Nume: _____ **Data:** _____ **Punctaj:** _____

Atacuri ransomware și afaceri Recuperare

Execuția sarcinii utile, criptarea fișierelor, copiile de rezervă offline, procedurile de izolare și recuperarea în caz de dezastru.

PREZENTARE GENERALĂ DE ÎNVĂȚARE DESPRE ATACURILE RANSOMWARE

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin atacurile ransomware și recuperarea afacerii. Vei explora execuția sarcinii utile, criptarea fișierelor, copiile de rezervă offline, izolarea amenințărilor, plățile în criptomonede și planurile de recuperare în caz de dezastru.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/atac-ransomware/

Harta ta de învățare despre recuperarea după ransomware

- Diferențiază payload-urile de tip troian, ransomware și spyware.
- Analizează fișierele rău intenționate în medii sandbox securizate.
- Elaborează proceduri rapide de izolare și limitare a rețelei.

INSTRUCȚIUNI DIN GHIDUL DESPRE ATACURILE RANSOMWARE

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre recuperarea în urma ransomware-ului. Încheie cu activitatea bonus Gândește repede.

ATACURI RANSOMWARE ȘI RECUPERAREA DUPĂ DEZASTRE (INTRODUCERE)

Sarcinile utile ransomware blochează criptografic stocarea sistemului, cerând plăți în criptomonede pentru cheile de decriptare. Atenuarea acestei amenințări presupune reguli de izolare a rețelei, analiza software-ului rău intenționat în sandbox și copii de siguranță robuste, offline (air-gapped).

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Care este mecanismul principal al unui atac ransomware?

- A. Criptarea criptografică a fișierelor utilizatorului pentru a refuza accesul la sistem
- B. Injectarea de comenzi SQL rău intenționate în câmpurile de formular
- C. Interceptarea pachetelor de rețea într-o conexiune Wi-Fi publică
- D. Falsificarea antetelor e-mailului pentru a ocoli validarea SPF

2. Ce este o copie de rezervă offline (rece)?

- A. O copie de stocare deconectată de la rețea pentru a o proteja de propagarea malware-ului
- B. O copie de rezervă stocată pe hard disk-ul serverului web principal
- C. Un cache temporar al jurnalelor registrului de sistem
- D. Un instrument administrativ folosit pentru resetarea parolelor utilizatorilor

3. Cum ar trebui să izoleze echipele de securitate sistemele infectate în timpul unui atac ransomware?

- A. Deconectează imediat cablurile de rețea și dezactivează interfețele wireless
- B. Actualizarea bazei de date cu semnături antivirus
- C. Oprește serverul DNS principal
- D. Redenumește extensiile fișierelor compromise

4. De ce sfătuiesc agențiile de securitate să nu se plătească cererile ransomware?

- A. Plata fondurilor încurajează atacatorii și nu garantează livrarea cheii de decriptare
- B. Invalidează automat toate polițele de asigurare corporative
- C. Notifică automat fiecare client prin e-mail
- D. Corupe fișierele de backup rămase ale sistemului

5. Ce este un plan de recuperare în caz de dezastru (DRP)?

- A. Un proces structurat de restabilire a operațiunilor și a datelor după compromiterea sistemului
- B. O configurație de firewall care mapează porturile de rețea de intrare
- C. O schemă de bază de date care listează privilegiile administrative ale utilizatorilor
- D. Un protocol de autentificare a e-mailului care respinge domeniile falsificate

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Sarcinile utile ransomware se pot propaga ușor către copiile de siguranță online conectate la rețea.

