Proaktiv säkerhet och försvar i cybersäkerhet

Robin Kamo

Nion

Vad är ISO 27001

- Internationell standard för informationssäkerhet
- Vanligaste standarden för cybersäkerhet: ISO 27001
- Syfte: Skydda information och strukturera säkerhetsarbete genom en Information Security Management System (ISMS)
- Bygger på PDCA

Vad krävs för att följa ISO 27001?

För att följa ISO 27001 krävs:

- Implementering av kontroller: till exempel åtkomst, säkerhetskopiering, och loggning
- Skapande och underhåll av policyer för informationssäkerhet
- Regelbunden utbildning av personal i säkerhetsprinciper
- Kontinuerlig granskning och förbättring av säkerhetsarbetet

Riskbedömning och Hotanalys

Riskbedömning:

Identifiera, bedöma och prioritera risker. Vilka hot kan drabba vårt system, och hur allvarliga är de? Identifiera och prioritera risker baserat på sannolikhet och konsekvenser

Hotanalys:

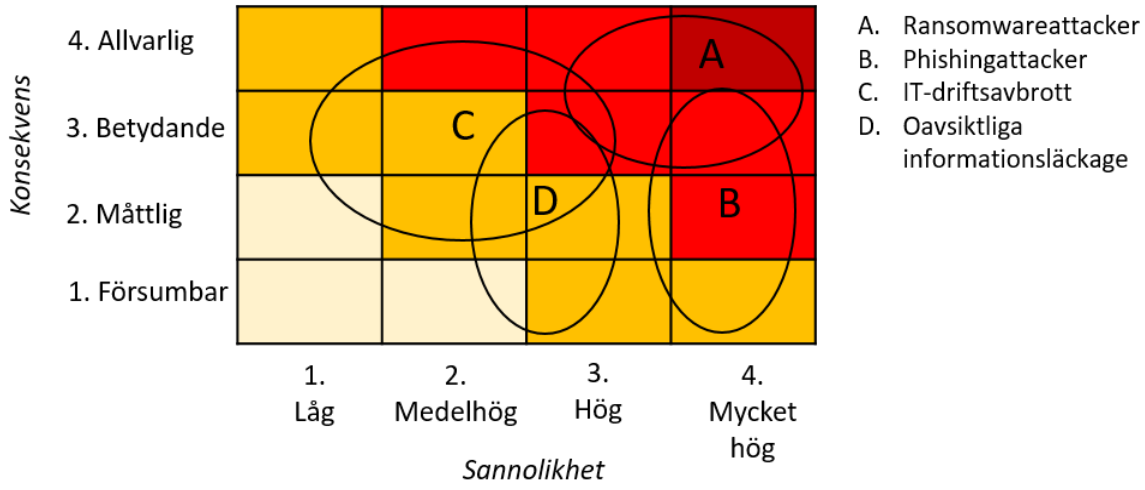
Genom att analysera potentiella hot, identifieras sårbara punkter och skyddsåtgärder utvecklas.

Riskmatris

- En riskmatris används för att visuellt prioritera risker
- Risker bedöms efter sannolikhet och konsekvens

Murphys Law:

- Anything that can go wrong will go wrong. If there is a possibility of several things going wrong, the one that will cause the most damage will be the one to go wrong. Corollary: If there is a worse time for something to go wrong, it will happen then.



Riskmatris

Risk	Sannolikhet	Konsekvens	Risknivå	Åtgärd/Förslag
Obehörig åtkomst	Hög	Hög	Kritisk	Implementera tvåfaktorsautentisering och åtkomstkontroll
Ransomware-angrepp	Medel	Hög	Hög	Säkerhetskopiera data regelbundet; utbilda personal i phishing
Phishing (nätfiske)	Hög	Medel	Hög	Träning för personal; användning av e-postfiltrering
Dataförlust (av misstag)	Låg	Medel	Måttlig	Automatiska säkerhetskopior; tydliga databehandlingspolicyer
Insiderhot (anställd)	Låg	Hög	Hög	Åtkomstbegränsning; regelbunden övervakning och revision
Svaga lösenord	Hög	Medel	Hög	Implementera lösenordspolicy; använd tvåfaktorsautentisering
Systemfel (serverkrasch)	Medel	Hög	Hög	Regelbunden systemuppdatering; redundans och säkerhetskopiering

Säkerhetsarkitektur

En strukturerad uppsättning av säkerhetsåtgärder som appliceras på en IT-miljö för att skapa skydd.

Exempel: Booking.com

Tillgångsskydd: Skydda användardata, betalningsinformation, och bokningsinformation.

Segmentering: Dela upp nätverket i olika delar för att minska risk om ett område utsätts för intrång.

Åtkomstkontroll: Endast behörig personal får komma åt kritiska system, med tvåfaktorsautentisering.

Incidenthantering och Återställningsplan

- **Incidenthantering**: Struktur för att upptäcka, isolera och åtgärda intrång
- **Återställningsplan**: Plan för att återgå till normal drift efter incident

Roller inom Cybersäkerhet

- **Cybersecurity Analyst**: Övervakar nätverk och system
- **Incident Response Technician**: Arbetar med incidenthantering
- **Risk Analyst**: Gör riskbedömningar och analyser

Roller inom Cybersäkerhet

- **Cybersecurity Analyst**: Övervakar nätverk och system
- **Incident Response Technician**: Arbetar med incidenthantering
- **Risk Analyst**: Gör riskbedömningar och analyser

Inlämningsuppgift 1