Măsuri de consolidare securitate cibernetică guvernamentală

Aria	**Managementul perimetrului de rețea (nivel local – instituții)**
Amenințări asociate	• Acces neautorizat la echipamentele de rețea locale (firewall, router, switch) • Exploatarea porturilor și serviciilor nesigure (Telnet, FTP, SNMPv1) • Atacuri de tip brute force asupra interfeței de administrare • Conectarea de echipamente neautorizate în rețea (rogue devices) • Creștere necontrolată a traficului (loop, broadcast storm) • Atacuri interne prin Wi-Fi nesecurizat sau necontrolat
Criticitate	**Înaltă** (compromiterea perimetrului local poate permite atacatorului acces în rețeaua internă și propagare către infrastructura centrală)
Contramăsuri	**Firewall local configurat corect** – blocare porturi/servicii neutilizate; –reguli specifice acces rețea (whitelist, access list, blacklist) **Acces remote securizat** – acces doar prin VPN (IPSec/SSL); – parolă + MFA pentru conturi de administrare; – logare și monitorizare a sesiunilor VPN. **Segmentarea internă a rețelei (VLAN-uri)** – separare utilizatori, servere și echipamente de management; – Wi-Fi „guest” separat de LAN intern. Protecție împotriva atacurilor interne – activarea port security pe switch-uri (blocare MAC-uri necunoscute); – dezactivarea automată a porturilor libere; – storm control activat pentru prevenirea broadcast flood. **Actualizări și management echipamente** – update firmware pentru router/firewall/switch; – dezactivarea conturilor predefinite sau preexistente; – backup periodic al configurației. **Monitorizare și logare** – loguri activate pe firewall/router; – retenție minim 30 zile; – verificare săptămânală pentru tentative suspecte. **Politici pentru utilizatori** – interzicerea routerelor Wi-Fi personale; – conectare doar echipamente aprobate; – Wi-Fi WPA2/WPA3 cu parolă complexă, schimbată periodic.
Indici de compromitere	• multiple încercări de login eșuate pe firewall/router; • creștere bruscă a traficului pe un port/IP; • dispozitive necunoscute conectate la LAN sau Wi-Fi; • loguri cu acces suspect din IP-uri externe; • instabilitate rețea (căderi, ping foarte ridicat, pachete pierdute).