Bune practici privind securizarea contului de e-mail

Majoritatea dintre noi utilizăm e-mail-urile ca cel mai principal canal de comunicare. Datele sensibile sunt adesea partajate prin e-mail, astfel păstrarea informațiilor în siguranță este un scop primordial. Pe lîngă aceasta, este importantă păstrarea contului e-mail în siguranță, departe de malware și compromitere de date.

Atacurile care folosesc ca vector de atac serviciul de e-mail sunt realizate dintr-o sursă de încredere, cu intenția de a convinge utilizatorul să deschidă un fișier atașat infectat sau să urmeze un URL către un site web fraudulos. Deși mecanismele atacurilor ce vizează conturile de e-mail variază, obiectivul este aproape întotdeauna același: furtul de bani sau date.

Tipuri de atacuri prin e-mail:

- **E-mail bombing**: transmiterea în mod repetat a unui e-mail cu fișier atașat de dimensiuni mari, la o anumită adresă de e-mail. Acest atac duce la umplerea spațiului disponibil pe server, făcând contul de e-mail inaccesibil.
- **E-mail spoofing**: trimiterea de e-mail-uri cu adresa expeditorului modificată. Acest tip de atac este folosit pentru a ascunde identitatea reală a expeditorului și pentru a afla detalii confidențiale sau credențale necesare pentru a acesa un cont.
- **E-mail spamming**: transmiterea de e-mail-uri nesolicitate cu conținut comercial. Scopul acestui atac este de a atrage destinatarii de e-mail-uri să acceseze unele site-uri web nesigure.
- **E-mail phishing**: transmiterea de mesaje pentru a determina destinatarii e-mail-urilor să furnizeze informații despre conturi bancare, carduri de credit, parole sau alte informații personale.

RECOMANDĂRI privind securizarea contului de e-mail:

- **Utilizați parole complexe, puternice și unice** - folosiți parole impredicibile, complexe și păstrați confidențialitatea acestora. O parolă trebuie să îndeplinească condiții precum, să aibă o lungime minimă de 8 caractere pentru conturile de utilizator și 12 caractere pentru conturile de administrator, să fie complexă, să includă combinații de cifre, caractere minuscule și majuscule, simboluri speciale și să fie schimbată periodic. Nu reutilizați aceeași parolă pentru mai multe servicii.

Bune practici privind securizarea contului de e-mail

- **Aplicați autentificarea multifactorială** - aceasta reprezintă o metodă foarte eficientă și modernă care folosește un dispozitiv suplimentar (de exemplu token de securitate sau smartphone-ul) pentru a confirma într-un pas suplimentar identitatea persoanei care se autentifică.
- **Păstrați-vă clientul de e-mail, sistemul de operare și browser-ul web actualizate și licențiate -** atunci cînd apar notificări de actualizare, instalați actualizările imediat ce acestea sunt disponibile.
- **Nu dați click pe link-uri și nu deschideți atașamente necunoscute sau suspecte** - programele malware, virușii sunt adesea ascunși în fișierele atașate. Dacă nu sunteți sigur cu privire la un atașament rulați o scanare de malware cu ajutorul antivirusului pentru a vă asigura. Rețineți că atașamentele periculoase pot avea orice format, dar extensia .HTML este o tactică de phishing foarte frecvent utilizată de către persoanele rău intenționate.
- **Nu utilizați adresele de e-mail corporative pentru mesaje private** - adresele de e-mail corporative trebuie utilizate doar în scop de serviciu. Odată ce angajații folosesc adresee de e-mail corporative în scopuri personale acestea devin în primul rînd mult mai solicitate, iar acest lucru mărește șansele de compromitere a e-mail-ului, punând în pericol întreaga organizație.
- **Dezactivați executarea automată a codului** - macrocomenzile, redarea graficelor și preîncărcarea link-urilor în clientul de e-mail.
- **Folosiți soluții de securitate pentru e-mail** - utilizați filtrele anti spam, scanerele antimalware și analizatoarele URL pentru a identifica site-urile de phishing în timp real.
- **Utilizați comunicarea securizată pentru e-mail, cu semnături digitale sau criptare** - în cazul în care transmiteți informații sensibile.
- **Nu accesați niciodată e-mail-urie folosind rețele de hotspot-uri și Wi-Fi public -** hotspot-urile și Wi-Fi-ul publc nu sunt sigure. Utilizați, în asemenea circumstanțe, rețeaua mobilă sau rețelele virtuale private (VPN).
- **Verificați din cel puțin 2 surse informațiile prestatorului băncii, prin canale diferite** - atunci când transferați bani.
- **Familiarizați-vă cu schemele comune de phishing** - de multe ori, subiectul mesajului va fi unul conceput în așa fel încât să atragă atenția (ex: “Mesaj important – Actualizarea datelor personale”). Cazurile tipice de acestfel de e-mail-uri pot să conțină solicitări de completare a unor formulare, în schimbul unor premii, solicitări de la bancă de a introduce datele personale, e-mailuri care discută anumite facturi, etc.