Sammanfattning av presentationen om informations- och cybersäkerhet – vad skyddar vi oss egentligen emot?

Vilka är de största hoten? Hur kan vi jobba praktiskt för att motverka säkerhetsrisker? Region Halland delar med sig av konkreta exempel från arbetet inom informations- och cybersäkerhetsområdet.
***Anders Boustedt**, verksamhetschef IT och digitalisering, **Fredrik Gustavsson**, avdelningschef Informationsteknologi, **Johan Hortling**, systemtekniker och **Felicia Svantesson**, systemtekniker*

1. Omvärldsläget förändrar hotbilden

Fredrik började med att sätta cybersäkerhet i ett större sammanhang. Han betonade att omvärldsläget påverkar säkerhetsområdet mer än många tror. Han lyfte särskilt fram:

- kriget i Ukraina och ett fortsatt aggressivt Ryssland
- konflikten mellan Kina och Taiwan
- konflikterna i Mellanöstern, bland annat kopplat till Iran

Hans poäng var att hotbilden håller på att skifta. Tidigare har mycket handlat om utpressningsvirus (ransomware), men nu ser man mer underrättelseinhämtning, statsstödda aktörer och mer sofistikerade metoder. Det blir alltså svårare att skydda sig.

Han tog också upp att cyberkrigföring blir ett allt mer sannolikt första steg i en konflikt. Det behöver inte börja med bomber och missiler. Han nämnde även exempel på att datacenter faktiskt blivit fysiskt attackerade, samt att intrång mot stora företag som Ericsson kopplats till statsstödda aktörer. I Sverige nämndes bland annat angrepp mot Region Värmland och CGI.

Samtidigt beskrev han en annan trend: större organisationer har blivit bättre på att skydda sig, vilket gör att många kriminella grupper i högre grad riktar in sig på små och medelstora aktörer.

2. Från tekniskt problem till verksamhetsrisk

Därefter tog Anders vid och flyttade perspektivet från teknik till verksamhet. Han knöt an till att IT, digitalisering och verksamhetsutveckling inte längre kan ses som separata saker. Detsamma gäller säkerhet.

Med stöd i Gartner beskrev han att cybersäkerhet inte längre ses som ett rent tekniskt problem, utan som verksamhetsrisker och affärsrisker. Fokus bör därför inte bara ligga på att försöka stoppa allt, utan på att bygga förmåga att klara angrepp när de kommer.

Han betonade ett skifte från förebyggande arbete till resiliens:

- hur man minimerar verksamhetspåverkan
- hur man står emot störningar
- hur man återhämtar sig

Cyberrisker går att hantera men aldrig eliminera helt. Därför måste cybersäkerhet byggas in i vanliga verksamhetsprocesser och i det löpande utvecklingsarbetet.

3. Vad EDR är och varför det behövs

Johan tog över och pratade om EDR, alltså skydd för klienter, telefoner, servrar och andra ’endpoints’.

Han förklarade skillnaden mellan traditionellt antivirus och EDR:

- traditionellt antivirus bygger mycket på signaturer eller fingeravtryck av filer
- det är relativt enkelt för angripare att ändra en fil så att signaturen inte längre känns igen
- EDR innehåller fortfarande signaturer, men är mycket bredare

EDR samlar in data från många enheter och korrelerar informationen centralt. Det ger:

- bättre överblick
- bättre logganalys
- bättre spårbarhet
- bättre möjlighet att upptäcka avvikelser

Han lyfte också att EDR öppnar för automatisering, larm och incidenthantering. Men ett viktigt budskap var att verktyget inte fungerar av sig självt. Det kräver människor som aktivt följer upp, analyserar och agerar på larm.

4. Konkreta exempel: ClickFix-angrepp via kompromitterad webbplats

Sedan beskrev Johan och Felicia ett konkret angrepp som Region Halland hanterat.

Det handlade om en leverantörswebbplats som regionen använde för inköp. Sajten hade blivit kompromitterad och angriparen hade lagt in skadlig kod. Själva sidan såg normal ut, men när användaren gick in kunde en falsk verifieringsruta visas, inspirerad av Cloudflare.

Angreppet fungerade så här:

- användaren klickade på en falsk verifiering
- därefter fick användaren instruktioner att trycka Windows+R, sedan Ctrl+V och Enter
- i själva verket hade ett skadligt kommando redan kopierats till urklipp
- kommandot startade PowerShell dolt i bakgrunden
- en fil laddades ner till datorn och kördes
- datorn infekterades

Felicia visade att kommandot hämtade en körbar fil från en skadlig domän och exekverade den. De bedömde att syftet sannolikt var att stjäla information, exempelvis cookies och lösenord.

Det intressanta var också att attacken bara utlöstes i vissa webbläsare, vilket visade att angriparen lagt ned tid på att göra angreppet mer selektivt och svårt att upptäcka.

När Region Halland upptäckte detta via EDR:

- blockerade de den kompromettерade webbplatsen
- kontaktade leverantören
- verifierade senare att sajten blivit sanerad innan blockeringen hävdes

Efter detta fick deltagarna diskutera hur de själva verifierar hot och incidenter.

5. Utbildning, phishingövningar och säkerhetskultur

Felicia gick sedan över till hur regionen arbetar med utbildning och övning.

Hon betonade att säkerhet är färskvara. Kunskap och förmåga måste tränas kontinuerligt för att säkerhetstänk ska bli en naturlig del av vardagen.

De arbetar bland annat med phishingövningar för alla anställda och hade genomfört tre sådana övningar.

