



GHID DE EVALUARE A RISCURILOR CIBERNETICE

Metode de prevenție și soluții de protecție

Meraki



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 breșele 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!





- Potrivit companiei de securitate cibernetică [Zscaler](#), atacurile împotriva dispozitivelor IoT au crescut cu 700% în ultimii doi ani, companiile de tehnologie fiind cele mai afectate, urmate de companiile industriale și cele de retail.
- Conform unui [raport](#) din 2020, 98% din traficul device-urilor conectate nu este criptat și mai mult de jumătate dintre aceste device-uri sunt vulnerabile în fața unor atacuri de o severitate medie sau mare.

În ceea ce privește atacurile care au ca țintă dispozitivele IoT:

41%

dintre atacuri sunt exploits
(buffer overflow, injections,
RCE)

33%

dintre atacuri sunt malware
(worms, ransomware, trojans,
botnets)

26%

dintre atacuri sunt datorate
practicilor utilizatorilor (parole,
phishing)

*În urma răspunsurilor tale,
business-ul tău este cel mai
vulnerabil în fața breșelor de
securitate via senzori și
sisteme IoT.*

Descoperă în continuare mai multe detalii despre cele mai importante breșe de securitate legate de senzori și sisteme de tip Internet of Things pe care trebuie să le ai în vedere și soluția pentru astfel de atacuri.

Cele mai importante 3 breșe de securitate via senzori și sisteme IoT de care trebuie să te ferești:



IoT botnets

Un atacator poate infecta un dispozitiv IoT cu malware printr-un port neprotejat sau phishing și poate coopta acel dispozitiv pentru a iniția atacuri cibernetice masive. IoT botnets sunt folosiți de obicei pentru a distribui atacuri de tip DDoS (denial-of-service) prin care copleșesc traficul de rețea al unei ținte.



Amenințări DNS

Multe organizații se folosesc de IoT pentru a colecta date din mașinării mai vechi, care nu sunt la cele mai înalte standarde de securitate. Când aceste sisteme vechi sunt combinate cu dispozitive IoT, rețeaua poate fi expusă la vulnerabilitățile device-urilor vechi. Conexiunea dispozitivelor IoT se bazează pe DNS, iar atacatorii se pot folosi de vulnerabilitățile DNS pentru a lansa atacuri prin care să extragă date sau să introducă malware.



IoT ransomware

Atacatorii pot infecta device-urile IoT cu malware și le pot transforma în botnets, pentru a căuta credențiale și pentru a avea acces în rețea. Având acces în rețea prin device-urile IoT, atacatorii pot extrage date în Cloud și pot amenința cu ștergerea sau publicare datelor, dacă nu primesc o recompensă.



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

Cisco Meraki este o soluție de gestiune a Cloud-ului, concepută să ofere management centralizat, vizibilitate la nivelul 7 a dispozitivelor și aplicațiilor, diagnoză în timp real, monitorizare sau raportare.

Soluția folosește o arhitectură de management din afara benzii, lucru care presupune că doar fluxurile de date de gestionare pot să curgă prin infrastructura Cloud Meraki. Toate datele rămân în rețea și niciun utilizator nu poate să treacă prin centrele de date Meraki.

Beneficiile utilizării platformei Cisco Meraki

Operare mult mai facilă a rețelei

Datorită tehnologiilor Cloud, update-urile, patch-urile și noile funcționalități sunt livrate "over the air" și pot fi implementate de îndată ce sunt făcute disponibile de către developeri. Mai mult, modalitatea de configurare a echipamentelor de rețea de tip plug and play face posibilă instalarea unor site-uri noi (magazine comerciale, clinici, benzinării, sucursale de bănci) într-un timp foarte scurt.

Performanță optimizată

Cisco Meraki beneficiază de metadatele primite de la peste trei milioane de rețele și 10 milioane de dispozitive pentru a îmbunătăți algoritmi folosiți în produsele sale și pentru a livra performanțe ridicate într-un mod constant.

Creșterea productivității

Indiferent de locația de unde se muncește, Cisco Meraki poate să ofere conexiuni sigure și stabile către aplicațiile din Cloud sau din data center-ul local pentru angajații, partenerii, contractorii și colaboratorii organizației.

Fidelizarea clienților existenți și atragerea clienților noi

Datele colectate despre utilizatori sunt o resursă prețioasă pentru organizații. Acestea pot fi folosite în industrii precum HoReCa și retail pentru a oferi promoții, reclame personalizate și campanii publicitare într-un mod relevant și cuantificabil.

Cisco Meraki este o soluție completă și capabilă să deschidă drumul transformării digitale, în timp ce satisface cerințele de business, de inovație și de evoluție ale companiilor. Meraki te ajută să reduci costurile de administrare centralizată și unitară a întregii infrastructuri, oferind protecție împotriva breșelor de securitate via senzori și sisteme IoT.



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

