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

Noțiuni de bază de securitate cibernetică și amenințări online Prevenire

Amenințări de securitate cibernetică, firewall-uri de rețea, autentificare multifactor, cadre de securitate

PREZENTARE GENERALĂ A ÎNVĂȚĂRII: NOȚIUNI DE BAZĂ DE SECURITATE CIBERNETICĂ

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 bazele securității cibernetice și ale prevenirii amenințărilor online. Vei explora malware-ul, autentificarea multifactor, firewall-urile și răspunsul la incidente.

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/

Harta ta de învățare despre bazele securității cibernetice

- Identifică vectorii frecvenți de malware, phishing și intruziune în rețeaua corporativă.
- Implementează controale standard de securitate cibernetică, inclusiv MFA, firewall-uri și apărarea punctelor terminale.
- Evaluează procedurile de răspuns la incidente pentru atenuarea impactului încălcărilor de securitate a datelor.
- Analizează factorii de risc organizaționali și alinierea de securitate conform ghidurilor NIST.
- Configurează practici de igienă a securității pentru a atenua atacurile automate de credential stuffing.

INSTRUCȚIUNI PENTRU GHIDUL DE SECURITATE CIBERNETICĂ

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 prevenirea amenințărilor. Încheie cu activitatea bonus Gândește repede.

NOȚIUNI DE BAZĂ DE SECURITATE CIBERNETICĂ ȘI PREVENIREA AMENINȚĂRILOR (INTRODUCERE)

Securitatea cibernetică protejează rețelele, sistemele și datele împotriva atacurilor digitale neautorizate. Dezvoltarea unor obiceiuri solide de securitate, configurarea firewall-urilor, solicitarea autentificării multifactor și instruirea personalului în recunoașterea amenințărilor sunt componente esențiale ale apărării rețelei corporative.

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

Punct de control 1: Provocare cu alegere multiplă

1. Care este obiectivul principal al unui atac de phishing?

- A. Furtul datelor de autentificare și al datelor sensibile ale utilizatorilor
- B. Îmbunătățirea vizibilității site-ului web în motoarele de căutare
- C. Creșterea capacității de lățime de bandă a rețelei
- D. Gestionarea replicării centrului de date de backup

2. Ce mecanism oferă cea mai puternică protecție a contului?

- A. Autentificare multi-factor cu chei hardware
- B. Parole complexe actualizate la fiecare treizeci de zile
- C. Restricționarea autentificării în cont la programul de lucru
- D. Ascunderea numelui de utilizator al contului din directoarele publice

3. Ce definește încărcătura unei infecții cu ransomware?

- A. Criptarea fișierelor de sistem și cererea unei plăți
- B. Înregistrarea discretă a tastelor apăsate pe servere la distanță
- C. Injectarea de reclame neautorizate în browsere
- D. Folosirea resurselor CPU locale pentru minarea de criptomonede

4. Cum afectează un exploit zero-day apărările de securitate?

- A. Vizează vulnerabilități necorectate și necunoscute
- B. Dezactivează automat firewall-ul corporativ
- C. Forțează sistemul să efectueze o repornire completă
- D. Nu necesită niciun buget pentru remediere

5. Ce cadru guvernează controalele de securitate corporative?

- A. Ghidurile NIST Cybersecurity Framework
- B. Specificațiile schemei de document W3C HTML5
- C. Manuale de instalare a driverelor de imprimantă
- D. Definiții IETF ale protocoalelor de rutare

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare adevărat/fals 6

6. Atacurile de phishing vizează doar conturile personale de e-mail.

- ( ) Adevărat
- ( ) Fals

7 Întrebare adevărat/fals 7

7. Autentificarea multifactor ajută la blocarea atacurilor de tip credential stuffing.

- ( ) Adevărat
- ( ) Fals

8 Întrebare adevărat/fals 8

8. Firewall-urile inspectează traficul de rețea pentru a bloca accesul neautorizat la porturi.

- ( ) Adevărat
- ( ) Fals

9 Întrebare adevărat/fals 9

9. Remedierea exploatărilor zero-day necesită actualizări standard ale definițiilor antivirus.

- ( ) Adevărat
- ( ) Fals

10 Întrebare adevărat/fals 10

10. Un honeypot este un server-momeală folosit pentru a atrage infractorii cibernetici.

- ( ) 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. Administratorii de rețea instalează un _____ pentru a filtra traficul de intrare.

