Fișă de lucru:

Noțiuni de bază în securitate și nivele minime de securitate

Competența vizată: Identifică fundamentele și principiile securității sistemelor de calcul și a rețelelor de calculatoare.

Partea I – Fundamente (45 min)

Activitatea 1 – Securitate la nivel fizic și la nivel informatic (10 min)

Sarcină: Bifează categoria din care face parte fiecare element.

Element	Securitate la nivel fizic	Securitate la nivel informatic
Lacăt	☐	☐
Ușă metalică	☐	☐
Firewall	☐	☐
Antivirus	☐	☐
Cabinet pentru servere	☐	☐
Intrusion Detection System (IDS)	☐	☐
Cameră de supraveghere	☐	☐
Criptarea hard disk-ului	☐	☐

Activitatea 2 – Concepte și principii de securitate

A. Completează spațiile libere folosind termenii din casetă. Un termen poate fi folosit o singură dată.

Termeni: *security in depth · security by design · mitigation · contingency · 90 · patch-uri · weakest link*

1. Strategia de ansamblu, bazată pe mai multe straturi de protecție, se numește _____.
2. Securitatea implementată încă din faza de proiectare se numește _____ și se folosește în zone cu acces foarte restrictiv (de exemplu, rețelele care controlează traficul aerian).
3. Planurile de reducere a expunerii la un risc se numesc _____, iar cele de reducere a impactului după producerea riscului se numesc _____.
4. În medie, _____ % din brețele de securitate se datorează instalării și configurării necorespunzătoare sau nerespectării procedurilor, nu problemelor tehnologice.
5. Menținerea la zi a sistemelor înseamnă aplicarea periodică a _____ și fix-urilor.

6. Un sistem este atât de sigur cât este cea mai slabă componentă a sa – principiul „_____”.

B. Adevărat sau fals? Încercuiește A sau F. Rescrie corect afirmațiile false.

Nr.	Afirmație	A / F
1	Principiul „least privilege” înseamnă că se dă acces doar dacă este necesar și doar pentru ceea ce este obligatoriu.	A / F
2	Setările de securitate pot elimina complet orice risc.	A / F
3	Este sigur să construim relații de încredere bazate pe adrese IP.	A / F
4	Informațiile sensibile trimise în text simplu printr-o rețea nesigură pot fi ușor interceptate.	A / F
5	Un singur strat de protecție, dacă este foarte bun, este suficient.	A / F

Corectări:

_____

Activitatea 3 – Tipuri de atacuri asupra rețelelor (20 min)

Sarcină: Completează tabelul cu **literele** atacurilor din listă, în coloana corespunzătoare.

Lista atacurilor:

a) atacuri la autentificare b) interceptarea informației c) interferențe (de exemplu, *ping flood*) d) furtul sesiunilor e) divulgarea neglijentă f) supresia jurnalizării g) abuz de privilegii h) explorarea ușilor din spate (*backdoors*) i) acumularea informațiilor j) furnizarea de informații neașteptate k) atacuri de protocol l) tehnici de manipulare (*social engineering*) m) metode de acces neglijente

Atacuri contra confidențialității	Atacuri contra disponibilității	Atacuri contra integrității

Întrebare: De ce se spune că integritatea este cea mai importantă dintre cele trei?

_____

Partea a II-a – Aplicații

Activitatea 4 – Atacuri, scenarii și contramăsuri

A. Potrivire. Asociază fiecare atac (1–6) cu măsura de prevenire potrivită (A–F).

Atac	Măsură de prevenire
1. Atacuri la autentificare (*shoulder-surfing*)	A. Analiza protocoalelor criptografice de către experți
2. Furtul sesiunilor	B. Protocoale de criptare și VPN
3. Atacuri de protocol	C. Update-uri și fix-uri
4. Interceptarea informației	D. Educarea utilizatorilor
5. Furnizarea de informații neașteptate	E. Politici privind aplicațiile folosite și antivirus
6. Supresia jurnalizării	F. Analiză statistică a jurnalelor și canale de administrare private

Răspuns: 1 – ____ 2 – ____ 3 – ____ 4 – ____ 5 – ____ 6 – ____

B. Scenarii. Pentru fiecare situație, stabilește categoria atacului (confidențialitate, disponibilitate, integritate), tipul atacului și o măsură de prevenire.

Nr.	Situație	Categorie	Tip de atac	Măsură
1	Un coleg se uită peste umărul tău când introduci parola pe laptop.			
2	Serverul școlii primește mii de cereri *ping* pe secundă și nu mai răspunde elevilor.			
3	Un fost angajat nemulțumit, al cărui cont de administrator nu a fost dezactivat, copiază baza de date cu elevii.			
4	Un utilizator trimite datele contului printr-o rețea Wi-Fi publică, fără criptare, iar cineva le captează.			
5	Primești un telefon de la „departamentul IT” care îți cere parola „pentru verificare”.			

