Fișă de lucru

Noțiuni de bază în securitatea sistemelor de calcul

Timp de lucru: 50 de minute • Mod de lucru: individual • Total: 100 de puncte

Scop: identificarea măsurilor de securitate fizică și informatică și explicarea modului în care acestea protejează împreună un sistem de calcul. Citește cerințele și formulează răspunsuri clare, folosind noțiunile din fișa de documentare 1.1.

1 Completează enunțurile

10 puncte • Câte 2 puncte pentru fiecare spațiu completat.

a) Un sistem de calcul cuprinde componente _____ și componente _____.
b) Protecția prin uși cu încuietori aparține securității la nivel _____.
c) Securitatea realizată prin mai multe straturi de protecție se numește _____.
d) Integrarea securității încă din faza de proiectare se numește _____.

2 Clasifică măsurile de protecție

12 puncte • Bifează o singură categorie pe fiecare rând. Câte 2 puncte pe rând.

Măsură sau soluție	Securitate fizică	Securitate informatică
Lacăt montat la intrarea într-o încăpere	□	□
Ușă metalică încuiată	□	□
Dulap de servere încuiat	□	□
Firewall configurat pentru filtrarea traficului	□	□
Program antivirus	□	□
IDS care monitorizează traficul rețelei	□	□

3 Asociază soluția cu rolul ei

8 puncte • Scrie litera potrivită. Fiecare literă se utilizează o singură dată.

1. Firewall ___ 2. Antivirus ___ 3. IDS ___ 4. IPS ___

A. Detectează activități suspecte și transmite alerte.
B. Filtrează traficul conform regulilor de acces.
C. Poate bloca automat traficul asociat unei tentative de intruziune.
D. Detectează și combate viruși, viermi și alte coduri malițioase.

4 Apreciază corectitudinea afirmațiilor

20 de puncte • Notează A pentru adevărat sau F pentru fals (2 puncte fiecare). Reformulează cele două afirmații false (5 puncte fiecare).

a) Instalarea unui antivirus este suficientă pentru securitatea întregului sistem. ___
b) Actualizările sistemului de operare și ale aplicațiilor contribuie la securitate. ___
c) Securitatea depinde exclusiv de tehnologie. ___
d) Mai multe niveluri de protecție contribuie la o abordare de ansamblu. ___
e) Configurarea corectă și respectarea procedurilor sunt importante. ___

Reformulări:

5 Explică și aplică noțiunile

20 de puncte • Câte 10 puncte pentru fiecare cerință.

a) Explică diferența dintre security in depth și security by design. Oferă câte un exemplu pentru fiecare concept.

b) Distinge între reducerea expunerii la un risc (mitigation) și reducerea impactului dacă riscul se produce (contingency). Oferă câte un exemplu pentru o posibilă infectare cu un program malițios.

Repere pentru răspuns: ce măsură reduce probabilitatea incidentului și ce măsură limitează consecințele lui?

6 Analizează un caz practic

20 de puncte • Citește situația și rezolvă cerințele.

Într-un laborator de informatică, ușa rămâne descuiată după program. Calculatoarele au antivirus, dar sistemele de operare și aplicațiile nu au mai fost actualizate de mult. Firewallul este dezactivat. Elevii folosesc același cont cu drepturi de administrator. Nu există proceduri pentru raportarea incidentelor.

a) Identifică patru probleme distincte și propune pentru fiecare o măsură adecvată. (16 puncte: 2 puncte pentru fiecare problemă și 2 puncte pentru măsura asociată.)

Problema identificată	**Măsura propusă**

b) Explică, în 2–3 enunțuri, de ce măsurile propuse trebuie aplicate împreună. Folosește ideea de securitate pe mai multe niveluri. (4 puncte)

Autoevaluare

Bifează ce poți face după rezolvarea fișei. Această secțiune nu se punctează.

□ Deosebesc măsurile de securitate fizică de cele informatice.
□ Explic rolurile firewallului, antivirusului și IDS/IPS.
□ Propun măsuri care combină tehnologia, oamenii și procedurile.

Noțiunea pe care vreau să o clarific:

Sursa activităților: materialul atașat „Noțiuni de bază în securitate – nivele minime de securitate acceptabile”, fișa de documentare 1.1. Situațiile practice sunt create pentru aplicarea noțiunilor.