Resultaten som visades var ungefär:

- första övningen: cirka 19 procent klickade
- andra övningen: cirka 4 procent skrev in sina inloggningsuppgifter
- tredje övningen: cirka 5 procent skrev in sina inloggningsuppgifter

Samtidigt rapporterade många användare mejlen, vilket presenterades som ett gott tecken. Rund tusen rapporteringar kom in via Outlook-funktionen vid varje utskick, plus ett antal ärenden via ärendehanteringssystemet.

Budskapet här var att rapporteringskulturen är viktig. När användare rapporterar kan säkerhetsteamet:

- undersöka mejlen
- hitta fler mottagare
- rensa bort meddelanden
- undersöka om någon klickat
- vid behov trigga automatiserade åtgärder, som lösenordsbyte eller återkallade sessioner

De visade också verkliga exempel på phishing från legitima, men kompromettерade, konton hos andra offentliga aktörer. Det ledde till en diskussion om att även legitima leverantörer ibland skickar mejl som ser så misstänkta ut att de i praktiken lär användarna fel beteende. Ett inspel från publiken var att krav bör ställas på leverantörers utskick, så att de inte underminerar organisationens säkerhetsarbete.

6. MISP och nationell informationsdelning

Johan gick sedan vidare till MISP, en nationell plattform för att dela information om sårbarheter, IOC:er (Indicators of Compromise)och hotaktörer.

Han berättade att MCF driver en större satsning för att få in kommuner, regioner, myndigheter och andra aktörer i en gemensam svensk MISP-plattform. Syftet är att snabbt kunna dela information om hot mellan offentliga aktörer.

Johan beskrev också en övning de deltagit i under hösten, där deltagarna jobbade i Blue Team (försvarare - upptäcker, förebygger och svarar på attacker) mot Red Team (angripare - hittar sårbarheter, gör intrång) i ett realistiskt scenario. Han tyckte att övningen var väl förberedd och pedagogisk.

Hans förhoppning var att satsningen på en gemensam svensk MISP ska bli framgångsrik, eftersom den skulle kunna ge ett snabbt och effektivt sätt att dela indikatorer och hotinformation mellan exempelvis regioner och kommuner. Han såg det som en av de största satsningarna på cyberområdet från nationellt håll.

7. Planerad ransomwareövning i Region Halland

Därefter berättade Johan att Region Halland planerar en ransomwareövning under våren.

Övningen ska inte bara omfatta IT-säkerhetsteamet utan även:

- serverpersonal
- nätverk
- klientfunktioner
- ledningsgrupper

Syftet är att testa om dokumentation, planer och resurser faktiskt håller när organisationen utsätts för ett allvarligt angrepp. Han uttryckte ganska tydligt att poängen med övningen sannolikt är att upptäcka brister och förbättra arbetssätten innan något verkligt händer.

Även här fick deltagarna kort diskutera hur de själva arbetar med cyberövningar.

8. CGI-incidenten och lärdomar om leverantörer

Sedan tog Johan upp det då aktuella intrånget hos CGI.

Han sa att CGI bekräftat ett dataintrång, men att ganska lite information hade kommit offentligt. CGI beskrev det som att en testmiljö drabbats, medan angriparen enligt Johan påstod att denne fått tag på källkod, lösenord och signerade dokument.

Han var tydlig med att detaljerna ännu var osäkra, men att Region Halland agerade snabbt eftersom de hade CGI-konsulter i sin egen miljö. De spärrade därför dessa konton och bytte lösenord redan nästa dag.

Den större lärdomen han drog handlade om default-konfigurationer:

- default-lösenord
- standardbehörigheter
- färdigkonfigurerade miljöer
- dåligt genomtänkt placering i nätverket

Han var tydlig i sitt budskap här: när man installerar system är man inte färdig när installationen är klar, det är då arbetet börjar. Man måste:

- byta standardlösenord

- ta bort onödiga konton
- se över behörigheter
- förstå vilket nätverk och vilka beroenden systemet har
- tänka på hela kedjan, inte bara själva applikationen

Han nämnde särskilt risker med exempelvis Docker-miljöer som körs med standardinställningar eller för höga rättigheter.

9. Avslutande budskap

Avslutningen hölls åter av Anders, som sammanfattade med några budskap:

- **Cybersäkerhet är en lagsport**
  Det är inte en fråga för en enskild person eller en liten grupp, utan ett gemensamt ansvar i hela verksamheten.
- **Teknisk skuld är ett stort problem**
  Gammal teknik i serverhallar, klienter och mobila enheter innebär många sårbarheter. Därför krävs bra processer för patchning och uppdatering. Tiden från upptäckt sårbarhet till faktisk exploatering blir allt kortare.
- **Omvärlden har förändrats**
  Hoten kommer inte bara från opportunistiska angripare och ekonomiskt motiverad brottslighet. Statsstödda aktörer kan ha som mål att skapa kaos och störa samhällsviktig verksamhet, inte att tjäna pengar.
- **Säkerhetskultur är avgörande**
  Teknik räcker inte om användare ändå klickar fel. Därför behövs phishingövningar, utbildning och kontinuerlig träning.
- **Man blir aldrig färdig**
  Cybersäkerhet är inget projekt som blir klart. Det är ett ständigt pågående arbete.

Kärnan i presentationen

Om man kokar ner presentationen till några få huvudpunkter så var budskapet ungefär detta:

Cybersäkerhet har gått från att vara en teknisk specialfråga till att vara en central verksamhetsfråga. Hotbilden blir mer komplex, mer geopolitisk och mer sofistikerad. Därför måste organisationer jobba både med teknik, övning, kultur, processer och leverantörsstyrning. Det viktiga är inte bara att försöka förhindra allt, utan att bygga motståndskraft när något faktiskt händer.