarrje dëshiron të hartojë një strategji kopjeruajtjeje që zvogëlon rrezikun e kompromentimit të kopjeve rezervë edhe nëse rrjeti lokal kryesor kapet plotësisht nga ransomware.
- Strategjia dhe zgjidhja e rekomanduar: Zbato ruajtje write-once-read-many (WORM). Krijo një air-gap logjik duke e shkëputur sistemin e kopjeve rezervë nga të gjitha rrjetet dhe zbato rotacion ditor të medias fizike.