2. Un atacator folosește un _____ zero-day pentru a ocoli patch-urile sistemului.

3. Atacatorii trimit e-mailuri falsificate pentru a desfășura campanii de _____ împotriva angajaților.

4. Ransomware-ul este o formă distructivă de _____ care blochează datele utilizatorilor.

5. O bună _____ a parolelor reduce riscurile de furt de credențiale.

6. Pentru a proteja comunicațiile sensibile, utilizatorii aplică protocoale de _____ .

BANCĂ DE CUVINTE DIN VOCABULAR

CRIPTARE EXPLOIT FIREWALL HONEYPOT IGIENĂ MALWARE MULTIFACTOR PHISHING

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre securitate

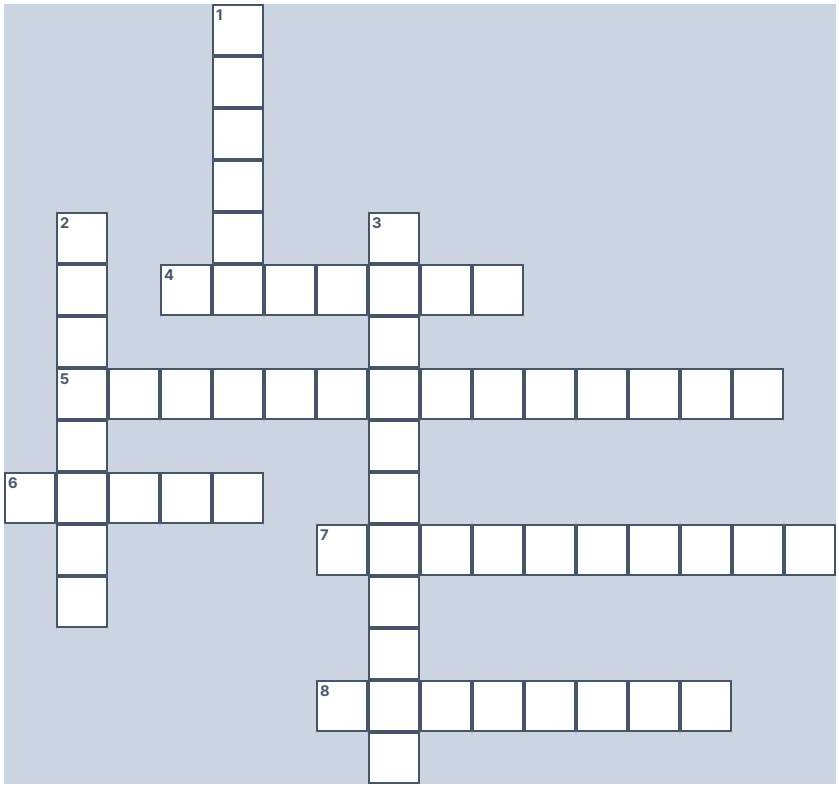
ASOCIEREA DEFINIȚIILOR

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

☐	1. Amenințarea ransomware	A	Linii directoare structurate, precum NIST, folosite pentru gestionarea riscurilor cibernetice.
☐	2. Autentificare multifactor	B	Plan structurat pentru gestionarea și atenuarea breșelor de securitate.
☐	3. Exploatare zero-day	C	Barieră de rețea care filtrează traficul pe baza regulilor de securitate.
☐	4. Honeypot de momeală	D	Software rău intenționat care criptează datele și cere o plată financiară pentru decriptare.
☐	5. Firewall de prevenire a intruziunilor	E	Exploatare a unei vulnerabilități vizate înainte de lansarea unui patch de la producător.
☐	6. Răspuns la incidente	F	Bune practici pentru gestionarea datelor de autentificare și a cheilor de autentificare.
☐	7. Igiena parolelor	G	Validare de securitate care necesită doi sau mai mulți factori de autentificare.
☐	8. Cadru de securitate	H	Sistem-capcană creat pentru a atrage și a analiza actorii rău intenționați.

