dendrix

GHID DE EVALUARE A RISCURILOR CIBERNETICE

Metode de prevenție și soluții de protecție

Cloud Mailbox Defense

Cisco Partner
Gold Integrator

Introducere

Un atac cibernetic este o tentativă de a invada un computer, un sistem de computere sau o rețea de infrastructură, cu scopul de a aduce anumite prejudicii. Scopul atacatorilor este de a fura, manipula sau distruge date importante, dar și de a cere recompense în schimbul datelor extrase.

Echipele de IT și securitate cibernetică sunt forțate să fie mereu cu un pas în fața atacatorilor și să prioritizeze resursele, astfel încât să protejeze constant cele mai vulnerabile zone ale afacerii.

Conform unui raport de securitate cibernetică:

- **45%** dintre business-uri afirmă că procesele interne sunt ineficiente în prevenirea atacurilor
- **65%** dintre business-uri au experimentat un atac cibernetic în ultimele 12 luni
- **69%** dintre business-uri spun că atacurile cibernetice au devenit mai targetate

Tipuri de atacuri:

- Malware și spyware sunt cele mai costisitoare tipuri de atacuri și produc cele mai mare daune pentru organizații, urmate de data breach.
- Atacurile de tip ransomware au reprezentat 27% din brețele de securitate care au implicat infecții cu malware.
- Google a detectat în jur de 2 milioane de site-uri ca fiind site-uri de tip phishing în 2020.
- În jur de 5200 de atacuri sunt lansate împotriva device-urilor IoT în fiecare lună.

Vezi mai departe care sunt cele mai mari riscuri cibernetice pentru compania ta și soluțiile de protecție!

În urma răspunsurilor la quiz, a reieșit faptul că business-ul tău este cel mai expus în fața unor atacuri de tip phishing, spoofing, business email compromise și exfiltrarea de informații confidențiale din perimetrul organizației.

Phishing-ul este un atac cibernetic foarte răspândit prin care utilizatorii sunt direcționați către pagini web false, care imită foarte bine site-ul original, iar datele introduse pe astfel de pagini sunt furate.

- Peste 18.000 de site-uri de tip phishing sunt înregistrate în fiecare zi. (HelpNet Security, 2020)
- 96% dintre atacurile de tip phishing sunt trimise prin email, 3% sunt rezultatul accesării directe a unui site și 1% încep prin comunicarea prin telefon (sms) sau documente malițioase. (Verizon, 2021)
- Aproximativ 5% dintre emailuri sunt phishing. (Avanon, 2021)

Spoofing-ul este un atac cibernetic care provine dintr-o sursă necunoscută, dar care este deghizată într-o sursă cunoscută de către receptor. De obicei, spoofing-ul este întâlnit în cadrul mecanismelor de comunicare care nu au un nivel ridicat de securitate.

Business Email Compromise (BEC) este un scam prin care atacatorii păcălesc angajații în a face plăți sau a trimite date sensibile, acest atac fiind extrem de greu de prevenit. Atacatorii se bazează pe tehnici de inginerie socială și impersonări pentru a păcăli oamenii, iar metodele tradiționale de detectare care analizează email-urile, link-urile și metadata nu sunt atât de precise.

Un atac de tip BEC are 4 faze:

Research
Se face o cercetare amănunțită și se identifică persoanele care urmează să fie atacate.

Pregătire
Se creează un domeniu fictiv sau se face rost de o adresă de email legitimă.

Executare
Se trimit email-uri în care se cer tranzacții de date sau tranzacții financiare.

Diseminare
Se transferă banii în conturi multiple pentru a se elimina trasabilitatea.

Tipuri de atacuri BEC:

CEO Fraud

Atacatorii joacă rolul unui CEO sau a unui membru executiv și cer angajaților din departamentele contabile sau de finanțe să transfere sume de bani în conturi controlate de atacatori.

Impersonarea unui avocat

Atacatorii joacă rolul unui avocat și cer date de la angajații care nu au cunoștințele și experiența necesară pentru a pune la îndoială validitatea unei astfel de cereri.

Furt de date

Este vizat departamentul de HR, în vederea obținerii informațiilor personale ale CEO-ului companiei sau ale altor membrii importanți. Aceste date pot fi folosite atacuri viitoare precum CEO fraud.

Email Account Compromise

Email-ul unui angajat este furat și folosit pentru a cere plăți din partea unor vendori.

Exfiltrarea de informații confidențiale din perimetrul organizației presupune furtul de date și transferul acestora dintr-un computer, un storage device sau un sistem electronic, pentru a fi accesate de către persoane care nu au autorizația necesară. Astfel de atacuri se produc atunci când există breșe de securitate, email-uri cu date sensibile trimise de către angajați, device-uri pierdute sau un sistem Cloud slab.

*Pentru a te proteja de astfel de atacuri, soluția pe care ți-o propunem este **Cloud Mailbox Defense**.*

Cloud Mailbox Defense este o soluție de securitate complexă, Cloud-native, care îți poate proteja atât afacerea, cât și utilizatorii, prin mitigarea pericolelor, din Cloud, până în inbox.

Mai mult, Cloud Mailbox Defense se integrează cu Microsoft 365, oferind o vizibilitate mai mare în mailurile primite, care pleacă sau în cele trimise în interiorul companiei. Fiecare email este scanat, iar soluția examinează fiecare componentă a mesajului pentru a intercepta orice amenințare: se verifică documentele, conținutul mesajului și reputația sender-ului și a link-urilor atașate. În plus, soluția oferă și protecție împotriva spam-ului.

Fiind ușor de activat și potrivită pentru orice tip de organizație, soluția propusă de noi scanează și identifică noi atacuri, link-uri periculoase, malware și spoofuri, prevenind astfel ultimele tipuri de atacuri.

Deoarece este o soluție bazată pe Cloud, utilizatorii vor avea acces de oriunde, rapid și ușor.

Cloud Mailbox Defense oferă o vizualizare ușoară asupra întregii conversații, pentru o remediere automată sau manuală rapidă a eventualelor probleme, fără a întrerupe trimiterea obișnuită de mesaje.

dendrio

83% *Dintre business-urile mici și mijlocii nu sunt echipate pentru recuperare în cazul unui atac cibernetic.*

Protejează-ți afacerea în fața unui astfel de atac prin soluții moderne, sigure și ușor de implementat.

Ai nevoie de ajutor în a-ți proteja zonele vulnerabile ale afacerii tale din calea unor atacuri cibernetice?

Discută cu un consultant Dendrio