- ◯ Adevărat
- ◯ Fals

7 Întrebare 7

7. Plata răscumpărării în criptomonedă garantează că fișierele vor fi decriptate cu succes.

- ◯ Adevărat
- ◯ Fals

8 Întrebare 8

8. Deconectarea sistemelor infectate de la rețea ajută la oprirea răspândirii ransomware-ului către sistemele adiacente.

- ◯ Adevărat
- ◯ Fals

9 Întrebare 9

9. Criptografia simetrică nu este niciodată folosită de ransomware pentru a cripta stocarea sistemului.

- ◯ Adevărat
- ◯ Fals

10 Întrebare 10

10. Testarea periodică a procedurilor de restaurare a datelor este o parte esențială a recuperării în caz de dezastru.

- ◯ Adevărat
- ◯ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Refuzul accesului la fișierele locale folosește o _____ criptografică.
2. Codul rău intenționat activ executat pe un sistem este _____ .
3. Copiile de stocare deconectate, aflate în afara sediului, reprezintă un _____ sigur.
4. Oprirea răspândirii malware-ului necesită o _____ a rețelei endpoint-urilor.
5. Plata în criptomonedă pe care o cer infractorii cibernetici se numește _____ .
6. Restaurarea fișierelor de date operaționale reprezintă o _____ în caz de dezastru.

BANCĂ DE CUVINTE DIN VOCABULAR

BACKUP OFFLINE | CRIPTARE | DEZASTRU | IZOLARE | PAYLOAD | RĂSCUMPĂRARE | RECUPERARE | TROJAN

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre securitate

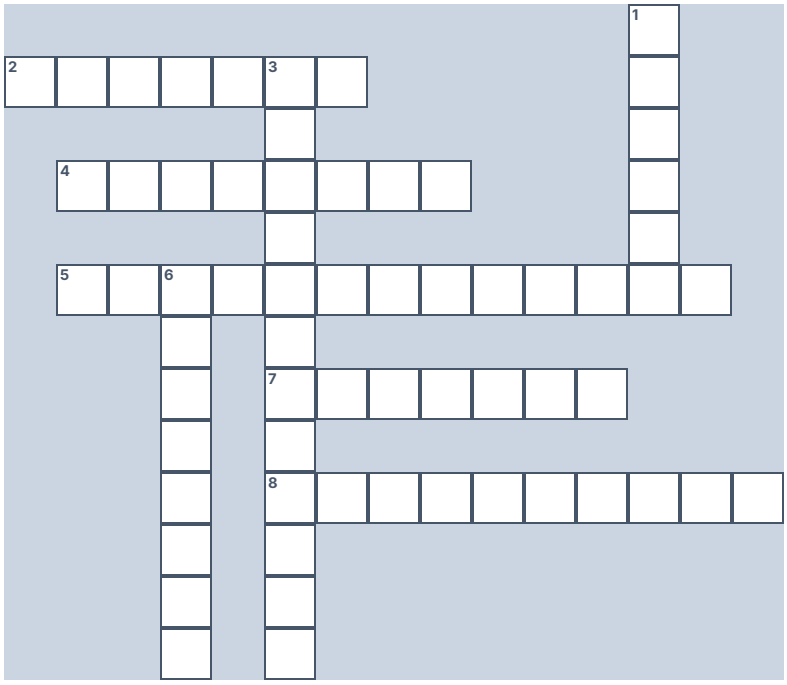
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. CRIPTARE	A	Deconectarea sistemelor de rețea infectate.
☐	2. SARCINĂ UTILĂ	B	Fișier rău intenționat deghizat în fișier curat.
☐	3. BACKUP LA RECE	C	Blocarea fișierelor prin criptare.
☐	4. IZOLARE	D	Eveniment major de perturbare a sistemului.
☐	5. RĂSCUMPĂRARE	E	Executarea de software rău intenționat.
☐	6. RECUPERARE	F	Copie offline deconectată.
☐	7. DEZASTRU	G	Restaurarea bazei de date din copia de rezervă.
☐	8. TROIAN	H	Cerere de plată a unei chei criptografice.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

2. Deconectarea sistemelor de rețea infectate. (7)

4. Eveniment major de perturbare a sistemului. (8)

5. Copie deconectată, offline. (13)

7. Executarea software-ului rău intenționat. (7)

8. Restaurarea bazei de date din copia de rezervă. (10)

VERTICAL

1. Fișier rău intenționat deghizat în fișier curat. (6)

3. Cerere de plată pentru cheia criptografică. (12)

6. Blocarea criptografică a fișierelor. (8)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

2 orizontal: Deconectarea sistemelor de rețea infectate. (7 litere):

4 orizontal: Eveniment major de perturbare a sistemului. (8 litere):

5 orizontal: Copie deconectată, offline. (13 litere):

