Măsuri de consolidare securitate cibernetică guvernamentală

Aria	**Managementul Anti malware (soluții Antivirus)**
Amenințări asociate	• Infectarea cu viruși, troieni, spyware sau ransomware • Descărcarea și rularea accidentală de fișiere malițioase • Exploatarea vulnerabilităților prin atașamente de e-mail sau linkuri • Persistența malware-ului prin rootkit-uri sau backdoor-uri • Botnet și control remote al stațiilor compromise
Criticitate	**Înaltă** (compromiterea endpoint-urilor afectează confidențialitatea și disponibilitatea datelor, dar și integritatea rețelei interne.)
Contramăsuri	• Instalarea unei soluții antivirus/EDR pe toate stațiile și serverele. • Activarea actualizării zilnice a semnăturilor de viruși la soluții antivirus. • Scanări automate săptămânale și scanări la cerere pentru fișiere suspecte. • Activarea protecției în timp real (real-time protection). • Configurarea alertelor centralizate către echipa IT. • Interzicerea dezinstalării sau dezactivării anti malware de către utilizatori. • Politici de blocare a aplicațiilor necunoscute (application whitelisting, dacă este disponibil). • Integrarea cu SIEM pentru corelarea incidentelor.
Indici de compromitere	• Detectări repetate de malware pe același endpoint. • Stații cu antivirus dezactivat sau neactualizat. • Activitate neobișnuită: consum CPU/RAM ridicat, procese necunoscute. • Conexiuni suspecte către IP-uri externe neautorizate.
Raportare	**Local** Utilizatorul raportează imediat incidentul la echipa IT. IT verifică, izolează dispozitivul afectat și transmite logurile. **Central** la **CERT GOV MD** Tichet www.suport.gov.md solicitare cu anexă dovezi (log, print scree) E-mail: info@cert.gov.md text cu anexă dovezi (log, print scree)