Scenarii de incidente de securitate

Unknown Exfiltration

Într-o seară de sâmbătă, unul dintre senzorii ce detectează intruziunile la nivelul rețelei organizației avertizează asupra unei activități anormale care implică transferuri mari de fișiere. Analistul ce se ocupă de detectarea intruziunilor analizează alertele primite și descoperă că mii de fișiere de tip .RAR sunt copiate de pe o stație internă pe o stație din exterior, aflată în altă țară. Analistul contactează echipa de intervenție în caz de incidente pentru a investiga în continuare activitatea. Echipa nu reușește să acceseze conținutul fișierelor .RAR întrucât acesta a fost criptat. După o analiză complexă a stației interne pe care se regăseau acele fișiere .RAR au fost constatate urme de existență a unui bot.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?

  Echipa de intervenție în caz de incident ar trebui să includă cel puțin un coordonator de răspuns la incident, un specialist în securitate cibernetică și un analist de rețea. Numărul exact de membri va depinde de complexitatea incidentului.

- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul *organizației* ar trebui implicate în soluționarea incidentului?

  Departamentul IT al organizației, pentru a asigura suport tehnic.

  Departamentul juridic sau de conformitate, în special dacă datele sensibile sunt implicate.

  Echipele de management și de comunicare pentru a gestiona comunicarea cu părțile interesate.

  Echipa de audit intern sau extern, pentru a evalua impactul și consecințele incidentului.

- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?

  Incidentul ar trebui raportat autorităților locale sau internaționale în conformitate cu legile și reglementările aplicabile, cum ar fi GDPR sau legi privind infracțiunile informatice.

- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?

  În funcție de natura incidentului, echipa ar trebui să fie pregătită să coopereze cu autoritățile locale sau internaționale, furnizori de servicii de securitate cibernetică și alte părți interesate.

- Raportarea ar trebui efectuată imediat ce incidentul este confirmat și ar trebui să includă o descriere detaliată a incidentului, impactul, datele afectate și măsurile luate.

  Incidentul ar trebui raportat autorităților locale sau internaționale în conformitate cu legile și reglementările aplicabile, cum ar fi GDPR sau legi privind infracțiunile informatice.

  Raportarea ar trebui efectuată imediat ce incidentul este confirmat și ar trebui să includă o descriere detaliată a incidentului, impactul, datele afectate și măsurile luate.

- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?

  Instrumente de analiză a securității, cum ar fi platforme de detecție a amenințărilor și analiză forensic.

Resurse de stocare sigură pentru evidențe, cum ar fi servere dedicate sau soluții cloud securizate.

- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?

  Dacă incidentul ar fi avut loc în timpul programului de lucru, timpul de răspuns ar fi fost mai scurt, iar coordonarea cu membrii cheie ai organizației ar fi fost mai rapidă.

- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

  Dacă incidentul ar fi avut loc în altă locație fizică, echipa ar fi trebuit să coordoneze cu resursele locale sau să utilizeze soluții de comunicare și monitorizare la distanță.

Intrebari specifice

- Cum ar putea echipa determina ce se afla cel mai probabil în acele fișiere .RAR?

  Echipa ar trebui să folosească instrumente de analiză de securitate pentru a încerca să decripteze conținutul fișierelor .RAR. De asemenea, ar trebui să analizeze metadatele și originile acestor fișiere pentru a determina natura lor.

- Dacă echipa stabilește că stația internă a fost compromisă prin intermediul unui stick wireless cu conexiune la internet, cum va decurge ancheta în continuare?

  Identificarea și izolarea dispozitivului wireless compromis.

  Analiza activității dispozitivului și identificarea modului de compromitere.

  Verificarea dacă există alte dispozitive compromise în rețea.

- Dacă echipa stabilește că stația internă a fost folosită pentru a modifica o serie de fișiere sensibile aflate pe o altă stație din rețea, cum va decurge ancheta în continuare?

  Identificarea și izolarea stației compromise.

  Restaurarea fișierelor la versiunea originală.

  Analiza modalității prin care stația a fost compromisă pentru a preveni recidiva.

Unauthorized Access to Payroll Records

Într-o seară de miercuri, structura/departamentul de securitate al organizației primește un apel telefonic de la șefa sectorului financiar care susține că a văzut o persoană necunoscută părăsind biroul ei, alergând pe hol si ieșind din clădire. Aceasta și-a lăsat stația de lucru deblocată și nesupravegheată pentru doar câteva minute. Programul cu ștatele de plata (programul de salarizare) era încă deschis și se afla în pagina principală, așa cum a fost lăsat, dar șefa financiarului susține că mouse-ul pare a fi mutat din poziția inițială. Echipa de intervenție în cazuri incidente a fost rugată să obțină dovezi legate de incident și sa determine ce acțiuni au fost efectuate.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?