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

4. Plan structurat pentru gestionarea și limitarea efectelor breșelor de securitate (7)

5. Exploatare a unei vulnerabilități vizate înainte de lansarea unui patch de către furnizor (14)

6. Ghiduri structurate, precum NIST, folosite pentru gestionarea riscurilor cibernetice (5)

7. Malware care criptează datele și cere o plată în bani pentru decriptare (10)

8. Sistem-momeală creat pentru a atrage și a analiza actorii rău intenționați (8)

VERTICAL

1. Bune practici pentru gestionarea acreditărilor și a cheilor de autentificare (6)

2. Barieră de rețea care filtrează traficul pe baza regulilor de securitate (8)

3. Validare de securitate care cere doi sau mai mulți factori de autentificare (11)

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

4 orizontal: Plan structurat pentru gestionarea și limitarea efectelor breșelor de securitate (7 litere):

5 orizontal: Exploatare a unei vulnerabilități vizate înainte de lansarea unui patch de către furnizor (14 litere):

6 orizontal: Ghiduri structurate, precum NIST, folosite pentru gestionarea riscurilor cibernetice (5 litere):

7 orizontal: Malware care criptează datele și cere o plată în bani pentru decriptare (10 litere):

8 orizontal: Sistem-momeală creat pentru a atrage și a analiza actorii rău intenționați (8 litere):

VERTICAL

1 vertical: Bune practici pentru gestionarea acreditărilor și a cheilor de autentificare (6 litere):

2 vertical: Barieră de rețea care filtrează traficul pe baza regulilor de securitate (8 litere):

3 vertical: Validare de securitate care cere doi sau mai mulți factori de autentificare (11 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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

RANSOMWARE MULTIFACTOR EXPLOITZERODAY HONEYPOT FIREWALL
RĂSPUNS IGIENĂ CADRU

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. RANSOMWARE
B. MULTIFACTOR
C. EXPLOITZERODAY
D. HONEYPOT
E. FIREWALL
F. RĂSPUNS
G. IGIENĂ
H. CADRU

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

_____ 1. Barieră de rețea care filtrează traficul pe baza regulilor de securitate.

_____ 2. Plan structurat pentru gestionarea și limitarea efectelor breșelor de securitate.

_____ 3. Malware care criptează datele și cere o plată în bani pentru decriptare.

_____ 4. Validare de securitate care cere doi sau mai mulți factori de autentificare.

_____ 5. Bune practici pentru gestionarea acreditărilor și a cheilor de autentificare.

_____ 6. Ghiduri structurate, precum NIST, folosite pentru gestionarea riscurilor cibernetice.

_____ 7. Exploatare a unei vulnerabilități vizate înainte de lansarea unui patch de către furnizor.

_____ 8. Sistem-momeală creat pentru a atrage și a analiza actorii rău intenționați.

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. RWMOARAESN
2. OXIPTAEDZY ROEL
3. EIFWALLR
4. ĂEINIG
5. TUCALRIFMO T
6. OTEPHYON
7. RNUSĂPS
8. UCDRA

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Meserii din securitatea cibernetică			
2	Motive pentru care ar trebui să actualizezi software-ul			
3	Lucruri pe care le poate bloca un firewall			
4	Semnale de avertizare într-un e-mail			
5	Lucruri pe care le salvezi într-o copie de rezervă			
6	Tipuri cunoscute de atacuri cibernetice			
7	Lucruri pe care le poate atrage un honeypot			
8	Informații pe care nu ar trebui să le dai niciodată			
9	Semne că un calculator este infectat			
10	Filme sau seriale despre hackeri			
11	Straturi de securitate pe care le poți construi			
12	Lucruri de exersat într-un exercițiu de securitate			
13	Instrumente de securitate pe care le cunoști			
14	Persoane pe care le poți întreba pentru ajutor IT			
15	Cuvinte care încep cu „cyber”			

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: STRATEGIA DE RECUPERARE ÎN URMA UNUI RANSOMWARE



Scenariu: O rețea corporativă este infectată cu ransomware, care blochează baze de date critice. Atacatorii cer o plată în criptomonedă de 100.000 USD. Compania are copii de rezervă offline de acum 24 de ore.

Întrebare de discuție: Analizează riscurile plății și evaluează strategia de recuperare.

STUDIU DE CAZ 2: APĂRĂRI ÎMPOTRIVA CREDENTIAL STUFFING



Scenariu: Un serviciu online suferă un atac de tip credential stuffing, în care hackerii testează milioane de perechi nume de utilizator/parolă furate de pe alte site-uri.

Întrebare de discuție: Detaliază mecanismul acestui atac și descrie pe scurt două sisteme de apărare.

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

19	21	18	24	7	13	7	1	31	2		22	11	22	24	7	16	26	15
5	26		1	26	24	7	17	24	11	8	11	5	1	21	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: Care este obiectivul principal al securității cibernetice?

Obiectivul principal este protejarea rețelelor, a dispozitivelor și a datelor împotriva accesului neautorizat, a atacurilor și a daunelor accidentale.

