dendrio

GHID DE EVALUARE A RISCURILOR CIBERNETICE

Metode de prevenție și soluții de protecție

Cisco Umbrella

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 la DNS venite din surse malițioase.

Un DNS attack este un tip de atac cibernetic care exploatează vulnerabilitățile sistemelor de nume de domenii. Atunci când are loc un atac la DNS, persoanele care vor să acceseze un anumit site sunt trimise la o adresă greșită, prin schimbarea adresei IP autorizate, cu o adresă IP greșită.

- În medie, timpul necesar pentru identificarea și preluarea controlului asupra unei astfel de breșe de securitate a fost de 280 de zile. (IBM, 2021)
- Peste o treime din toate atacurile cibernetice sunt atacuri la DNS. (Global Cyber Alliance, 2021)

Tipuri de atacuri la DNS pe care trebuie să le știi:

1

DNS cu flux rapid

Atacatorii schimbă înregistrările DNS în interior și la o frecvență ridicată pentru a redirecționa solicitările DNS. Folosind un astfel de atac, atacatorii pot să evite detectarea.

2

Atacuri de tip Zero-day

Hackerul exploatează o vulnerabilitate necunoscută în software-ul serverului DNS, pentru care nu există încă niciun patch.

3

Man in the middle

Atacatorul reușește să se interpună între utlizator și serverul DNS, alterând înregistrările de pe ambele dispozitive. Astfel, atacatorul reușește să redirecționeze atât utilizatorul curent, cât și orice utilizator care folosește serverul de DNS infectat

4

DNS spoofing

Utilizatorul este forțat să navigheze către un site fraudulos, care are scopul de a intercepta traficul utilizatorului sau credențialele de acces ale acestuia.

5

DNS cache poisoning

Atacatorul reușește să obțină control deplin asupra serverului de DNS, putând astfel direcționa utilizatorul către site-uri frauduloase.

6

Server hijack

Atacatorul reușește să obțină control deplin asupra serverului de DNS, putând astfel direcționa utilizatorul către site-uri frauduloase.

Tipuri de atacuri la DNS pe care trebuie să le știi:

Furt de date

Atacatorii au o afinitate pentru "clonarea" site-urilor de comerț online. Utilizatorii sunt redirecționați către o clonă a site-ului, oferind atacatorilor acces la credențiale, informații personale și datele de card.

Infecție cu malware

Utilizatorii pot fi direcționați către site-uri care găzduiesc malware. Atacuri de tip drive-by download sunt un mod foarte ușor de a infecta un dispozitiv care vizitează site-ul, printre cele mai populare descărcări fiind spyware și keylogger.

Blocarea accesului la site-uri care oferă patch-uri de securitate, update-uri de software și semnături antivirus

Utilizatorul nu se mai poate proteja de anumite variante de malware sau atacuri de tip ziua zero, întreg sistemul fiind expus pe o perioadă îndelungată.

Pentru a te proteja de astfel de atacuri, soluția pe care ți-o propunem este ***Cisco Umbrella.***

Cisco Umbrella utilizează infrastructura internetului pentru a bloca destinațiile malițioase înainte de a se stabili o legătură cu acestea. Fiind o primă linie de apărare în Cloud, te ajută să salvezi bani și adaugă un layer de securitate foarte eficient prin:

- Verificarea cererilor la nivel de DNS și IP înainte de stabilirea conexiunii, indiferent de port sau protocol.
- Proxy inteligent pentru domeniile riscante, astfel încât fișierele și URL-urile să fie analizate înainte de accesare.
- Blocarea comunicațiilor cu servere de tip command & control pentru oprirea sustragerii de informații sau executarea ransomware-urilor cu criptare.

Prin Cisco Umbrella, utilizatorii beneficiază de aceeași protecție, indiferent dacă sunt în rețeaua de la birou, în delegație sau de acasă.

Pentru administratorii infrastructurii IT, Umbrella oferă vizibilitate în URL-urile accesate de fiecare utilizator, de pe fiecare dispozitiv, din orice locație și blochează atacurile înainte ca acestea să ajungă în rețea sau pe dispozitiv.

Deoarece este o platformă open, care rulează în Cloud, Umbrella poate fi integrată ușor cu sistemele actuale de securitate, oferind informații în timp real despre amenințări curente și în desfășurare.

Cisco Umbrella nu îngreunează traficul de date, analizând doar DNS-ul înainte de stabilirea conexiunii, utilizatorii observând chiar o îmbunătățire a vitezei de accesare a site-urilor.

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