WEB-ADMIN.RO
SOLUȚII WEB COMPLETE

Ghid: Cum Recunoști și Previi Cele Mai Comune Atacuri Cibernetice

Atacurile cibernetice pot fi devastatoare dacă nu sunt identificate și gestionate rapid. Acest ghid te ajută să recunoști cele mai comune semnale de avertizare pentru a proteja afacerea și datele critice.

---

1. Semnale de Avertizare pentru Phishing

- **Emailuri sau mesaje suspecte:**
    - Adrese de email necunoscute sau ușor modificate (ex. exemple@micr0soft.com).
    - Solicitări urgente de a face clic pe linkuri sau de a descărca atașamente.
    - Mesaje care cer informații personale, parole sau detalii bancare.
- **Cum să reacționezi:**
    - Nu deschide atașamentele sau linkurile.
    - Raportează mesajul către echipa IT sau manager.

---

2. Semnale de Avertizare pentru Malware/Ransomware

- **Comportament anormal al dispozitivului:**
    - Computerul devine brusc foarte lent.
    - Fereastra cu mesaj de tip „plătiți pentru deblocarea fișierelor” apare pe ecran.
    - Fișierele sunt criptate sau au extensii schimbate (ex. .locked).
- **Cum să reacționezi:**
    - Deconectează imediat dispozitivul de la rețea (Wi-Fi sau cablu).
    - Notifică tehnicianul IT.
    - Nu plăti răscumpărarea!

Mobil: 0744 / 706225
office@web-admin.ro | www.web-admin.ro

3. Semnale de Avertizare pentru Breșe de Securitate

- **Acces neautorizat:**
    - Observi conexiuni suspecte în log-uri sau notificări de autentificare din locații necunoscute.
    - Conturi compromise sau schimbări neautorizate în setările de securitate.
- **Cum să reacționezi:**
    - Schimbă imediat parolele pentru toate conturile afectate.
    - Activează autentificarea cu doi factori (2FA).

---

4. Semnale de Avertizare pentru Atacuri asupra Rețelei

- **Trafic neobișnuit:**
    - Creșteri subite de trafic pe rețea fără motiv aparent.
    - Rețeaua devine lentă, iar serviciile nu mai funcționează corect.
- **Cum să reacționezi:**
    - Verifică cu tehnicianul IT dacă traficul este legitim.
    - Izolează dispozitivele suspecte din rețea.

---

5. Semnale de Avertizare pentru Conturi Compromise

- **Activitate suspectă în conturi:**
    - Emailuri trimise fără știrea ta din adresa companiei.
    - Schimbări neautorizate în fișiere sau aplicații.
- **Cum să reacționezi:**
    - Schimbă parola imediat.
    - Informează echipa pentru a verifica alte conturi afectate.

6. Semnale de Avertizare pentru Încercări de Social Engineering

- **Apeluri sau mesaje ciudate:**
  - Persoane care pretind că sunt din departamentul IT sau de la un partener de încredere.
  - Solicită urgent informații confidențiale sau acces la sistem.
- **Cum să reacționezi:**
  - Nu oferi informații fără verificarea identității apelantului.
  - Anunță managerul sau echipa IT.

---

7. Semnale de Avertizare pentru Website-uri sau Aplicații Periculoase

- **Accesarea unui site infectat:**
  - Browserul afișează avertizări de securitate (ex. „Acest site nu este sigur”).
  - Descărcări automate de fișiere necunoscute.
- **Cum să reacționezi:**
  - Închide imediat site-ul.
  - Rulează o scanare antivirus.

---

8. Semnale de Avertizare pentru Pierderea Datelor

- **Fișiere lipsă sau șterse:**
  - Date importante care dispar brusc sau fișiere corupte.
  - Activitate neautorizată în serverul de backup.
- **Cum să reacționezi:**
  - Notifică imediat tehnicianul IT.
  - Verifică dacă există copii recente ale fișierelor în backup.

Checklist Rapid pentru Acțiune

1. **Raportează imediat incidentele către persoana responsabilă sau echipa IT.**
2. **Deconectează dispozitivele suspecte de la rețea.**
3. **Nu oferi informații confidențiale sau acces neautorizat.**
4. **Verifică întotdeauna autenticitatea mesajelor sau apelurilor.**
5. **Asigură-te că toate sistemele au antivirus activ și actualizat.**

Concluzie

Identificarea rapidă a semnalelor de avertizare poate preveni pierderi semnificative de date și bani. Educă-ți echipa, implementează politici clare și folosește acest ghid ca un instrument de protecție esențial.

Fii proactiv, nu reactiv!

Mobil: 0744 / 706225
office@web-admin.ro | www.web-admin.ro