Tema 10 Securitate ofensiva

Scenariul nr. 1

Mai multe departamente ale companiei observă o întrerupere neașteptată în funcționarea rețelei. După ce discuți cu diverse departamente, colectează informații despre problemă și coordonează acțiuni comune pentru a identifica și rezolva cauzele întreruperii. Oferă o descriere detaliată a pașilor necesari pentru a clarifica circumstanțele problemei, pentru a colabora cu colegii și pentru a soluționa eficient situația.

1. Colectare informații - Contactez imediat departamentele afectate și solicit detalii specifice despre problemele întâmpinate. Verific logs-urile de sistem și monitorizarea rețelei pentru a identifica anomalii. Stabilesc cronologia exactă a incidentului.
2. Coordonare echipe - Formez rapid o echipă de intervenție cu specialiști IT, securitate și reprezentanți departamentali. Creez un grup Microsoft Teams pentru comunicare în timp real. Îmi asum rolul de coordonator central.
3. Diagnosticare problema - Verific serverele, routerele și conexiunile fizice. Testez conectivitatea între nodurile critice. Analizez traficul de rețea pentru a identifica tipare suspecte.
4. Implementare soluție - Aplic măsuri imediate pentru a restabili serviciile esențiale. După identificarea cauzei principale, implementez soluția permanentă. Monitorizez atent sistemele după remediere.
5. Documentare și prevenție - Creez un raport detaliat al incidentului. Organizez o întâlnire post-incident cu toate echipele. Actualizez procedurile și implementez măsuri preventive.

Exemplu: Atac DDoS

- Primesc alerte de la mai multe departamente despre întreruperi de rețea. Observ imediat trafic anormal de mare în logs-uri.

- Convoc echipa de intervenție și anunț: "Avem indicii clare de atac DDoS. Vedem trafic masiv pe porturile 80 și 443 din multiple surse IP."

- Implementez filtrare de trafic la nivel de firewall. Contactez ISP-ul: "Experimentăm un atac DDoS semnificativ, avem nevoie de asistență pentru filtrare upstream."

- Activez serviciul nostru de mitigare DDoS. Redirecționez traficul prin soluția cloud anti-DDoS.

- Serviciile sunt restaurate. Continui monitorizarea și ajustez filtrele în funcție de evoluția atacului.

- Realizez analiza detaliată a atacului și implementez reguli permanente de protecție la nivelul firewallului și al sistemului de prevenire a intruziunilor.

Scenariul nr. 2

Compania a fost victima răspândirii de software malițios printr-un atac de tip phishing. Sarcina ta este să reacționezi imediat la acest incident, inclusiv să izolezi amenințarea, să analizezi daunele și să restabilești securitatea rețelei. Oferă o descriere detaliată a pașilor ce trebuie urmați pentru a soluționa incidentul și a strategiilor pentru a preveni astfel de atacuri în viitor.

1. Reacționare imediată - Izolez sistemele infectate, notific echipa de securitate și colectez probe digitale. Identific email-ul malițios și alertez toți utilizatorii.

2. Analiză incident - Examinez malware-ul în mediu izolat, verific logs-urile și identific sistemele compromise. Determin impactul și datele afectate.

3. Remediere situație - Elimin malware-ul, resetez credențialele, aplic patch-uri necesare și restaurez din backup-uri verificate.

4. Prevenire incidente viitoare - Implementez autentificare multi-factor, actualizez filtrele anti-spam și organizez training de conștientizare.

5. Documentare și raportare - Creez un raport detaliat și organizez analiză post-incident.

Exemplu practic:

* Primesc alertă despre activitate suspectă. Descopăr un email de phishing care pretinde a fi o factură urgentă.
* Izolez stațiile de lucru infectate și notific: "Am identificat un atac de phishing cu malware care se propagă. Deconectați imediat sistemele suspecte."
* Extrag mostre de malware pentru analiză și descopăr că acesta fură credențiale și încearcă să se răspândească lateral.
* Utilizez instrumentele de remediere pentru a elimina malware-ul și resetez toate parolele conturilor afectate.
* Restaurez sistemele compromise din backup-uri și verific integritatea acestora.
* Implementez reguli suplimentare în gateway-ul de email și organizez sesiune de instruire pentru toți angajații privind recunoașterea atacurilor de phishing.

Scenariul nr. 3

Un angajat încearcă să obțină ilegal acces la datele confidențiale ale companiei. Descrie abordarea ta pentru a detecta această amenințare, pentru a dezvolta mecanisme de detectare și prevenire a amenințărilor interne, precum și strategiile pentru a preveni astfel de cazuri în viitor. Răspunsul tău trebuie să includă descrierea fiecărei etape a procesului de detectare și prevenire a amenințărilor interne, precum și recomandări concrete pentru îmbunătățirea protecției datelor companiei.

1. Detectare comportament suspect - Monitorizez activitatea neobișnuită: accesări de date în afara programului, volume mari de descărcări, accesarea fișierelor fără justificare legitimă.

2. Investigare amenințare - Colectez dovezi digitale, analizez logs-urile de acces și activitățile utilizatorului suspect. Documentez toate acțiunile pentru investigații ulterioare.

3.Răspuns la incident - Revoc temporar accesul angajatului, notific managementul și departamentul juridic. Previn răspândirea incidentului și protejez datele sensibile.

4. Implementare măsuri preventive - Aplic principiul privilegiului minim, segmentez accesul la date și implementez monitorizare avansată a comportamentului utilizatorilor.

5. Îmbunătățire politici- Revizuiesc procedurile de angajare și acordare a accesului. Implementez verificări periodice și instruiri de conștientizare.

Exemplu practic:

- Soluția DLP alertează despre transfer neautorizat de documente financiare marcate ca "Confidențial" către un drive USB.

- Inițiez investigația și descopăr că angajatul a încercat să dezactiveze agenții DLP și a ocolit restricțiile de copiere pentru baza de date clientVIP.

- Raportez incidentul: "DLP a blocat exportul neautorizat de date sensibile. Utilizatorul a încercat multiple metode de ocolire a protecțiilor."

- Suspend temporar contul angajatului și securizez stația de lucru pentru analiză forensică.

- Actualizez politicile DLP pentru a restricționa mai bine transferurile de date și implementez monitorizare endpoint avansată.