Q2: Prin ce diferă phishing-ul de spear phishing?

Phishing-ul este o campanie largă de e-mailuri care vizează utilizatori aleatorii, în timp ce spear phishing-ul vizează persoane specifice folosind date personalizate.

Q3: Ce este un firewall de rețea?

Un firewall este un sistem de securitate a rețelei care monitorizează și filtrează traficul de intrare și de ieșire pe baza unor reguli de securitate predefinite.

Q4: De ce este necesară autentificarea multifactor (MFA)?

MFA adaugă un strat esențial de apărare, împiedicând accesul chiar dacă atacatorii fură sau sparg credențialele principale ale parolei.

Q5: Ce definește un virus de calculator?

Un virus este un malware care se autoreplică, se atașează la fișiere inofensive și se răspândește în sisteme odată ce este executat.

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

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Cum blochează ransomware-ul datele locale?

Ransomware-ul folosește algoritmi criptografici pentru a cripta fișierele utilizatorilor, făcându-le ilizibile până la aplicarea unei chei de decriptare.

Q7: Ce este o vulnerabilitate zero-day?

Un zero-day este o defecțiune de securitate dintr-un software necunoscută furnizorului, ceea ce nu lasă timp pentru dezvoltarea unui patch înainte de exploatare.

Q8: Care este rolul cadrului NIST?

Cadrul NIST oferă ghiduri și standarde voluntare care ajută organizațiile să gestioneze și să reducă riscurile de securitate cibernetică.

Q9: Ce este un plan de răspuns la incidente de securitate?

Este un set documentat de proceduri pentru detectarea, limitarea și recuperarea după breșe de securitate și compromiteri ale rețelei.

Q10: Cum exploatează ingineria socială utilizatorii?

Ingineria socială folosește manipularea psihologică pentru a păcăli angajații să dezvăluie parole sau să descarce fișiere rău intenționate.

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 copleșește un atac DDoS serverele web?

Un atac DDoS coordonează milioane de dispozitive compromise dintr-un botnet pentru a inunda un server cu trafic, epuizând limitele de lățime de bandă și de CPU.

Q2: Care este diferența dintre criptarea simetrică și cea asimetrică?

Criptarea simetrică folosește o singură cheie pentru criptare și decriptare, în timp ce criptarea asimetrică folosește o pereche de chei publică și privată.

Q3: Cum execută hackerii atacuri de tip SQL injection?

Atacatorii introduc comenzi SQL rău intenționate în câmpurile de formular, păcălind baza de date din backend să furnizeze înregistrări neautorizate ale utilizatorilor.

Q4: Ce este mișcarea laterală în intruziunile în rețea?

Este tehnica prin care atacatorii exploatează accesul inițial la un server pentru a compromite alte sisteme interconectate din rețeaua internă.

Q5: Cum redirecționează falsificarea DNS (DNS spoofing) traficul web?

Falsificarea DNS modifică înregistrările din cache ale serverelor de nume, direcționând utilizatorii legitimi către site-uri malițioase care imită domeniile țintă.

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: Ce este un token de securitate hardware?

Este un dispozitiv fizic (precum YubiKey) care generează dovezi criptografice de autentificare, oferind apărare maximă împotriva phishingului de la distanță.

Q7: Cum folosesc echipele de securitate honeypot-urile momeală?

Echipele implementează servere-momeală din afara producției pentru a detecta din timp intruziunile și a analiza tiparele de atac ale actorilor neautorizați.

Q8: Care este principiul privilegiului minim?

Este standardul de securitate care restricționează drepturile de acces ale utilizatorilor la minimul absolut necesar pentru a-și îndeplini rolurile de lucru.

Q9: Cum exploatează un atac Man-in-the-Middle conexiunile?

Un atacator interceptează și modifică comunicațiile dintre două dispozitive din rețele necriptate, furând token-uri de sesiune și date de autentificare.

Q10: Ce sunt indicatorii de compromitere (IOC)?

IOC-urile sunt indicii criminalistice, precum modificări neobișnuite ale registrului sau trafic IP suspect, care arată că un sistem a fost compromis.

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 scanează constant internetul în căutarea serverelor vulnerabile și trimit e-mailuri de phishing în căsuțele de e-mail ale angajaților.

2. INFORMAȚII DESPRE SECURITATE

Eroarea umană, precum accesarea link-urilor de phishing, este un factor frecvent în breșele de date, motiv pentru care instruirea contează.