Numărul de membri ai echipei depinde de dimensiunea organizației și de complexitatea incidentului. Cu toate acestea, este important să aibă cel puțin un coordonator al echipei și să se asigure că sunt acoperite toate aspectele incidentului.

- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul organizației ar trebui implicate în soluționarea incidentului?

Echipa ar trebui să implice departamentele de securitate, resurse umane, IT și juridic pentru a coordona răspunsul la incident.

- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?

Incidentul ar trebui raportat autorităților competente, cum ar fi poliția, în conformitate cu legile și reglementările locale. Raportarea trebuie făcută imediat. Cu privire la informații, se ar trebui raportate doar detaliile necesare pentru a investiga incidentul.

- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?

In funcție de natura incidentului, poate fi necesară colaborarea cu firme de securitate cibernetică sau alte organizații specializate pentru a investiga incidentul.

- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?

Echipa ar trebui să utilizeze instrumente de analiză a log-urilor, instrumente forensice, camere de supraveghere, instrumente de securitate cibernetică și alte resurse pentru a investiga incidentul.

- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?

O zi sau oră diferită poate afecta răspunsul și accesul la resurse. Incidentele care au loc în afara programului de lucru pot necesita o reacție imediată și coordonată.

- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

Locația fizică poate afecta investigația, deoarece pot exista mai multe camere de supraveghere sau infrastructură de securitate diferită.

Intrebari specifice

- Cum ar putea afla echipa ce acțiuni au fost întreprinse?

Echipa ar trebui să investigheze înregistrările camerei de supraveghere și log-urile de sistem pentru a reconstitui activitatea.

- Cum s-ar schimba modul de abordare al acestui incident dacă șefa sectorului financiar a recunoscut persoana ce-i părăsea biroul drept un fost angajat al sectorului financiar?

Dacă persoana este un fost angajat, se poate investiga dacă acesta avea încă acces legitim la clădire sau la sistemele informatice. Se va lua în considerare implicarea departamentului de resurse umane pentru gestionarea situației.

- Cum s-ar schimba modul de abordare al acestui incident dacă echipa are motive să creadă că persoana în cauză este un angajat actual?

Dacă persoana este angajată în prezent, se va investiga dacă acțiunile sale au fost autorizate. Pot fi implicate departamentele de resurse umane și juridic pentru a investiga abaterile disciplinare sau penale.

- Cum s-ar schimba modul de abordare al acestui incident dacă structura de securitate a stabilit că persoana în cauză a folosit tehnici de inginerie socială pentru a obține acces fizic în clădire?

Prezența tehnicii de inginerie socială ar putea indica o amenințare mai amplă și necesită măsuri suplimentare pentru a preveni astfel de incidente în viitor.

- Cum s-ar schimba modul de abordare al acestui incident dacă jurnalele cu log-uri din săptămâna precedentă arată un număr neobișnuit de mare de încercări nereușite de conectare la distanță, folosind ID-ul de utilizator al șefei contabil?

Apariția încercărilor nereușite de conectare ar putea indica o încercare de acces la distanță neautorizată. Aceasta ar putea necesita o investigație de securitate cibernetică suplimentară și potențial implica autorități de aplicare a legii.

- Cum s-ar schimba modul de abordare al acestui incident dacă echipa de intervenție în caz de incident descoperă că un keylogger a fost instalat pe computer cu două săptămâni înainte?

Descoperirea unui keylogger arată un potențial compromis de securitate și poate necesita investigații forensice suplimentare pentru a determina extinderea compromiterii și pentru a identifica atacatorul.

Identificarea și izolarea keylogger-ului:

Primul pas este să se identifice și să se izoleze keylogger-ul. Acesta ar trebui să fie dezinstalat sau dezactivat pentru a preveni înregistrarea ulterioară a datelor sensibile.

Analiza impactului keylogger-ului:

Echipa ar trebui să determine ce date au fost înregistrate de keylogger în cele două săptămâni. Aceasta implică identificarea și verificarea datelor înregistrate, cum ar fi parole, nume de utilizator și alte informații sensibile.

Determinarea sursei și scopului keylogger-ului:

Echipa ar trebui să investigheze cum a fost instalat keylogger-ul și care a fost scopul acestuia. S-a făcut acest lucru de către cineva din interiorul organizației sau de către o entitate externă? Este vorba de o amenințare intenționată sau de o eroare neintenționată?

Evaluarea impactului asupra securității datelor:

Trebuie să se evalueze dacă datele înregistrate de keylogger au ajuns în mâinile neautorizate sau dacă au fost utilizate în moduri care pot pune în pericol securitatea organizației.