7 orizontal: Executarea software-ului rău intenționat. (7 litere):

8 orizontal: Restaurarea bazei de date din copia de rezervă. (10 litere):

VERTICAL

1 vertical: Fișier rău intenționat deghizat în fișier curat. (6 litere):

3 vertical: Cerere de plată pentru cheia criptografică. (12 litere):

6 vertical: Blocarea criptografică a fișierelor. (8 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

E I S Z Ș E R R U D A A R O M
R U P T X Q Î E S T C S B M Y
A R N Ă F S W C W Î R A R Z Y
R T A Y I K F U I M I R Î L L
Ă S J T Z O G P Q Q P G Z A O
P A O U O F Ț E Â Y T S Y Ă G
M Z R L L Z F R Î N A P N W Â
U E T L A Z Y A F X R O V Ț J
C D U P R Ă N R U T E L G U B
S X Ț J E R Ă E W Z X L S Q W
Ă B A C K U P O F F L I N E H
R O C A B Î Q V W W K I H T H
F Ă P A Y L O A D D I J Ș S V
R Z D H D S Â A K Q Â Z L J U
S Ț A S W Î L L G H M H R F K

LISTĂ DE CUVINTE DIN VOCABULAR

CRIPTARE PAYLOAD BACKUPOFFLINE IZOLARE RĂSCUMPĂRARE RECUPERARE DEZASTRU TROJAN

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR
A. CRIPTARE
B. PAYLOAD
C. BACKUPOFFLINE
D. IZOLARE
E. RĂSCUMPĂRARE
F. RECUPERARE
G. DEZASTRU
H. TROJAN

	DEFINIȚII ȘI CÂMPURI DE ASOCIERE
	1. Copie deconectată, offline.
	2. Fișier rău intenționat deghizat în fișier curat.
	3. Blocarea criptografică a fișierelor.
	4. Cerere de plată pentru cheia criptografică.
	5. Deconectarea sistemelor de rețea infectate.
	6. Eveniment major de perturbare a sistemului.
	7. Executarea software-ului rău intenționat.
	8. Restaurarea bazei de date din copia de rezervă.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. **RPTCAREI** _____
2. **NUAPCBIOEFLFK** _____
3. **RĂĂPRRSMEUAC** _____
4. **ARUTSDEZ** _____
5. **ODLYPAA** _____
6. **ROAILEZ** _____
7. **EURREAREPC** _____
8. **ONTAJR** _____

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Informații pe care nu ar trebui să le dai niciodată			
2	Dispozitive care pot fi sparte			
3	Motive pentru care să nu plătești o răscumpărare			
4	Obiceiuri sigure pe care le poți începe de azi			
5	Instrumente de securitate pe care le cunoști			
6	Moduri de a-ți proteja conturile			
7	Semne că un calculator este infectat			
8	Locuri în care poți păstra o copie de rezervă			
9	Fișiere pe care nu vrei să le pierzi niciodată			
10	Moduri în care se răspândește ransomware-ul			
11	Lucruri de făcut în prima oră a unui atac			
12	Persoane pe care le contactezi în timpul unui atac			
13	Lucruri pe care le poate bloca ransomware-ul			
14	Cuvinte legate de securitatea cibernetică			
15	Organizații care sunt adesea vizate			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: LIMITAREA ÎNCĂRCĂTURII UNUI RANSOMWARE ÎNTR-O ORGANIZAȚIE



Scenariu: O rețea locală corporativă a fost compromisă de un ransomware activ. Serverele de fișiere cheie au început să afișeze fișiere cu extensia .locked.

Întrebare de discuție: Detaliază pașii de izolare și descrie pe scurt protocolul de recuperare a datelor.

STUDIU DE CAZ 2: EVALUAREA ARHITECTURILOR DE BACKUP OFFLINE



Scenariu: O companie vrea să proiecteze o strategie de backup a datelor care să reducă riscul ca backup-urile să fie compromise, chiar dacă rețeaua locală principală este complet preluată de ransomware.

Întrebare de discuție: Proiectează un sistem securizat de seif pentru stocarea copiilor de rezervă offline.

