Măsuri de consolidare securitate cibernetică guvernamentală

Aria	**Managementul Serviciului de Poștă Electronică Guvernamentală (SPEG)**
Amenințări asociate	• Atacuri de tip phishing / spear-phishing prin e-mailuri frauduloase • Atașamente malițioase (macro-uri, fișiere infectate, executabile) • Acces neautorizat la conturile de e-mail prin parole slabe sau furate • Exfiltrare de date sensibile prin e-mail • Abuz de resurse (spam, campanii malițioase) din conturi compromise
Criticitate	**Critică** (compromiterea serviciului de e-mail afectează comunicarea oficială și poate fi vector de atac pentru întreaga infrastructură guvernamentală)

Configurări de securitate implicite disponibile	• **Autentificare bifactorială (2FA)**
	  ◦ Parolă + cod TOTP (Google/Microsoft Authenticator) pot fi instalate pe mai multe telefoane/dispozitive ale persoanelor autorizate.
	  ◦ Chei de aplicație pentru clienți de e-mail (Outlook, Thunderbird).
	  ◦ 10 coduri de recuperare a parolei accesibile direct din Zimbra.
	• **Autentificare prin certificat (MPASS)**
	  ◦ Login fără introducerea parolei, bazat pe certificat digital.
	• **Politică de parole Zimbra implicit configurată pentru siguranța utilizatorilor**

Contramăsuri conturi instituționale	**Conturile instituționale** sunt adesea folosite de mai multe persoane din aceeași echipă **(secretariat@, info@, suport@ etc).** Pentru a evita incidentele **nu permiteți partajarea parolei**, pentru asta există mai multe opțiuni:
	• **Setarea aceluiași cont pe mai multe PC-uri, cu 2FA activ**
	  ◦ Exemplu: secretariat@ este configurat pe calculatorul de la recepție și pe cel din biroul directorului.
	• **Forward automat către persoane desemnate**
	  ◦ Toate mesajele care intră în secretariat@ pot fi trimise automat și către prenume.nume@ (angajați specifici). Astfel, mai multe persoane pot citi mesajele fără să intre direct în contul „secretariat@”.
	  ◦ Mesajele pot fi păstrate și în cutia poștală originală, pentru arhivă.
	• **Partajarea întregului cont instituțional cu conturi nominale**
	  ◦ Administratorul poate oferi acces la secretariat@ pentru conturile personale (prenume.nume@).
	  ◦ Persoanele cu acest acces pot citi, organiza și trimite e-mailuri direct din numele contului instituțional.
	• **Transmiterea de mesaje din numele contului instituțional**
	  ◦ Dacă ai acces partajat la secretariat@, poți trimite un e-mail care apare ca fiind expediat de „secretariat@”.
	  ◦ Totuși, în loguri rămâne clar că expeditorul real este prenume.nume@ (pentru responsabilitate).

Măsuri de consolidare securitate cibernetică guvernamentală

Aria	**Managementul Serviciului de Poștă Electronică Guvernamentală (SPEG)**
Indicatori compromitere la nivel de cont utilizator	• E-mailuri expediate fără știrea utilizatorului (spam, phishing). • Mesaje de tip bounce (livrare eșuată) pentru e-mailuri neverificate de utilizator. • Raportări de la parteneri sau colegi care primesc mesaje suspecte de la adresa instituțională. • Cont blocat sau inaccesibil (parola schimbată fără autorizare).
Indicatori compromitere la nivel de conținut e-mail	• Atașamente suspecte (exe, js, vbs, macro-uri Office). • Linkuri ascunse sau scurtate către domenii necunoscute. • Mesaje cu solicitări urgente: resetare parolă, plăți rapide, actualizări cont. • Texte cu erori gramaticale, traduceri neclare, provenite aparent de la surse oficiale.
Raportare	**Utilizator final raportează imediat către echipa IT locală orice** • e-mail suspect (phishing, atașamente neobișnuite); • notificare că parola a fost schimbată fără știrea sa; • imposibilitate de accesare a contului; • sesizare de la parteneri că din contul său se trimit mesaje dubioase. **Către STISC** Tichet www.suport.gov.md solicitare cu anexă dovezi (log, print screen) E-mail: info@cert.gov.md text cu anexă dovezi (log, print screen)