Revizuirea politicilor de securitate:

Dacă keylogger-ul a fost instalat pe un computer intern, este important să se revizuiască politicile de securitate și să se determine cum a fost posibilă instalarea acestuia. Este nevoie de măsuri suplimentare pentru a preveni astfel de incidente în viitor.

Comunicarea internă și externă:

Dacă incidentul are un impact semnificativ asupra securității datelor sau a confidențialității, ar trebui să se comunice incidentul părților interesate, inclusiv departamentului juridic, departamentului de resurse umane și, în funcție de natura incidentului, autorităților competente.

Monitorizarea ulterioară:

După ce keylogger-ul a fost îndepărtat și impactul a fost evaluat, echipa ar trebui să monitorizeze continuu sistemul pentru a se asigura că nu există alte amenințări sau comportamente suspecte.

Măsuri de prevenire suplimentare:

Pentru a preveni incidente similare în viitor, echipa ar trebui să pună în aplicare măsuri de securitate suplimentare, cum ar fi autentificarea cu doi factori, formare în securitate cibernetică pentru angajați și monitorizarea continuă a sistemelor.

Abordarea trebuie să fie echilibrată, axându-se atât pe remedierea incidentului cât și pe prevenirea viitoarelor incidente de securitate.

Peer-to-Peer File Sharing

Organizația a interzis utilizarea serviciilor de partajare a fișierelor de tip peer-to-peer. Senzorii de detectare a intruziunii la nivelul rețelei organizației au abilitatea de a detecta utilizarea mai multor servicii populare de partajare a fișierelor de tip peer-to-peer. Într-o seară de luni, analistul ce se ocupă de detectarea intruziunilor la nivelul rețelei observă că au avut loc mai multe alerte privind partajarea de fișiere în ultimele trei ore, toate implicând aceeași adresă IP internă.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?
- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul organizației ar trebui implicate în soluționarea incidentului?
- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?
- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?
- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?
- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?
- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

Intrebari specifice

- Ce criterii de evaluare ar trebui folosite pentru a prioritiza modul în care acest incident este tratat (de exemplu, conținutul fișierelor care sunt distribuite)?
- Ce aspecte privind confidențialitatea ar putea influența modul în care acest incident este abordat?
- Cum s-ar schimba modul de abordare al acestui incident în cazul în care computerul care efectuează partajarea de fișiere peer-to-peer conține informații sensibile (spre exemplu, informații personale de identificare)?

Worm and Distributed Denial of Service (DDoS) Agent Infestation

Într-o dimineață de marți, un nou tip de ”vierme” este lansat în rețea; acesta se răspândește prin intermediul suporturilor de memorie portabile și se poate copia singur pe stațiile de lucru, având și posibilitatea de a deschide datele/folder-ele personale de pe un sistem de operare Windows sau de a porni anumite procese. În momentul în care viermele infectează o stație (host), acesta instalează un agent DDoS (Distributed Denial of Service). O organizație a fost infectată cu câteva ore înainte ca semnăturile antivirus să devină disponibile, iar viermele a avut timp să se răspândească.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?
- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul organizației ar trebui implicate în soluționarea incidentului?
- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?
- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?
- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?
- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?
- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

Intrebari specifice

- Cum s-ar putea identifica toate host-urile infectate?
- Cum ar fi putut organizația să împiedice intrarea viermelui înainte ca semnăturile antivirus să fi intrat in funcțiune?
- Cum ar fi putut organizația să împiedice răspândirea viermelui la nivelul rețelei de către host-urile infectate înainte ca semnăturile antivirus să fi intrat in funcțiune?
- Ar putea organizația să găsească o soluție de compromis pentru stațiile vulnerabile? Dacă da, cum ar putea fi făcută aceasta?
- Ce s-ar întâmpla și ce s-ar putea face în cazul în care host-urile infectate cu agentul DDoS au fost configurate să atace site-ul unei alte organizații în dimineața următoare?
- Cum s-ar schimba modalitatea de tratare a acestui incident în cazul în care unul sau mai multe host-uri infectate conțin informații sensibile despre angajații organizației?
- Cum ar trebui echipa (echipa de intervenție în caz de incident) să-i țină informați pe utilizatorii rețelei din cadrul organizației despre starea incidentului?
- Ce măsuri suplimentare ar putea fi luate pentru host-urile care nu sunt conectate la rețea la momentul respectiv (de exemplu, personal ce se află în vacanță, angajați externi ce se conectează ocazional, etc)?