Activitatea 5 – Măsuri minime de securitate

A. Potrivire. Asociază fiecare măsură minimă (1–8) cu descrierea ei (A–H). Consultă Fișa 1.3.

Măsura	Descriere
1. Actualizarea sistemelor	A. Verificarea expeditorilor, a linkurilor și a atașamentelor; raportarea mesajelor de phishing
2. Protecția antimalware	B. Regula 3-2-1, cu restaurare testată
3. Firewall	C. Parole unice, manager de parole, MFA, passkeys

Măsura	Descriere
4. Parole și autentificare	D. Se permit doar conexiunile și serviciile necesare, pe baza unor reguli documentate
5. Criptare și acces	E. Verificarea alertelor și a jurnalelor, procedură de raportare, izolare și recuperare
6. Comportament precaut	F. Actualizări automate pentru sistemul de operare, aplicații, browser și firmware
7. Copii de siguranță	G. HTTPS/TLS, criptarea datelor sensibile, drepturi minime pentru fiecare utilizator
8. Monitorizare și reacție	H. Antivirus/antimalware (EDR în organizații), cu actualizări și monitorizare

Răspuns: 1 – ____ 2 – ____ 3 – ____ 4 – ____ 5 – ____ 6 – ____ 7 – ____ 8 – ____

B. Adevărat sau fals? Încercuiește A sau F.

Nr.	Afirmație	A / F
1	Pentru autentificarea exclusiv cu parolă, se recomandă minimum 15 caractere.	A / F
2	Parola trebuie schimbată obligatoriu din 30 în 30 de zile, chiar fără suspiciuni de compromitere.	A / F
3	Regula 3-2-1 înseamnă trei copii, pe două medii diferite, dintre care una în altă locație.	A / F
4	Un firewall bine configurat înlocuiește antivirusul și actualizările.	A / F
5	Este acceptabil să dezactivezi antivirusul ca să rulezi un fișier necunoscut.	A / F
6	O copie de siguranță este utilă doar dacă restaurarea ei a fost testată.	A / F
7	La un firewall, politica recomandată este „implicit respins dacă nu este permis”.	A / F

Activitatea 6 – Mini-audit de securitate pe stația de lucru

Sarcină: Verifică, împreună cu colegul de bancă, starea de securitate a calculatorului din laborator (sau a unui calculator personal, dacă profesorul permite). Completează tabelul.

> ***Reguli:*** *nu nota parolele reale, nu modifica setări fără acordul profesorului și nu dezactiva nicio protecție.*

Nr.	Verificare	Unde verifici (Windows)	Rezultat (✓ / ✗)	Observații
1	Sistemul de operare este actualizat	Setări → Windows Update		

Nr.	Verificare	Unde verifici (Windows)	Rezultat (✓ / ✗)	Observații
2	Antimalware activ și actualizat	Securitate Windows → Protecție împotriva virușilor și amenințărilor		
3	Firewall activat	Securitate Windows → Firewall și protecția rețelei		
4	Contul folosit este de utilizator standard (nu administrator)	Setări → Conturi		
5	Browserul este actualizat	Meniul browserului → Despre		
6	Discul este criptat (dacă este disponibil)	Setări → Confidențialitate și securitate / BitLocker		
7	Există o copie de siguranță recentă	Istoric fișiere / unitate externă / cloud		

Concluzii:

1. Cele mai importante 2 probleme descoperite:
   _____
2. Ce măsură de remediere ai aplica primul și de ce:
   _____
3. Care dintre cele 7 verificări ține de *comportamentul utilizatorului*, nu de tehnologie?
   _____

Activitatea 7 – Studiu de caz: risc versus cost

Situație: Un mic service IT are 4 calculatoare, o conexiune la internet și o bază de date cu clienți păstrată pe un singur calculator. Se folosește doar un antivirus gratuit; firewallul este dezactivat, nu se fac copii de siguranță, iar toți angajații folosesc conturi de administrator.

(Valorile de mai jos sunt fictive și servesc doar exercițiului.) Pierderea bazei de date ar însemna aproximativ 8 000 lei, plus 3 zile de activitate oprită. Un hard disk extern pentru copii de siguranță costă aproximativ 250 lei.

Cerințe:

1. Ordonează măsurile minime în ordinea priorității pentru acest service (1 = cea mai urgentă) și justifică alegerea.

Măsură	Prioritate (1–8)	Justificare
Actualizarea sistemelor		
Protecția antimalware		
Firewall		
Parole și autentificare		
Criptare și acces (drepturi minime)		

Măsură	Prioritate (1–8)	Justificare
Comportament precaut		
Copii de siguranță		
Monitorizare și reacție		

2. Este justificată investiția de 250 lei în backup? Compară costul cu pierderea posibilă.
   _____
3. De ce nu este suficient doar antivirusul? Răspunde folosind conceptul *security in depth*.
   _____
4. Ce principiu este încălcat prin faptul că toți angajații au drepturi de administrator?
   _____
5. Enumeră trei tipuri de pierderi pe care le poate produce o breșă de securitate.
   _____

Activitatea 8 – Autoevaluare

Completează cu ✓ în dreptul fiecărei afirmații.

Pot să…	Da	Parțial	Nu încă
deosebesc securitatea fizică de cea informatică	☐	☐	☐
explic *security in depth* și *security by design*	☐	☐	☐
clasific un atac după confidențialitate, disponibilitate, integritate	☐	☐	☐
asociez unui atac o măsură de prevenire	☐	☐	☐
enumăr măsurile minime de securitate	☐	☐	☐
justific o decizie de securizare după raportul risc/cost	☐	☐	☐

Un lucru nou pe care l-am învățat: _____

O întrebare rămasă fără răspuns: _____