6 PAȘI PENTRU UN RĂSPUNS EFICIENT LA INCIDENTE DE SECURITATE CIBERNETICĂ

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

1. Pregătirea

Pregătirea este cea mai importantă parte a unui răspuns eficient la un incident de securitate cibernetică.

Pregătirea corectă implică:

- Întocmirea/elaborarea de politici și de bune practici (planuri) dedicate angajaților
- Pregătirea comunicării interne și externe
- Documentarea privind cine, ce, unde, când, cum și de ce execută o anumită acțiune
- Stabilirea echipei de răspuns la incidente (CSIRT)
- Asigurarea că echipa are la dispoziție uneltele potrivite și că are parte de instruire continuă în domeniul securității cibernetice, cu scopul de a o păstra mereu vigilentă și pregătită

2. Identificarea

Când există o deviere de la procesele obișnuite, cum ar fi evenimente anormale de securitate, fișiere suspecte și registry keys sau flux de trafic neobișnuit, este necesar să identificați rapid dacă este vorba despre un incident.

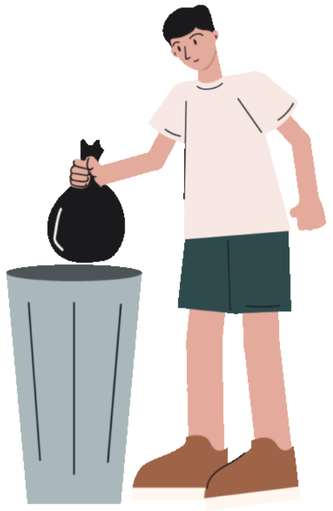
Dacă evenimentul se dovedește a fi un incident de securitate cibernetică, echipa de răspuns trebuie să lucreze pentru a identifica detalii esențiale referitoare la incident, de tipul “cine, ce, unde, când și cum”.

3. Izolarea

Odată ce atacul a fost identificat, personalul care gestionează incidentul trebuie să se concentreze pe limitarea daunelor și pe implementarea măsurilor de prevenire a eventualelor pagube.

Trebuie să luați în considerare izolarea pe termen scurt, backup-ul sistemului și izolarea pe termen lung.

4. Eradicarea



Faza de eradicare implică eliminarea amenințării din infrastructura IT a organizației., precum și restaurarea sistemelor afectate.

Determinați cauza incidentului precum și simptomele sale, îndepărtați artefactele atacatorilor din sistemele compromise și îmbunătățiți apărărarea pentru a preveni incidente similare în viitor.

5. Recuperarea

Recuperarea vizează când și cât de bine vor fi restabilite sistemele afectate, astfel încât să poată fi utilizate din nou.

Acest lucru trebuie făcut cu mare grijă, pentru a evita un alt potențial incident din pricina acelorași probleme care au cauzat problema inițială.

Echipa de răspuns ar trebui să ia în considerare când să restaureze, cum să restaureze, cum să testeze și cât timp să monitorizeze.

6. Lecții învățate

Odată ce toate sistemele afectate sunt din nou în uz și nu mai există semne de reinfectare sau alte probleme, operatorul de sistem și echipa de răspuns pot trece evenimentul la faza “Lecții învățate”.

Învățarea este, probabil, cel mai valoros aspect pe care tu, ca organizație, îl poți obține dintr-un incident de securitate cibernetică, procesul fiind unul practic, nu doar teoretic.

Mare parte din această fază se concentrează pe documentație, pentru că toate concluziile pe care le-ai generat în timpul incidentului (sau după) ar trebui să fie compilate într-un raport final.

Raportul ar trebui apoi să fie revizuit și folosit ca bază pentru îmbunătățirea activităților de prevenire, detectare și răspuns ale posibilelor viitoare incidente.