Uppdaterad 2023-11-15

Välkommen till:

NCSC Cybersäkerhetskonferens 5 december 2023

Tema Incidenthantering:
från förberedelse till hantering och lärdomar

Välkommen till NCSC-konferensen 2023

Årets upplaga fokuserar på incidenthantering utifrån ett helhetsperspektiv, med presentationer om allt från att förbereda sig, till att identifiera, hantera och dra lärdom. För att prata om detta har vi samlat några av branschens mest framstående experter.

Omvärldsläget har under senare tid försämrats kraftigt och cyberhot är en verklighet som vi måste förhålla oss till. Förmågan att stå emot och hantera cyberangrepp vilar på såväl övergripande strategiska vägval som på individers skicklighet och kunnande. Ambitionen med NCSC-konferensen 2023 är att samla flera perspektiv på incidenthantering i ett och samma program.

Konferensen är helt kostnadsfri och lunch ingår. Dessutom får ni gärna stanna på vårt mingel efter konferensen där det erbjuds lättare förtäring och alkoholfri dryck.

Utställare

I programpauserna finns gott om tid att stifta närmare bekantskap med konferensens talare och centrets ingående myndigheter.

På konferensen deltar följande utställare:

- Försvarets materielverk (FMV)
- Försvarets radioanstalt (FRA)
- Försvarsmakten
- Myndigheten för samhällsskydd och beredskap (MSB)
- Polismyndigheten
- Post- och telestyrelsen (PTS)
- Säkerhetspolisen

Tid och plats

- Clarion Hotel Sign i Stockholm
- 5 december
- Klockan 8.30-16.15

Konferensen är kostnadsfri

- NCSC står för lunch, fika och lättare förtäring i samband med det avslutande minglet.

Målgrupp

- De som arbetar med cybersäkerhet inom privat eller offentlig sektor och bidrar till svensk samhällssäkerhet, konkurrenskraft och välfärd.

Anmälan

- Anmälan är stängd och konferensen fullbokad.

Program - NCSC-konferensen 2023

08.30 Fika och registrering

09.00 Välkommen till NCSC-konferensen 2023
Talare: Therese Naess, Chef för Nationellt cybersäkerhetscenter

09.15 Ministern för civilt försvar har ordet
Ministern för civilt försvar, Carl-Oskar Bohlin, ger sin syn på aktuella utmaningar och viktiga framtidsfrågor inom cybersäkerhetsområdet.

Talare: Carl-Oskar Bohlin, minister för civilt försvar

09.30 Övning – från tanke till genomförande
Övning, övning, övning. Vi ska öva mer, större, och bättre. Kraven på organisationer från både den egna linjen och andra intressenter ökar, och man måste ständigt hålla sig ajour för att kunna hantera den snabba utvecklingen i omvärlden. Men hur bygger man egentligen en övning som bidrar till att organisationens förmåga ökar, och hur upprätthåller man sedan den förmågan? *Försvarsmakten och MSB/CERT-SE*, återger sina erfarenheter och tips för att bygga en övningsorganisation i en föränderlig omvärld.

Talare: Tobias Malm, Major, Försvarsmakten och
Rebecca Karlsson, övningskoordinator, MSB/CERT-SE

10.10 Kaffe

10.40 Från cybersäkerhet till business resiliens – hur samhällsviktiga funktioner kan stärka sin motståndskraft mot cyberattacker
Den ständigt växande attackytan gör oss mer utsatta och istället för att endast bygga fler, tjockare och högre murar behöver vi investera i en bredd av åtgärder. SEB, Handelsbanken och Swedbank berättar om hur man kan öka sin motståndskraft mot cyberhot genom att förstärka förmågor över hela säkerhets- och resiliens-området. Den tekniska utvecklingen erbjuder många effektiv lösningar men vi måste också fokusera på människan som är den viktigaste pusselbiten i ett starkt cyberförsvar.

Talare: Sam Graflund Wallentin, Swedbank; Christine Dovander, SEB;
Fredrik Malmström, Handelsbanken

11.20 Hästen, vattenhålet och elefanten i rummet
Nära nog alla informationssystem har idag externa kopplingar och beroenden som måste omhändertas ur ett säkerhetsskyddsperspektiv. Under de senaste åren har it-världen återkommande upplevt incidenter till följd av exempelvis cyberangrepp mot och genom leverantörer och leveranskedjorna som dessa är den del av. I detta pass kommer vi att titta på utmaningar kring leveranskedjor och risken för incidenter i dessa, samt hur man kan förhålla sig till detta i sitt säkerhetsarbete.

Talare: Säkerhetspolisen

12.00 Lunch

Program - NCSC-konferensen 2023

13.00 Cyber Pearl Harbor, digital bombs & binary bullets - myt vs. empirisk verklighet
Det finns många sätt att försöka översätta internets komplexitet till lättbegriplig information. Detta har inte minst gällt kommunikation om cyberkrigföring. Men hur väl stämmer dessa beskrivningar med den empiriska verkligheten? Och vad kan konsekvenserna bli av att vår situationsförståelse formas av metaforer? Detta är frågor som kommer att tas upp i denna föreläsning.

Talare: Dr. Sarah Backman, Försvarshögskolan

13.40 Angreppsytan du glömde – din infrastruktur är också sårbar
Det är inte bara dina klienter, servrar och mobiler som är måltavlor. Andra typer av enheter, såsom routrar, brandväggar och fjärråtkomstlösningar är under angrepp. Tyvärr hanteras sådana enheter inte sällan som om de vore ohackbara, vilket får till följd att de lämnas utan tillräckligt skydd. I denna presentation berättar Magnus Melkersson från FRA vad man bör tänka på och vilka åtgärder som bör vidtas.

Talare: Magnus Melkersson, FRA

14.20 Kaffe

14.50 När cyberattacken kom - insikter och lärdomar från ett allvarligt dataintrång
I slutet av november 2022 drabbades Norrköpings kommun av en allvarlig cyberattack som hotade kommunens hela IT-miljö. Två professionella hacker-grupperingar tog sig in, kommunen gick upp i stabsläge och vidtog drastiska åtgärder för att ta sig ur krisen. Niklas Ohrmér berättar hur kommunen lyckades avvärja hotet genom modiga beslut, agilt krisarbete, en kultur och ett ledarskap som höll i en kris-situation. Ta del av vad kommunen lärt sig och vilket åtgärdspaket som togs fram för att ytterligare förstärka skydd, reaktionsförmåga och resiliens.

Talare: Niklas Ohrmér, Norrköpings kommun

15.30 Cyber Defense Reinvented: Ukraine's Battle-Proven Framework for Resilient Cybersecurity
In a world beset by daily adversaries and ruthless cyberattacks, organizations often lack the resources and expertise to respond effectively. Join Yegor Aushev and Ole Dubnov, architects of Ukraine's Cyber Defence, as they unveils Ukraine's battle-tested incident response framework which aims to rapidly enhance cyber resilience for all organizations, regardless of their resources. Discover the power of true cyber resilience through effective interoperability, engaging the entire organization in the incident response process.

Talare: Yegor Aushev (remotely from Kyiv) and Ole Dubnov, Cyber Unit Technologies

16.10 Summering av dagen
Therese Neass, Chef för NCSC

16.15 Mingel
Alkoholfritt bubbel och snittar