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

21	7	22	24	1	26	21	7	1	31	2		6	1	24	7	15	7
5	21	11	19	24	1	24	7		6	11	17		4	1	5	14	26	19
18	8	8	15	11	17	7											

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: Ce este ransomware-ul?

Ransomware-ul este software rău intenționat conceput pentru a bloca accesul la sisteme informatice sau la fișiere până la plata unei sume de răscumpărare.

Q2: Cum se răspândește ransomware-ul?

Prin atașamente de phishing din e-mail, vulnerabilități ale software-ului nepatch-uit și sisteme de acces la distanță compromise. [1]

Q3: De ce se cere plata în criptomonede?

Criptomonedele precum Bitcoin oferă un anonimat relativ, ceea ce face dificilă urmărirea fondurilor de către autorități.

Q4: Blochează antivirusul ransomware-ul?

Da, dar antivirusul bazat pe semnături poate eșua în fața unor încărcături ransomware zero-day nou create.

Q5: Ce este o copie de siguranță izolată fizic (air-gapped)?

O copie de rezervă fără nicio legătură fizică sau logică cu rețeaua principală, ceea ce o protejează de răspândire.

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Ce este dubla extorcare?

Atunci când atacatorii nu doar criptează fișierele, ci și fură date sensibile pentru a amenința cu divulgarea publică dacă nu se plătește.

Q7: Ce este un decriptor?

Un utilitar software care conține cheia criptografică necesară pentru a restaura fișierele blocate la text clar.

Q8: Cum detectezi ransomware-ul din timp?

Prin monitorizarea sistemelor de fișiere pentru activitate bruscă și masivă de modificare și redenumire a fișierelor.

Q9: Care este rolul asigurării?

Asigurarea cibernetică poate ajuta la acoperirea costurilor de recuperare, dar condițiile de acoperire și regulile privind plata răscumpărării diferă de la o poliță la alta.

Q10: Ar trebui să repornesc un sistem infectat?

Nu, repornirea poate distruge dovezile din memoria volatilă; izolează în schimb dispozitivul de rețea. [1]

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum folosește ransomware-ul criptarea asimetrică?

Folosește o cheie publică încorporată în malware pentru a cripta fișierele, fiind necesară cheia privată a atacatorului pentru a le decripta.

Q2: De ce se folosește și criptarea simetrică?

Criptarea simetrică (precum AES) este rapidă și poate bloca baze de date uriașe în câteva minute, în timp ce cheile asimetrice securizează cheia AES.

Q3: Ce este segmentarea logică?

Împărțirea rețelelor în zone izolate, care împiedică software-ul rău intenționat să se propage lateral de la stațiile de lucru către serverele de bază.

Q4: Ce este stocarea WORM?

Suport Write-Once, Read-Many, care împiedică editarea, suprascrierea sau ștergerea datelor de rezervă de către încărcăturile ransomware.

Q5: Ce sunt copiile umbră (shadow copies)?

Instantanee locale de backup create de Windows; ransomware-ul le șterge de obicei primele, folosind instrumente administrative.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: Cum permite furtul de acreditări atacurile ransomware?

Atacatorii cumpără date de autentificare de administrator scurse pentru a se conecta prin desktop-uri la distanță și a executa manual ransomware în rețea.

Q7: Ce este testarea restaurării prin simulare (dry-run)?

Restaurarea periodică a bazelor de date din copii de rezervă în medii de testare izolate, pentru a verifica dacă viteza de restaurare și integritatea datelor respectă indicatorii de recuperare în caz de dezastru.

Q8: Cum oprește detecția la nivel de endpoint (EDR) ransomware-ul?

Prin analiza comportamentului proceselor (de exemplu, criptarea rapidă) și suspendarea rapidă a aplicației necontrolate.

Q9: Ce este un model ransomware-as-a-service (RaaS)?

Un model de tip franciză în care dezvoltatorii de malware închiriază generatoare de ransomware afiliaților, în schimbul unui procent din plăți.

Q10: Cum declanșează RDP nepatch-uit ransomware?

Gateway-urile Remote Desktop Protocol expuse și neactualizate le permit atacatorilor să forțeze prin încercări repetate (brute-force) datele de autentificare și să lanseze manual software rău intenționat.

