AI-analys

Cyberhot 2025: Så skyddar vi oss mot nya faror

Petra Klein
CSO, Swedbank

Tomas Beeckman-Norrström
operativ chef, Nationellt cybersäkerhetscenter

Moderator: Aline Peters
PwC

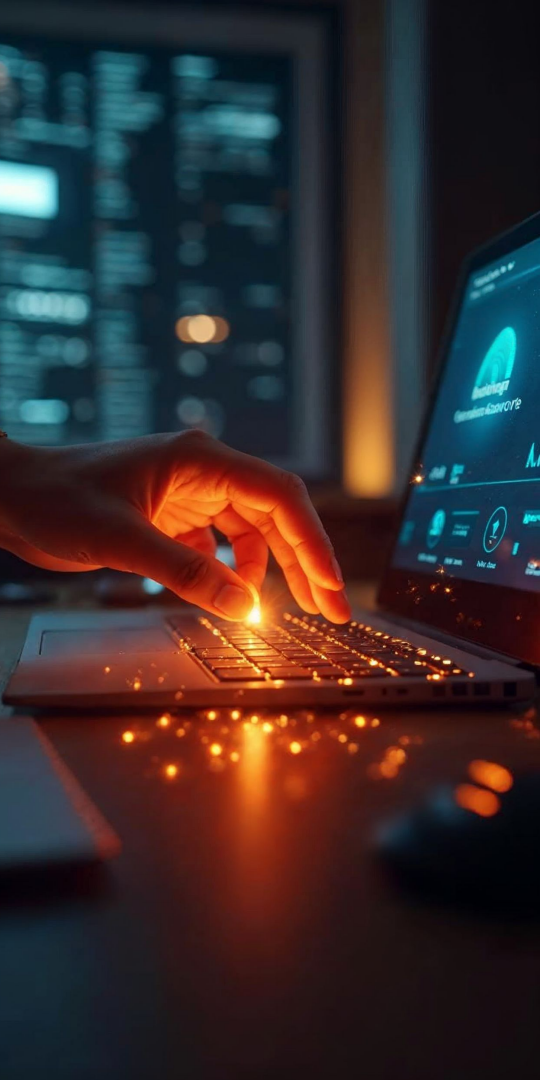
Moderator: Ulrika Fejne
PwC

Sammanfattning

Sessionen fokuserade på det växande hotet inom cybersäkerhet, med en presentation som belyste de viktigaste trenderna och hoten under det gångna året. Ett centralt tema var den ökande användningen av sårbarheter, med en 31% ökning av avslöjanden och utnyttjanden. Värt att notera är att proof-of-concept och dess tillgänglighet gör det enklare för både avancerade och mindre sofistikerade hotaktörer att genomföra attacker. Dessutom betonas samband mellan geopolitik och cyberattacker, där konflikter och politiska spänningar driver cyberoperationer, med Ryssland, Iran och Kina som framstående aktörer. AI och ransomware framhölls som betydande faktorer för hur moderna cyberattacker genomförs, med AI:s förmåga att generera trovärdiga material och skripts som gör angreppen mer sofistikerade och svårupptäckta.

Paneldiskussionen behandlade hur organisationer kan skydda sig mot de hot som presenterats. Tomas Beeckman-Norrström från Nationellt cybersäkerhetscenter (NCC) betonade vikten av koordinering och stöd från myndigheter, och Petra Klein från Swedbank beskrev hur deras bank genomför samarbeten och arbetar med tredjepartsrisker och cybermodståndskraft. De lyfte fram behovet av konkreta åtgärder som att minska exponeringsytan, höja motståndskraften och ha kapacitet att hantera flera samtidiga attacker. Swedbank, SEB och Handelsbanken har etablerat samarbete för att stärka sina försvar, utbyta erfarenheter och bli bättre på att hantera ransomware.

Avslutningsvis diskuterades vikten av informationsdelning inom sektorn för att förbättra säkerheten generellt. Petra Klein påpekade att samarbete mellan olika aktörer är avgörande, medan Tomas Beeckman-Norrström framhöll att NCC har en roll här som Sveriges nav för cyberfrågor, inklusive incidenthantering och rådgivning. Det påpekades även att Sverige har en utmaning att balansera den snabba digitala utvecklingen med säkerhetsåtgärder, samt att det behövs en säkerhetskultur där alla nivåer av organisationer är engagerade. Rekommendationerna för organisationer inkluderade att fokusera på de mest relevanta hoten och att öva regelbundet för att vara förberedda vid en verklig attack.



Nyckelbudskap

Utnyttjande av sårbarheter ökar snabbt

Det har varit en dramatisk ökning i antalet avslöjanden och utnyttjanden av sårbarheter. Proof-of-concept tillgänglighet gör det enklare för hotaktörer att genomföra avancerade och mindre sofistikerade attacker. Organisationer måste fokusera på att identifiera och eliminera dessa sårbarheter för att minska risken för attacker.

Samarbete är avgörande för cyberförsvar

Paneldeltagarna betonade vikten av samarbeten inom sektorer för att stärka cyberförsvaret. Swedbank, SEB och Handelsbanken har etablerat ett samarbete för att dela kunskap och erfarenheter kring ransomware och andra cyberhot. Genom att arbeta tillsammans blir organisationerna bättre rustade att möta hoten.

Informationsdelning och övning är nyckeln till motståndskraft

Deltagarna underströk att informationsdelning inom sektorn är avgörande för att förbättra säkerheten. Regelbundna övningar och scenariobyggande skapar en beredskap för verkliga attacker och hjälper organisationer att reagera snabbt. En stark säkerhetskultur och proaktiva insatser är essentiella för ett effektivt cyberförsvar.

Powered by

voxoevent.ai