Noțiuni de bază în securitate

Schemă recapitulativă

1. Protecție pe două niveluri

Nivel fizic

garduri, uși cu încuietori, lacăte, control acces.

Nivel informațional

autentificare, aplicații software, protecția datelor, controlul accesului.

2. Concepte esențiale

Security in depth / Defence in depth

mai multe straturi de securitate pentru protecție mai bună.

Security by design

securitatea este integrată încă din faza de proiectare.

Securitatea sistemelor de calcul

Protejarea componentelor hardware, software și a informațiilor pentru funcționarea sigură a sistemului.

3. Security in depth – cum se aplică?

1. evaluarea infrastructurii IT
2. identificarea și clasificarea riscurilor
3. măsuri de reducere a expunerii (mitigation)
4. măsuri pentru reducerea impactului (contingency)
5. mai multe nivele de protecție, ideal de la producători diferiți

Un singur strat nu este suficient.

4. Măsuri minime recomandate

Firewall

filtrează și restricționează traficul.

Antivirus

detectează și blochează codurile malițioase.

IDS / IPS

monitorizează traficul și alertează sau blochează accesul neautorizat.

5. Idei-cheie pentru siguranță

- Uniformizarea infrastructurii
- Administrare centralizată
- Actualizare permanentă: patch-uri și fix-uri
- Configurări standard de securitate
- Proceduri clare de utilizare și administrare
- Securitatea implică: tehnologia + oamenii + procedurile

Multe breșe apar din configurare greșită sau din nerespectarea procedurilor.

Concluzie: Un sistem sigur este bine proiectat, implementat, utilizat și administrat.