

Inlämningsuppgift 2: Cybersäkerhetsrisker, incidenthantering och strategier

Syfte

Denna uppgift syftar till att studenten får möjlighet att analysera cybersäkerhetsincidenter genom att använda etablerade modeller som Kill Chain och de fem säkerhetsprinciperna (Defense in Depth, Least Privilege, Separation of Duties, Security by Design och KISS), samtidigt som **CIA-triaden (Confidentiality, Integrity, Availability)** används för att bedöma och säkerställa skyddet av digitala tillgångar.

Uppgiftsbeskrivning

Du ska analysera och hantera ett cybersäkerhetsincident-scenario där du beskriver attackens förlopp, identifierar sårbarheter och tillämpar relevanta principer för att föreslå åtgärder. Din lösning ska integrera Kill Chain, de fem säkerhetsprinciperna samt CIA-triaden för att säkerställa en heltäckande strategi. Reflektera också över juridiska och etiska aspekter.

Scenario

Du arbetar som cybersäkerhetskonsult åt **SecureCom AB**, ett medelstort företag med 150 anställda. Företaget erbjuder molnbaserade IT-lösningar för små och medelstora kunder, inklusive datalagring och applikationshosting. SecureCom hanterar känsliga kunduppgifter som personuppgifter, kontrakt och finansiell information.

Företaget har nyligen utsatts för ett omfattande ransomware-angrepp. Angriparna använde en riktad **phishing-kampanj** för att kompromettera en anställds e-postkonto och därigenom få åtkomst till företagets interna system. Efter att ha rört sig lateralt inom nätverket lyckades angriparna kryptera en stor del av företagets databaser, inklusive både kunddata och interna affärskritiska filer.

Bakgrundsinformation om SecureCom AB

1. IT-miljö:

- Företaget använder en hybrid molnmodell med servrar både lokalt och hos en extern molnleverantör.
- De har en grundläggande brandvägg och antivirusprogram, men saknar avancerade övervakningssystem som EDR (Endpoint Detection and Response).
- Åtkomst till system regleras via lösenord, men det finns ingen tvåfaktorsautentisering (2FA).

2. Angreppet:

- Angriparna använde phishing för att lura en medarbetare att öppna ett skadligt e-postmeddelande som såg ut att komma från en välkänd leverantör.
 - Ett ransomware-program laddades ner och installerades. Detta krypterade inte bara filer lokalt utan även säkerhetskopior i det lokala nätverket som var dåligt segmenterade.
 - Angriparna kräver 200 000 euro i lösensumma och hotar att publicera kunddata om inte pengarna betalas inom sju dagar.
3. **Pågående konsekvenser:**
- Företaget har förlorat tillgång till en stor del av sin data, vilket har stoppat flera affärsprocesser.
 - Kunder har börjat klaga på avbrutna tjänster, och företagets rykte står på spel.
 - Företaget är också juridiskt ansvarigt enligt GDPR att rapportera incidenten inom 72 timmar.

Instruktioner

1. **Hotbedömning och analys med Kill Chain (3 sidor):**
 - **Beskriv hotets förlopp** genom Kill Chain-modellen:
 - **Reconnaissance:** Hur angriparen samlade information.
 - **Weaponization:** Verktyg och tekniker som användes.
 - **Delivery:** Hur attacken levererades (t.ex. phishing).
 - **Exploitation, Installation, Command and Control, Action on Objectives:** Hur angreppet genomfördes steg för steg.
 - Identifiera sårbarheter och kritiska punkter i företagets försvar.
2. **CIA-triaden och påverkan på systemets säkerhet (2 sidor):**
 - Analysera hur angreppet påverkar de tre grundläggande aspekterna:
 - **Confidentiality (Sekretess):** Vilka data riskeras att exponeras?
 - **Integrity (Integritet):** Hur har datans noggrannhet och pålitlighet påverkats?
 - **Availability (Tillgänglighet):** Hur har system och tjänster påverkats av attacken?
 - Diskutera vilka åtgärder som behövs för att återställa och skydda varje aspekt av CIA-triaden.
3. **Åtgärdsplan baserad på de fem principerna (3 sidor):**
Föreslå en åtgärdsplan för att hantera incidenten och bygga ett mer motståndskraftigt försvar:
 - **Defense in Depth:** Hur flera lager av säkerhet kan minska risken för framtida attacker.
 - **Least Privilege:** Hur åtkomstbegränsning kan minska skador vid intrång.
 - **Separation of Duties:** Hur arbetsuppgifter kan delas för att förhindra missbruk.
 - **Security by Design:** Hur system kan utformas för att vara säkra från början.

- **KISS (Keep It Simple, Stupid):** Hur säkerhetslösningar kan hållas enkla och effektiva.
- 4. **Juridiska och etiska överväganden (1-2 sidor):**
 - Analysera juridiska frågor som rör dataskydd, t.ex. GDPR och rapporteringsskyldigheter.
 - Reflektera över etiska dilemman, som huruvida det är rätt att betala lösensumma.
- 5. **Reflektion och långsiktig förbättringsplan (1-2 sidor):**
 - Reflektera över vilka lärdomar organisationen kan dra av incidenten.
 - Beskriv en långsiktig strategi som inkluderar utbildning, regelbunden säkerhetsgenomgång och implementation av branschstandarder.
- 6. **Skapa en riskmatris (1-2 sidor):**
 - Identifiera minst fem risker som uppstod i samband med incidenten.
 - Bedöm varje risk utifrån sannolikhet och påverkan, och placera dem i en riskmatris.
 - Diskutera prioriteringar baserat på matrisen och föreslå åtgärder för de mest kritiska riskerna.

Bedömningskriterier

- **Godkänt (G):**
 - Studenten identifierar och beskriver hot och sårbarheter genom Kill Chain.
 - Skapar en korrekt riskmatris och prioriterar åtgärder baserat på den.
 - Relaterar åtgärder till CIA-triaden och de fem principerna.
 - Reflekterar över juridiska och etiska aspekter samt föreslår en lösning.
- **Väl godkänt (VG):**
 - Genomför en djupgående analys av hot och incidentens förlopp med Kill Chain.
 - Skapar en detaljerad och välmotiverad riskmatris med genomtänkta åtgärdsförslag.
 - Kopplar på ett tydligt och innovativt sätt sina åtgärder till CIA-triaden och de fem principerna.
 - Visar förståelse för hur juridiska och etiska frågor integreras i strategiska beslut.

Inlämning

- Längd: 10-15ish sidor exklusive referenser.
- Referenser skall vara med.
- Format: PDF, inlämnad via lärplattformen.

- Deadline: Söndag, vecka 51 kl. 23:59.