3. INFORMAȚII DESPRE SECURITATE

Costurile unei încălcări a securității datelor includ amenzi legale, pierderea clienților, investigații și remedieri, și pot ajunge la milioane de dolari.

4. INFORMAȚII DESPRE SECURITATE

MFA rezistentă la phishing, precum cheile de securitate hardware, este cel mai puternic tip de MFA și standardul pe care îl promovează CISA. [2]

5. INFORMAȚII DESPRE SECURITATE

Ransomware-ul rămâne o amenințare majoră pentru rețelele enterprise, iar CISA recomandă insistent copii de siguranță offline, criptate, ca apărare esențială. [4]

6. INFORMAȚII DESPRE SECURITATE

NIST Cybersecurity Framework 2.0 (2024) are șase funcții de bază: Guvernare, Identificare, Protejare, Detectare, Răspuns, Recuperare. [1]

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Boții de credential stuffing testează la scară largă perechi de nume de utilizator și parolă scurse, pe portalurile de autentificare ale băncilor și ale magazinelor online.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Există piețe de exploit-uri zero-day în întreaga lume, unde vulnerabilitățile de severitate ridicată pot fi vândute pe sume mari înainte de a fi remediate.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Un sistem-momeală de tip honeypot raportează imediat alertele de intruziune, deoarece utilizatorii legitimi nu au niciun motiv să îl acceseze.

10. INFORMAȚII DESPRE SECURITATE

Transport Layer Security (TLS) criptează sesiunile din browser, prevenind interceptarea pachetelor în rețelele Wi-Fi publice.

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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

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

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Barem: Punct de control 1 – Alegere multiplă

1 **Atacuri de phishing** PHISHING — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Campaniile de phishing încearcă să fure credențiale și date sensibile ale utilizatorilor folosind e-mailuri falsificate. Citație: OWASP Secure Configuration.

2 **Protecția contului** CHEIE MFA — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Autentificarea multifactor (MFA) cu token-uri hardware oferă cea mai puternică apărare a accesului la cont. Citare: NIST Digital Identity.

3 **Amenințarea ransomware** RANSOMWARE — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ransomware-ul criptează sisteme și date critice, cerând plata în criptomonede pentru cheile de decriptare. Citare: Center for Internet Security (CIS).

4 **Vulnerabilitate zero-day** ZERO-DAY — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Amenințările zero-day exploatează vulnerabilități de securitate necorectate și necunoscute, înainte ca un patch al producătorului să fie disponibil. Citare: OWASP Secure Configuration.

5 **Cadre de securitate** CADRE — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Cadre precum NIST oferă îndrumări structurate care ajută organizațiile să gestioneze și să reducă riscurile cibernetice. Citare: NIST Digital Identity.

Barem: Punct de control 2 – Adevărat sau fals

6 **Phishing țintit** PHISHING — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Atacurile de phishing vizează atât rețelele corporative, cât și conturile personale, pentru a extinde vectorii de atac. Citație: OWASP Secure Configuration.

7 **Întrebarea 7** — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

MFA cere un al doilea factor, așa că o parolă furată nu este de obicei suficientă pentru autentificare.

8 **Firewall de trafic** FIREWALL — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Firewall-urile inspectează și blochează traficul pe anumite porturi de rețea pentru a filtra conexiunile neautorizate. Citare: Center for Internet Security (CIS).

9 **Răspuns la zero-day** ZERO-DAY — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Remedierea defectelor zero-day necesită corecții de cod și filtrare WAF, deoarece semnăturile nu există încă. Citare: OWASP Secure Configuration.

10 **Honeypoturi capcană** HONEYPOT — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Honeypot-urile sunt servere-capcană folosite de echipele de securitate pentru a atrage, a alerta și a studia actorii rău intenționați. Citare: Center for Internet Security (CIS).

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

D 1. Amenințarea ransomware	G 2. Autentificare multifactor	E 3. Exploatare zero-day	H 4. Honeypot de momeală
C 5. Firewall de prevenire a intruziunilor	B 6. Răspuns la incidente	F 7. Igiena parolelor	A 8. Cadru de securitate

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 MALWARE
5 IGIENĂ	6 CRIPTARE		

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

1 E – FIREWALL	2 F – RĂSPUNS	3 A – RANSOMWARE	4 B – MULTIFACTOR
5 G – IGIENĂ	6 H – CADRU	7 C – EXPLOITZERODAY	8 D – HONEYPOT

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Amenințarea ransomware, Autentificare multifactor și Exploatare zero-day 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.

