Incident report analysis -

Datum: 20-02-2025

Rapport skriven av: Zayn AK

Summary	Företagets interna nätverkstjänster **slutade fungera i två timmar** på grund av en **DDoS-attack**. Angriparen använde en **flod av ICMP-paket** för att överbelasta nätverket, vilket ledde till att normal nätverkstrafik **inte kunde nå företagets resurser**. Angriparen utnyttjade en **felkonfigurerad brandvägg** som **inte hade några begränsningar för ICMP-trafik**. • Ingen **verifiering av käll-IP-adresser** fanns på plats, vilket gjorde att angriparen kunde använda **spoofade IP-adresser**. • Företaget hade **ingen aktiv nätverksövervakning**, vilket gjorde det svårt att upptäcka attacken i realtid.
Identify	• Brandväggen **saknade regler** för att hantera ICMP-trafik. • Ingen **övervakning av nätverkstrafik** identifierade den plötsliga ökningen av ICMP-paket. • **IP-adressverifiering saknades**, vilket möjliggjorde **spoofade IP-adresser**. • **Ingen begränsning av nätverkstrafik** gjorde att systemet lätt kunde överbelastas.

Protect	• Brandvägg uppdatering - Inför regler för att begränsa ICMP-trafik och blockera skadliga anslutningar. • IP-verifiering - Brandväggen verifierar nu IP-adresser för att blockera spoofade paket. • Nätverksövervakning Inför SIEM-system för att analysera och varna vid ovanlig trafik. • Intrångsdetektering (IDS/IPS) System för att filtrera och blockera skadlig ICMP-trafik.
Detect	**Live-nätverksövervakning** - Spåra och analysera ICMP-trafik i realtid. **SIEM-logganalys** - Automatiserad analys av nätverkstrafik och säkerhetshändelser. **Brandväggsloggar** - Regelbundna granskningar för att upptäcka mönster i DDoS-attacker. **Strategi:** Använda **AI-drivna övervakningsverktyg** för att identifiera och blockera attacker i realtid.
Respond	Vid framtida attacker ska säkerhetsteamet vidta följande åtgärder: 1. **Avskärma angriparen** – Blockera skadlig trafik genom **brandväggsregler**. 2. **Aktivera nödlägen** – Stäng av icke-kritiska tjänster för att begränsa påverkan. 3. **Analysera attack**– Samla in loggar och analysera **intrångs data.**

	4. **Samverka med internetleverantörer** – be ISP om hjälp med att blockera attack trafik.
Recover	**Systemåterställning -** Se till att alla nätverkstjänster är i drift igen. **Säkerhetsuppdateringar** - uppdatera konfigurationer för att förhindra liknande attacker. **Simulering av attacker** - Genomföra tester för att validera säkerhetsförbättringar. **Revidering av säkerhetsprotokoll** - Säkerställa att rätt processer finns på plats för framtiden.

Reflections/Notes:

DDoS-attacken orsakade stor påverkan på verksamheten genom att utnyttja brister i nätverkskonfigurationen. Genom att implementera brandväggsregler, SIEM-verktyg och intrångsdetektering kan företaget minimera risken för framtida incidenter.

📌 **Viktiga lärdomar**

Felkonfigurerade brandvägg möjliggjorde attacken ⟶ Fixad med nya regler.

Brist på övervakning ⟶ åtgärd med SIEM och IDS/IPS.

Attacken använde ICMP-paket ⟶ Nu begränsat och filtrerat.

Ett incidenthantering protokoll är på plats för framtida attacker.