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

Atacatorii ransomware folosesc adesea instrumente precum vssadmin.exe pentru a șterge copiile umbră Windows și a bloca restaurările locale. [1]

2. INFORMAȚII DESPRE SECURITATE

Cheile simetrice AES-256 sunt de obicei folosite pentru a cripta conținutul fișierelor, care sunt apoi blocate cu chei publice RSA.

3. INFORMAȚII DESPRE SECURITATE

Recuperarea în urma unui atac ransomware reușit poate dura săptămâni, motiv pentru care copiile de rezervă offline testate contează.

4. INFORMAȚII DESPRE SECURITATE

FBI nu sprijină plata unei răscumpărări și avertizează că plata nu garantează că îți vei recupera datele. [2]

5. INFORMAȚII DESPRE SECURITATE

Planurile de recuperare în caz de dezastru (DRP) ar trebui să definească un obiectiv de timp de recuperare (RTO) și un obiectiv de punct de recuperare (RPO).

6. INFORMAȚII DESPRE SECURITATE

FBI recomandă copii de siguranță criptate și imuabile, adică ce nu pot fi modificate sau șterse. [3]

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Dezvoltatorii de ransomware folosesc tehnici avansate de ofuscare pentru a ocoli scanerele antivirus tradiționale bazate pe semnături.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Segmentarea rețelei restricționează mișcarea laterală, ajutând la oprirea răspândirii ransomware-ului dincolo de prima gazdă infectată. [3]

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Serviciile la distanță expuse și slab securizate, precum Remote Desktop Protocol (RDP), reprezintă un punct frecvent de intrare pentru ransomware. [1]

10. INFORMAȚII DESPRE SECURITATE

CISA recomandă păstrarea offline a copiilor de rezervă criptate, deoarece multe variante de ransomware caută și șterg copiile de rezervă accesibile. [1]

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[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

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Care este mecanismul principal al unui atac ransomware? → Criptarea criptografică a fișierelor utilizatorului pentru a refuza accesul la sistem

2 Întrebarea 2 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este o copie de rezervă offline (rece)? → O copie de stocare deconectată de la rețea pentru a o proteja de propagarea malware-ului

3 Întrebarea 3 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Cum ar trebui să izoleze echipele de securitate sistemele infectate în timpul unui atac ransomware? → Deconectează imediat cablurile de rețea și dezactivează interfețele wireless

4 Întrebarea 4 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

De ce sfătuiesc agențiile de securitate să nu se plătească cererile ransomware? → Plata fondurilor încurajează atacatorii și nu garantează livrarea cheii de decriptare

5 Întrebarea 5 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este un plan de recuperare în caz de dezastru (DRP)? → Un proces structurat de restabilire a operațiunilor și a datelor după compromiterea sistemului

Barem: Punct de control 2 – Adevărat sau fals

6 **Întrebarea 6** — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Sarcinile utile ransomware se pot propaga ușor către copiile de siguranță online conectate la rețea.

7 **Întrebarea 7** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Fals: FBI avertizează că plata nu garantează că vei primi înapoi vreo dată.

8 **Întrebarea 8** — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Adevărat: CISA recomandă deconectarea gazdelor infectate sau scoaterea rețelei offline pentru a limita răspândirea.

9 **Întrebarea 9** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Fals: ransomware-ul criptează de obicei fișierele cu cifruri simetrice rapide, precum AES.

10 **Întrebarea 10** — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Testarea periodică a procedurilor de restaurare a datelor este o parte esențială a recuperării în caz de dezastru.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

C 1. CRIPTARE	E 2. SARCINĂ UTILĂ	F 3. BACKUP LA RECE	A 4. IZOLARE
H 5. RĂSCUMPĂRARE	G 6. RECUPERARE	D 7. DEZASTRU	B 8. TROIAN

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 CRIPTARE	2 PAYLOAD	3 BACKUP OFFLINE	4 IZOLARE
5 RĂSCUMPĂRARE	6 RECUPERARE		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 C – BACKUPOFFLINE	2 H – TROJAN	3 A – CRIPTARE	4 E – RĂSCUMPĂRARE
5 D – IZOLARE	6 G – DEZASTRU	7 B – PAYLOAD	8 F – RECUPERARE

