1.3 Nivele minime de securitate

Schema lecției: măsurile minime, detaliile esențiale și ideea de rezumat

Nivel minim de securitate

Măsuri complementare, nu un singur program; adaptate valorii datelor, tipului de utilizatori și riscurilor.

a Actualizarea sistemelor

Actualizări automate pentru sistemul de operare, aplicații, browser și firmware. Produsele fără actualizări de securitate se înlocuiesc sau se izolează.

b Protecția antimalware

Antivirus/antimalware, iar în organizații, după necesități, EDR; cu actualizări și monitorizare. Un anti-spyware separat nu e obligatoriu dacă protecția existentă îl acoperă.

c Firewall

Activat pe calculator și configurat la nivelul rețelei. Se permit doar conexiunile și serviciile necesare, pe baza unor reguli documentate.

d Parole și autentificare

Parole unice pentru fiecare cont, preferabil într-un manager de parole. Doar cu parolă: minimum 15 caractere (NIST SP 800-63B-4). MFA; unde se poate, passkeys/FIDO2.

e Criptare și acces

Criptarea datelor sensibile și a dispozitivelor; comunicații protejate (HTTPS/TLS); drepturile minime necesare fiecărui utilizator.

f Comportament precaut

Verifici expeditorii, linkurile și atașamentele; instalezi programe doar din surse de încredere; raportezi mesajele de phishing.

g Copii de siguranță

Backup periodic după regula 3-2-1 (trei copii, două medii, una în altă locație), cu cel puțin o copie offline sau izolată. Restaurarea se testează.

h Monitorizare și reacție

Verificarea alertelor și jurnalelor, identificarea activităților anormale, procedură simplă de raportare, izolare și recuperare după incidente.

Aprofundat în lecție

Detectare malware

Semnături (amenințări cunoscute), analiză euristică, monitorizarea comportamentului, uneori medii izolate. EDR adaugă vizibilitate și investigare. Nicio metodă nu garantează detectarea tuturor atacurilor. Atenție: „antivirușii” falși pot fi malițioși.

Tipuri de firewall

Pe calculator (host-based), în rețea sau ca serviciu. Mecanisme: filtrare de pachete, inspecție stateful, filtrare la nivel de aplicație/proxy. Politică: implicit respins, excepții documentate, revizuire periodică. Nu înlocuiește antivirusul, actualizările, instruirea sau backupul.

Risc versus cost

Compari pierderile posibile (date, întreruperi, remediere, reputație, consecințe juridice) cu investiția și efortul de administrare. Alegi proporțional cu riscul, bugetul, impactul asupra utilizatorilor și extinderea ulterioară.

Măsurile se aplică împreună și se revizuiesc periodic

măsuri tehnice (contur continuu)

utilizatori și proces (contur întrerupt)