



GHID DE EVALUARE A RISCURILOR CIBERNETICE

Metode de prevenție și soluții de protecție

Cisco Secure Endpoint



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!





În urma răspunsurilor la quiz, a reieșit faptul că business-ul tău este cel mai expus în fața unor atacuri de tip malware, ransomware și atacuri avansate și persistente (APP).

Un atac de tip malware presupune o aplicație anonimă sau un program care are scopul de a-ți infecta dispozitivul cu o aplicație malițioasă, furt de date sau afectarea negativă a performanțelor dispozitivului. Una dintre cele mai bune protecții care poate detecta și elimina malware-ul este un antivirus updatat constant.

- **94%** din malware este transmis prin email. ([CSO, 2020](#))
- **74%** din malware-ul transmis într-o companie a fost trimis între colegi. ([Comparitech, 2021](#))
- **98%** din malware-ul de pe mobil afectează utilizatorii cu device-uri Android. ([PurpleSec, 2021](#))

Un atac de tip ransomware presupune criptarea fișierelor și folderelor din dispozitivele afectate. Hackerii cer o răscumpărare pentru decriptarea fișierelor afectate. Exemple populare de astfel de atacuri sunt WannaCry, Petya, NotPetya etc.

- În urma unui atac de tip ransomware, timpul mediu de nefuncționare al unei companii este de 21 de zile. ([Coverware, 2021](#)).
- Cel mai proeminent tip de malware este ransomware. ([Datto, 2019](#))
- În medie, 1 din 5 companii mici și mijlocii au fost afectate de un atac de tip ransomware, companiile fără servicii de IT externalizate fiind cele mai expuse riscului. ([Datto, 2019](#))

Un atac de tip malware presupune o aplicație anonimă sau un program care are scopul de a-ți infecta dispozitivul cu o aplicație malițioasă, furt de date sau afectarea negativă a performanțelor dispozitivului. Una dintre cele mai bune protecții care poate detecta și elimina malware-ul este un antivirus updatat constant.

- ✗ Furt intelectual (ex: patente)
- ✗ Compromisul informațiilor sensibile (ex: informații despre angajați sau date confidențiale)
- ✗ Sabotarea infrastructurilor critice din organizație (ex: ștergerea bazelor de date)
- ✗ Preluarea controlului asupra site-ului

Atacurile avansate și persistente diferă de restul atacurilor cibernetice deoarece:



Sunt mult mai complexe



De îndată ce rețeaua este compromisă, atacatorul rămâne cât mai mult timp pentru a aduna cât mai multe informații



Sunt executate manual asupra unei ținte specifice

```
return false;
},
},

ajaxResponse: function(response, status)
{
    params = params || {};
    params.force_exec = params.force_exec || false;
    params.callback = params.callback || function(){};
    params.pre_processing = params.pre_processing || function(){};

    var regex_all = new RegExp(".*");
    var matches = [];
    var match = "";
    var elm;
    var data = response.data || {};

    // If pre_processing function is defined
    if (params.pre_processing)
    {
        if (typeof(params.pre_processing) === "function")
        {
            params.pre_processing(data);
        }
        else if (typeof(params.pre_processing) === "string")
        {
            // ...
        }
    }

    if (typeof(params.callback) === "function")
    {
        params.callback(data);
    }
}
```



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

Cisco Secure Endpoint (cunoscut înainte ca și Cisco Advanced Malware Protection) este o soluție de securitate care îmbină prevenția, detecția și vânărea amenințărilor, cu abilitățile de remediere, într-o singură soluție software.

Secure Endpoint este o soluție multiplatform (Windows, macOS, Linux, Android, iOS) care blochează malware-ul în punctul de intrare, oferind o monitorizare continuă a fișierelor și a activității acestora, pentru a detecta, izola și remedia orice amenințare capabilă să compromită dispozitivul utilizatorului. Soluția oferă un set robust de tehnologii preventive, care acționează în timp real:

1

File reputation

Secure Endpoint conține o bază de date cu toate fișierele posibile și variații ale acestora, pentru o detectare rapidă și o carantinare ușoară a fișierelor malițioase.

3

Polymorphic malware detection

Pentru a evita tehnicile de detecție, atacatorii pot folosi diferite variații ale aceluiași malware. Secure Endpoint poate detecta aceste variații.

2

Antivirus

Secure Endpoint include antivirus actualizat constant, care nu are nevoie de conectivitate în Cloud pentru a opera, dispozitivele fiind protejate atât online, cât și offline.

4

Machine learning analysis

Secure Endpoint este antrenat de algoritmi astfel încât să învețe să identifice fișierele malițioase și activitățile bazate pe atributele programelor malware cunoscute.

Cisco Secure Endpoint oferă protecție împotriva celor mai avansate amenințări, prevenind breșele de securitate, blocând malware-ul și analizând în mod continuu fișierele, pentru a detecta, a opri și a remedia orice amenințare care trece de protecția din prima linie.



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