Stolen Documents

Într-o dimineață de luni, departamentul juridic al organizației primește un apel telefonic din partea Biroului Federal de Investigații (FBI) cu privire la anumite activități suspecte ce implică sistemele organizației. Mai târziu în acea zi, un agent FBI se întâlnește cu conducerea și departamentul juridic al organizației pentru a discuta problemele apărute. Agentul le explică participanților la întâlnire că FBI a studiat și investigat activitatea de publicare a documentelor guvernamentale cu caracter sensibil, iar unele dintre documentele apărute în spațiul public aparțin organizației. Agentul FBI solicită asistență în rezolvarea cazului din partea organizației, iar consiliul de conducere cere ajutor echipei de intervenție în caz de incident pentru a obține dovezile necesare și a determina dacă aceste documente sunt legitime și cum s-au realizat scurgerile de informații.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?
- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul organizației ar trebui implicate în soluționarea incidentului?
- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?
- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?
- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?
- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?
- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

Intrebari specifice

- Din ce surse ar putea echipa aduna probe?
- Ce ar putea face echipa pentru a păstra confidențialitatea anchetei?
- Cum s-ar schimba modul de abordare al acestui incident în cazul în care echipa descoperă că o stație internă este a fost responsabilă pentru scurgerile de informații?
- Cum s-ar schimba modul de abordare al acestui incident în cazul în care echipa găsește un ”rootkit” instalat pe stația internă ce a fost găsită vinovată pentru scurgerile de informații? (rootkit – o colecție de mai multe software-uri malițioase ce pot oferi accesul la un computer unui utilizator neautorizat)

Compromised Database Server

Într-o seară de marți, un administrator al bazei de date efectuează o serie de operații de administrare în afara orelor de program pe mai multe servere ale acestei bazei de date. Administratorul observă câteva nume de fișier necunoscute și neobișnuite pe unul dintre servere. După examinarea atentă a unora dintre fișiere, administratorul ajunge la concluzia că serverul a fost atacat și sună echipa de intervenție în caz de incident pentru asistență. În urma unei anchete ample, echipa stabilește că atacatorul a preluat accesul deplin asupra serverului în urmă cu șase săptămâni.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?
- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul organizației ar trebui implicate în soluționarea incidentului?
- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?
- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?
- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?
- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?
- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

Intrebari specifice

- Ce surse ar putea echipa să folosească pentru a determina momentul în care a avut loc incidentul?
- Cum s-ar schimba modul de abordare al acestui incident în cazul în care echipa constată că serverul bazei de date rulează un ”sniffer” și captează parolele din rețea? (sniffer - program sau script folosit pentru a detecta și înregistra informații clasificate, în special parole pentru a obține acces la fișiere sau rețele de calculatoare)
- Cum s-ar schimba modul de abordare al acestui incident în cazul în care echipa constată că pe server rula în background o aplicație care putea copia bazele de date cu informații sensibile despre clienți în fiecare noapte și le putea transfere către o adresă externă?
- Cum s-ar schimba modul de abordare al acestui incident în cazul în care echipa găsește un ”rootkit” instalat pe server? (rootkit – o colecție de mai multe software-uri malițioase ce pot oferi accesul la un computer unui utilizator neautorizat)

Anonymous Threat

Într-o seară de joi, departamentul de securitate al organizației primește un apel telefonic de la șeful sectorului IT, acesta raportând că doi dintre angajații săi tocmai au primit o serie de amenințări anonime împotriva sistemelor organizației. Pe baza unei investigații, departamentul de securitate consideră că amenințările ar trebui luate în serios și informează echipele interne corespunzătoare, inclusiv echipa de intervenție în caz de incidente.

Intrebari generale

- Câți membri ai echipei ar trebui să participe/să se implice la rezolvarea acestui incident?
- În afara echipei (echipa de intervenție în caz de incident), ce grupuri din cadrul organizației ar trebui implicate în soluționarea incidentului?
- Cărei entități din exterior ar trebui raportat acest incident? Când ar trebui raportat? În ce mod ar trebui efectuată raportarea? Ce informații ar trebui sau n-ar trebui raportate și de ce?
- Ce alte căi/relații de comunicare cu entități exterioare ar mai putea apărea?
- Ce instrumente și resurse ar trebui echipa să folosească pentru tratarea acestui incident?
- Ce aspecte ale procesului de tratare al incidentului ar fi fost diferite dacă incidentul ar fi avut loc în altă zi și la altă oră (în timpul programului de lucru vs. în afara programului de lucru)?
- Ce aspecte ale procesului ar fi fost diferite dacă incidentul ar fi avut loc într-o altă locație fizică?

Intrebari specifice

- Ce ar trebui să facă echipa sau cum ar trebui să răspundă în legătură cu amenințările anonime primite?
- Ce impact ar avea accentuarea controalelor de securitate asupra modului în care se răspunde la incidente de genul acesta?