1.3 Nivele minime de securitate

Măsuri minime de securitate

Protecția eficientă se bazează pe mai multe măsuri complementare, nu pe instalarea unui singur program. Nivelul minim se adaptează valorii datelor, tipului de utilizatori și riscurilor concrete.

a) **Actualizarea sistemelor** – actualizări automate pentru sistemul de operare, aplicații, browser și firmware; produsele care nu mai primesc actualizări de securitate trebuie înlocuite sau izolate.
b) **Protecția antimalware** – activarea unei soluții de securitate pentru dispozitive (antivirus/antimalware, iar în organizații, după necesități, EDR), cu actualizări și monitorizare. Un program anti-spyware separat nu este obligatoriu dacă protecția existentă acoperă această categorie.
c) **Firewall** – activarea firewallului pe calculator și configurarea unuia la nivelul rețelei; se permit numai conexiunile și serviciile necesare, pe baza unor reguli documentate.
d) **Parole și autentificare** – parole unice pentru fiecare cont, preferabil gestionate cu un manager de parole. Pentru autentificarea exclusiv cu parolă, NIST SP 800-63B-4 prevede minimum 15 caractere; nu impune simboluri obligatorii și nici schimbări periodice fără suspiciuni de compromitere. Se activează MFA; unde este posibil, se preferă cheile de acces (passkeys/FIDO2).
e) **Criptare și acces** – criptarea datelor sensibile și a dispozitivelor, utilizarea comunicațiilor protejate (HTTPS/TLS) și atribuirea drepturilor minime necesare fiecărui utilizator.
f) **Comportament precaut** – verificarea expeditorilor, linkurilor și atașamentelor; instalarea programelor doar din surse de încredere; raportarea mesajelor suspecte de phishing și respectarea avertismentelor de securitate.
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 trebuie testată.
h) **Monitorizare și reacție** – verificarea alertelor și jurnalelor, identificarea activităților anormale și pregătirea unei proceduri simple de raportare, izolare și recuperare după incidente.

Raportul dintre riscuri și costurile securității

Decizia de securizare trebuie să compare pierderile posibile cu investiția și efortul de administrare. Breșele pot provoca pierderi de date, întreruperea activității, costuri de remediere, afectarea reputației și consecințe juridice. Soluțiile trebuie alese proporțional cu riscul, bugetul, impactul asupra utilizatorilor și posibilitatea extinderii ulterioare.

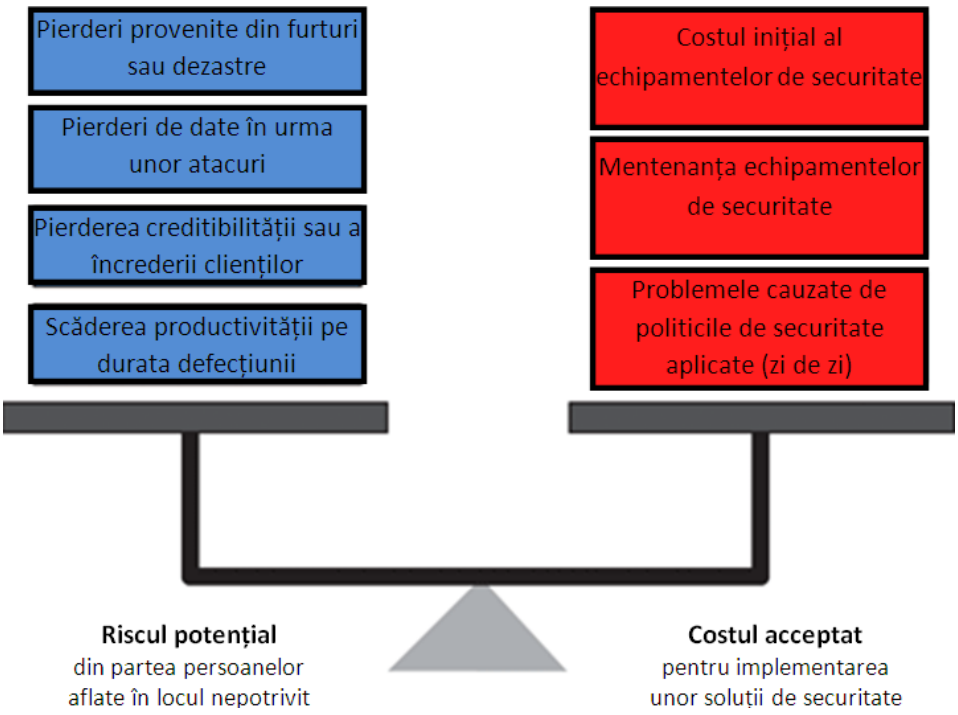


Fig. 1.3.1. Diagrama decizională: pierderi potențiale versus costul măsurilor de securitate (preluată din materialul inițial).

Software de tip antimalware (antivirus/anti-spyware)

Soluțiile actuale combină detectarea prin semnături (amenințări cunoscute), analiza euristică (caracteristici suspecte), monitorizarea comportamentului și, uneori, analiza în medii izolate. EDR adaugă vizibilitate și instrumente de investigare pe dispozitivele administrate. Nicio metodă nu garantează detectarea tuturor atacurilor.

Atenție: aplicațiile care pretind că elimină viruși pot fi ele însele malițioase. Instalați numai produse legitime și verificați notificările, fără a dezactiva protecția pentru a rula fișiere necunoscute.

Aplicațiile de tip firewall

Un firewall controlează traficul dintre dispozitive și/sau rețele pe baza unei politici de acces. Poate fi instalat pe calculator (host-based), la nivelul rețelei sau oferit ca serviciu. Principalele mecanisme sunt filtrarea pachetelor, inspecția stării conexiunilor (stateful) și filtrarea la nivel de aplicație/proxy; produsele avansate pot include funcții suplimentare.

Politica recomandată: identificați serviciile și grupurile care au nevoie de acces, configurați reguli restrictive (implicit respins dacă nu este permis), documentați excepțiile și revizuiți periodic regulile și jurnalele.

Limitări: firewallul nu înlocuiește antivirusul, actualizările, instruirea utilizatorilor sau backupul; nu blochează automat toate atacurile de phishing, amenințările de pe USB ori acțiunile care ocolesc filtrarea. IDS/IPS sunt funcții complementare de detectare/prevenire, nu o componentă obligatorie a oricărui firewall.

Rezumat – ideile esențiale

Un nivel minim actual de securitate înseamnă dispozitive actualizate, protecție antimalware și firewall, parole unice și MFA, criptare, copii de siguranță verificabile, utilizatori informați și o reacție pregătită la incidente. Măsurile se aplică împreună și se revizuiesc periodic, în funcție de riscuri și de costuri.