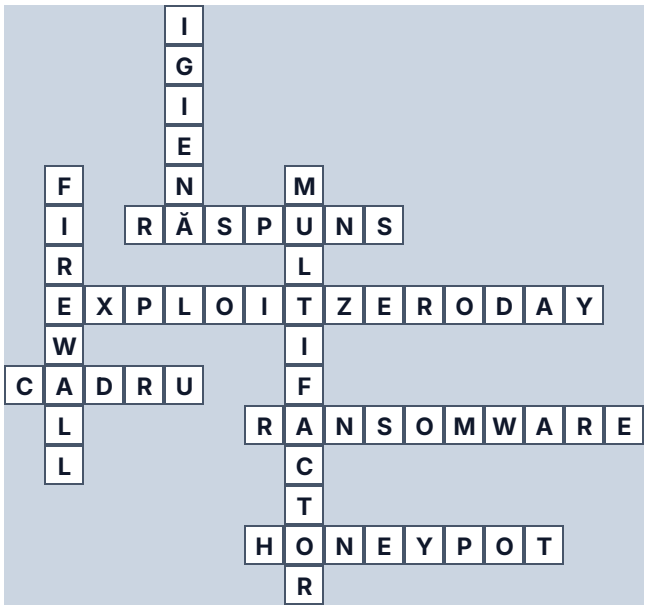
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

4 orizontal: RĂSPUNS Plan structurat pentru gestionarea și limitarea efectelor breșelor de securitate (7 litere)

5 orizontal: EXPLOITZERODAY Exploatare a unei vulnerabilități vizate înainte de lansarea unui patch de către furnizor (14 litere)

6 orizontal: CADRU Ghiduri structurate, precum NIST, folosite pentru gestionarea riscurilor cibernetice (5 litere)

7 orizontal: RANSOMWARE Malware care criptează datele și cere o plată în bani pentru decriptare (10 litere)

8 orizontal: HONEYPOT Sistem-momeală creat pentru a atrage și a analiza actorii rău intenționați (8 litere)

VERTICAL

1 vertical: IGIENĂ Bune practici pentru gestionarea acreditărilor și a cheilor de autentificare (6 litere)

2 vertical: FIREWALL Barieră de rețea care filtrează traficul pe baza regulilor de securitate (8 litere)

3 vertical: MULTIFACTOR Validare de securitate care cere doi sau mai mulți factori de autentificare (11 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. R W M O A R A E S N — **RANSOMWARE**
2. O X I P T A E D Z Y R O E L — **EXPLOITZERODAY**
3. E I F W A L L R — **FIREWALL**
4. Ă E I N I G — **IGIENĂ**
5. T U C A L R I F M O T — **MULTIFACTOR**
6. O T E P H Y O N — **HONEYPOT**
7. R N U S Ă P S — **RĂSPUNS**
8. U C D R A — **CADRU**

BAREMUL PROVOCĂRII CU CODUL SECRET

"PROTEJEAZĂ SISTEMUL CU AUTENTIFICARE"

Barem pentru studiile de caz

A Studiu de caz 1: Strategia de recuperare în urma unui ransomware

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O rețea corporativă este infectată cu ransomware, care blochează baze de date critice. Atacatorii cer o plată de 100.000 de dolari în criptomonedă. Compania are copii de rezervă offline de acum 24 de ore.
- Strategie și soluție recomandată: Riscurile plății: Plata nu garantează decriptarea fișierelor, marchează compania ca țintă care plătește și finanțează activitatea criminală. Strategia de recuperare: Echipa ar trebui să izoleze gazdele infectate, să șteargă serverele compromise și să restaureze datele din copii de rezervă offline. Trebuie să remedieze vectorul inițial de acces (phishing sau exploit) pentru a preveni reinfectarea imediată.

B Studiu de caz 2: Apărări împotriva credential stuffing

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un serviciu online suferă un atac de tip credential stuffing, în care hackerii testează milioane de perechi nume de utilizator/parolă furate de pe alte site-uri.
- Strategie și soluție recomandată: Mecanism: Atacatorii exploatează reutilizarea parolelor pe mai multe site-uri, folosind boți automatizați pentru a se conecta la conturile utilizatorilor. Apărări: 1. Autentificarea multifactor (MFA) blochează încercările de autentificare chiar dacă parola este corectă. 2. Implementarea limitării ratei (rate-limiting) și a CAPTCHA-urilor blochează traficul boților automatizați care inundă punctele de autentificare.