ROMÂNIA

MINISTERUL AFACERILOR INTERNE

INSTITUŢIA PREFECTULUI - JUDEŢUL OLT

Digitalizarea instituţiilor publice

Atacul de tip phishing – noţiuni generale; măsuri preventive

Definiţii

- **Malware** - software ce îndeplineşte scopuri nelegitime de accesare a unui dispozitiv, reţea sau sistem IT&C, fără acordul sau cunoştinţa proprietarului; exemple: troian, virus, spyware, backdoor, etc.
- **Tehnici de phshing -** tehnici ce au ca scop obţinerea de date confidenţiale (ex. Credenţiale ale aplicaţiilor de tip Internet banking, comerţ electronic, carduri de credit, etc.) prin folosirea ingineriei sociale; se realizează prin intermediul e-mail-ului sau prin clonarea site-urilor şi transmiterea de solicitări referitoare la datele conturilor personale.
- **Credenţiale** - nume utilizator şi parolă

Atacul cibernetic

- Atacul cibernetic debutează prin aplicarea unor tehnici de **inginerie socială** în urma cărora victima recepţionează un mesaj electronic pe contul de e-mail, care fie are inclus un link (iar infectarea se realizează la accesarea acestuia), fie are un ataşament (la deschiderea căruia se iniţiază descărcarea conţinutului *malware*). Pentru a le asigura un caracter legitim, autorii mesajelor electronice folosesc, în textul acestora, termeni specifici instituţiei vizate ori contextului

Măsuri preventive

Specialistii din domeniu recomandă aplicarea mai multor măsuri/soluţii tehnice pentru prevenirea şi limitarea efectelor compromiterii cu agenţi malware, precum:

- dezactivarea rulării automate a elementelor macro din fişierele Microsoft Office
- scanarea tuturor e-mail-urilor (în special a linkurilor şi ataşamentelor)
- implementarea unor filtre la nivelul **gateway**-ului de e-mail, pentru înlăturarea mesajelor electronice cu indicatori cunoscuți de **spam** sau **malware** și pentru blocarea adreselor IP suspecte din **firewall**

Măsuri preventive

- actualizarea sistemului de operare şi păstrarea activă a **Real-time protection**, oferit de Windows Defender, în lipsa unui alt produs **antivirus**
- restrângerea privilegiilor utilizatorilor
- actulizarea tuturor credențialelor de acces (inclusiv la serviciile de e-mail, platforme web, etc.) și implementarea unor mecanisme de autentificare care să presupună parole de complexitate ridicată
- implementarea unor politici de tip **password-reuse** și folosirea de parole diferite pentru fiecare cont de acces; activarea, acolo unde este posibil, a autentificării în doi pași

Măsuri preventive

- configurarea politicilor de restricție în **firewall** (blocarea tuturor porurilor a căror folosire nu este necesară, restricționarea temporară a accesului de la distanţă şi a serviciilor suplimentare, blocarea accesului din afara țării)
- avertizarea şi instruirea utilizatorilor să verifice, în permanenţă, corespondenţa dintre numele expeditorului şi adresa de email de la care provine mesajul
- instruirea utilizatorului cu privire la accesarea de link-uri din mesajele e-mail

Concluzie

- Infectarea cu agenţi **malware** a resurselor informatice aferente unor infrastructuri IT&C publice poate perturba activitatea curentă a instituţiilor publice, vulnerabilizează datele cu caracter personal / confidenţiale gestionate şi poate afecta impact semnificativ imaginea publică a entităţilor publice compromise

- **LUAŢI MĂSURI DE PROTECŢIE IT&C !!!!**