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica CRIPTARE, SARCINĂ UTILĂ și BACKUP LA RECE cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

E	I	S	Z	Ș	E	R	R	U	D	A	A	R	O	M
R	U	P	T	X	Q	Î	E	S	T	C	S	B	M	Y
A	R	N	Ă	F	S	W	C	W	Î	R	A	R	Z	Y
R	T	A	Y	I	K	F	U	I	M	I	R	Î	L	L
Ă	S	J	T	Z	O	G	P	Q	Q	P	G	Z	A	O
P	A	O	U	O	F	Ț	E	Â	Y	T	S	Y	Ă	G
M	Z	R	L	L	Z	F	R	Î	N	A	P	N	W	Â
U	E	T	L	A	Z	Y	A	F	X	R	O	V	Ț	J
C	D	U	P	R	Ă	N	R	U	T	E	L	G	U	B
S	X	Ț	J	E	R	Ă	E	W	Z	X	L	S	Q	W
Ă	B	A	C	K	U	P	O	F	F	L	I	N	E	H
R	O	C	A	B	Î	Q	V	W	W	K	I	H	T	H
F	Ă	P	A	Y	L	O	A	D	D	I	J	Ș	S	V
R	Z	D	H	D	S	Â	A	K	Q	Â	Z	L	J	U
S	Ț	A	S	W	Î	L	L	G	H	M	H	R	F	K

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE

													T	
I	Z	O	L	A	R	E							R	
					Ă								O	
	D	E	Z	A	S	T	R	U					J	
					C								A	
	B	A	C	K	U	P	O	F	F	L	I	N	E	
			R		M									
			I		P	A	Y	L	O	A	D			
			P		Ă									
			T		R	E	C	U	P	E	R	A	R	E
			A		A									
			R		R									
			E		E									

GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: IZOLARE Deconectarea sistemelor de rețea infectate. (7 litere)

4 orizontal: DEZASTRU Eveniment major de perturbare a sistemului. (8 litere)

5 orizontal: BACKUPOFFLINE Copie deconectată, offline. (13 litere)

7 orizontal: PAYLOAD Executarea software-ului rău intenționat. (7 litere)

8 orizontal: RECUPERARE Restaurarea bazei de date din copia de rezervă. (10 litere)

VERTICAL

1 vertical: TROJAN Fișier rău intenționat deghizat în fișier curat. (6 litere)

3 vertical: RĂSCUMPĂRARE Cerere de plată pentru cheia criptografică. (12 litere)

6 vertical: CRIPTARE Blocarea criptografică a fișierelor. (8 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. RPTCAREI — **CRIPTARE**
2. NUAPCBIOEFLFK — **BACKUPOFFLINE**
3. RĂĂPRRSMEUAC — **RĂSCUMPĂRARE**
4. ARUTSDEZ — **DEZASTRU**
5. ODLYPAA — **PAYLOAD**
6. ROAILEZ — **IZOLARE**
7. EURREAREPC — **RECUPERARE**
8. ONTAJR — **TROJAN**

BAREMUL PROVOCĂRII CU CODUL SECRET

"RESTAUREAZĂ DATELE CRIPTATE DIN BACKUP OFFLINE"

Barem pentru studiile de caz

A Studiu de caz 1: Limitarea încărcăturii unui ransomware într-o organizație

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O rețea locală corporativă a fost compromisă de un ransomware activ. Serverele de fișiere cheie au început să afișeze fișiere cu extensia .locked.
- Strategie și soluție recomandate: Deconectează toate serverele afectate de la rețeaua locală. Încheie sesiunile administrative active. Restaurează fișierele necompromise dintr-un sistem securizat de copii de siguranță offline, protejat la scriere.

B Studiu de caz 2: Evaluarea arhitecturilor de backup offline

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O companie dorește să proiecteze o strategie de backup al datelor care reduce riscul compromiterii copiilor de siguranță chiar dacă rețeaua locală principală este preluată complet de ransomware.
- Strategie și soluție recomandată: Implementează stocare write-once-read-many (WORM). Creează o separare logică (air-gap) deconectând sistemul de backup de la toate rețelele și impune rotirea zilnică a mediilor fizice.