IT-säkerhet mm

Anders Olsson

Allmänt om cyberattacker

- Antalet cyberattacker ökar för varje år och andelen ransomware-attacker ökade med cirka 300 procent globalt under 2021
- Såväl privata som offentliga aktörer har blivit drabbade

➢ Syfte med attacker

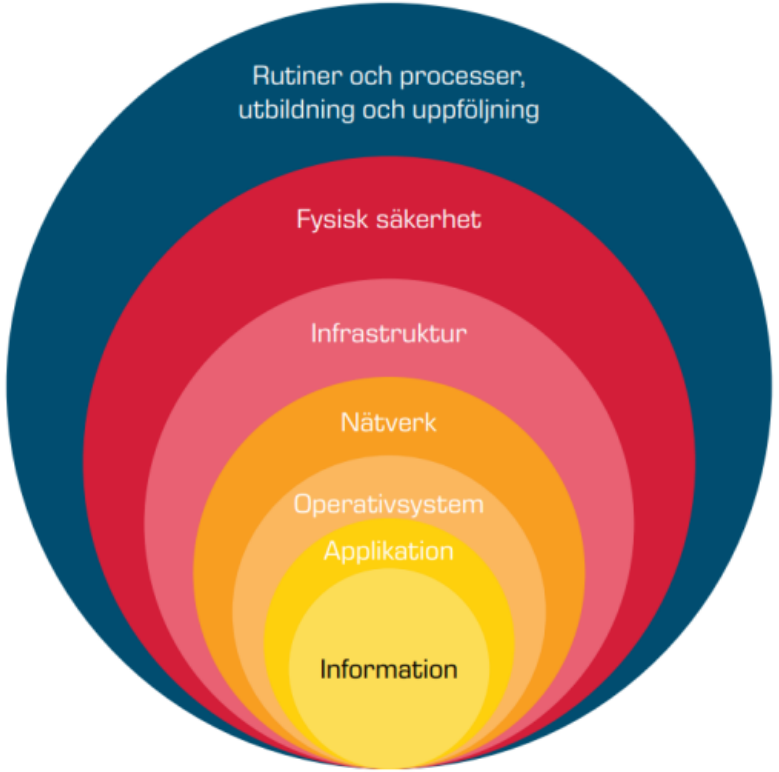
➢ Vem utför attacker

➢ Hur utförs attacker

Strategier för utformning av säkerheten

- Systematiskt informationssäkerhetsarbete inom alla verksamheter
- Riskbaserat
- Kontinuitetsplanering såväl teknik som verksamhetsmässig
- Utgå från att någon obehörig finns i vår IT-miljö

Lökprincipen – defence in depth



Vad gör vi för att skydda oss –
ett urval av genomförda åtgärder

- Information och utbildning av användare
- Virusskydd klienter och servrar
- Säkrare (längre) lösenord
- ”Karantän” för misstänkt e-post och bilagor
- Undvika att många har höga behörigheter – helst att man ”eleverar sig vid behov” exv ”make med admin” men även för högre behörigheter.
- Begränsar hur olika systemmiljöer kan nå varandra i händelse av ett intrång
- Loggning och övervakning
- Systematiskt sårbarhetsarbete

MSB’s rekommendationer

- Se till att multifaktorsautentisering används för all distansanslutning till nätverket samt alla användarkonton, särskilt administratörs- och andra priviligierade konton.
- Se till att all kommunikation med organisationens nätverk och tjänster säkras genom exempelvis vpn-anslutning.
- Se över vilka användare som har administratörsrättigheter, så att endast it-avdelningen kan installera programvara.
- Öka kontrollen och vaksamheten kring avvikelser på systemnivå.
- Kontrollera resultat från backuper, samt säkerställ att offline-kopior finns.
- Blockera icke auktoriserad programvara, tillåt endast att användare kör godkända applikationer.
- Installera säkerhetsuppdateringar så fort det är möjligt. Prioritera system som exponeras mot internet, de som är verksamhetskritiska och system där sårbarheter riskerar att utnyttjas.