Măsuri de consolidare securitate cibernetică guvernamentală

Aria	**Accesul și managementul resurselor MCloud și Sisteme interne**
Amenințări asociate	• Exploatare neautorizată resurse (brute force, credential stuffing, privilege escalation) • Furt de date/Exfiltrare date (SQL Injection, phishing, malware beaconing) • Alterare/Ștergere informații (insider threats, ransomware) • Zero-Day CVE exploit (remote code execution, misconfiguration exploit) • Compromiterea sesiunilor de administrare (session hijacking) • Abuz de privilegii interne (lack of segregation of duties SoD)
Criticitate	**Înaltă**
Contramăsuri	**Acces pe roluri (Role-Based Access Control – RBAC)** – fiecare utilizator primește doar drepturile necesare pentru activitatea sa. **Autentificare cu mai mulți factori (MFA/2FA)** – obligatoriu pentru conturi de administrare și acces remote. – se recomandă aplicații mobile (ex: Microsoft Authenticator, Google Authenticator) sau token hardware. **Managementul conturilor** – dezactivarea imediată a conturilor la demisie/transfer. – parole schimbate periodic (90 zile) și reguli de complexitate (minim 12 caractere, litere mari/mici, cifre, simboluri). **Patch & Update Management** – instalarea lunară a actualizărilor de securitate pentru sisteme, servere și aplicații. – folosirea de surse oficiale/verificate. – testare în mediu de pre-producție înainte de implementare (dacă există). **Monitorizare și logare centralizată** – păstrarea logurilor cel puțin 6 luni. – colectare în SIEM sau syslog centralizat. – verificarea alertelor critice (login nereușite, acces neautorizat). **Copiile de rezervă** – backup zilnic pentru date critice. – copii salvate off-line sau în cloud securizat. – testarea restaurării datelor cel puțin o dată pe trimestru.
Indici de compromitere	• Performanță lentă a sistemelor sau conexiunilor • Prezența fișierelor neautorizate sau modificate • Modificări neautorizate ale setărilor desktop/profiluri • Congelări, crash-uri sau restarturi suspecte • Spațiu de stocare redus din cauza fișierelor ex filtrate/temporare • Conexiuni neautorizate către IP-uri externe • Evenimente multiple de autentificare eșuată
Raportare	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)