Cyber Threats

20. maj - CFL - Center for Ledelse, København

08:30 - 09:00	**Registrering, netværk og morgenmad**
09:00 - 09:05	**Velkomst** Frederik Therkildsen, Cyberredaktør og moderator, Computerworld
09:05 - 09:35	**Når geopolitik bliver en sikkerhedsrisiko: Kan vi stole på vores software i kritisk infrastruktur?** Chamara Bulathsinhala, ekspert i kritisk infrastruktur med speciale i supply chain
09:35 - 10:00	***Ægte* cyber-resiliens kræver mere end teknologi** Søren Pedersen, CTO, Orange Cyberdefense Denmark
10:00 - 10:25	**Pause & netværk**
10:25 - 10:50	**Hvad er de 10 vigtigste Cybertiltag, og hvordan får du ledelsen til at sponsorere dem?** Christian Schmidt, Direktør, Dediko
10:50 - 11:15	**Commvault - Taler kommer snart**
11:15 - 11:30	**Erfaringsudveksling og diskussion v. borde**
11:30 - 12:25	**Frokost & netværk**
12:25 - 12:55	**Operation Endgame: Hvordan politiet går efter infrastrukturen bag global cybercrime** Mathias Andersen, Fungerende politikommissær, National enhed for Særlig Kriminalitet
12:55 - 13:20	**Cohesity - Taler kommer snart**
13:20 - 13:35	**Erfaringsudveksling og diskussion ved borde**
13:35 - 13:55	**Pause & netværk**
13:55 - 14:20	**Taler kommer snart**
14:20 - 14:50	**Moderne dusørjægere: Hvordan venlige hackere hjælper med at styrke virksomheders IT-sikkerhed** Emil Hørning, Head of Hackers, Defend Denmark
14:50 - 14:50	**Opsummering og tak for idag**

08:30 - 09:00: Registrering, netværk og morgenmad

Kom og nyd en lækker bolle med ost og en croissant. Få en kop frisk brygget kaffe/the og hils på de andre deltagere.

09:00 - 09:05: Velkomst

Frederik Therkildsen
Cyberredaktør og moderator
Computerworld

09:05 - 09:35: Når geopolitik bliver en sikkerhedsrisiko: Kan vi stole på vores software i kritisk infrastruktur?

Chamara Bulathsinhala
ekspert i kritisk infrastruktur med speciale i supply chain / Keynote

Digitalisering, data og specialiseret software er centrale for driften af kritisk infrastruktur i Danmark. Geopolitiske spændinger er ikke længere et abstrakt vilkår, men en konkret cybersikkerhedsrisiko forankret i kildekode, tredjepartskomponenter og globale softwareleverandørkæder.

Chamara tager med dette indlæg afsæt i Agisoft-sagen, som har synliggjort brugen af russiskudviklede softwarekomponenter i løsninger til opmåling, fotogrammetri og GIS for dansk kritisk infrastruktur. Chamara viser, hvordan manglende transparens om oprindelse, afhængigheder og risikoprofil udfordrer forsyninger og myndigheder, også når databehandling sker i Danmark eller EU.

09:35 - 10:00: Ægte cyber-resiliens kræver mere end teknologi

Søren Pedersen
CTO
Orange Cyberdefense Denmark / Partner

Søren sætter i denne præsentation fokus på, hvad der i praksis skal til for at skabe ægte cyber-resiliens i en tid med komplekse trusler, udvidede angrebsflader og mangel på specialister. Cyberangreb lykkes sjældent på grund af én enkelt sårbarhed. De lykkes, når forskellige systemer ikke taler sammen, når sikkerhedsteams drukner i støj og når organisationer forsøger at løse et økosystemproblem i siloer med isolerede og reaktive og værktøjer.

Cybersikkerhed og et stærkt moderne cyberforsvar kræver mere end teknologi. Det kræver, at både systemer og mennesker arbejder sammen ogforstår at udnytte mulighederne i AI.

Søren dykker ned i:

· Hvordan et moderne cyberforsvar hænger sammen på tværs af teknologi, mennesker og processer
· Hvorfor de forskellige cybersikkerhedsroller og kompetencebehov er ved at ændre sig
· Hvorfor integration og samarbejde er centrale byggesten, når vi taler om cyber-resiliens
· Hvordan AI kan medvirke til at reducere støj og styrke beslutningsgrundlaget i sikkerhedsdriften

10:00 - 10:25: Pause & netværk

Nyd et stykke frugt og en kop kaffe og netværk med ligesindede.

10:25 - 10:50: Hvad er de 10 vigtigste Cybertiltag, og hvordan får du ledelsen til at sponsorere dem?

Christian Schmidt
Direktør
Dediko / Partner

Cybertruslen er strukturel og forretningskritisk – og under NIS2 er ansvaret entydigt placeret hos ledelsen. De fleste organisationer mangler
kontinuerlig prioritering, risikoforankring og ledelsens sponsorship.

Oplægget identificerer centrale Cybertiltag med dokumenteret risikoreducerende effekt. Fællesnævneren er, at disse tiltag reducerer sandsynligheden for kompromittering samt konsekvensen ved et brud. Men hvad er de egentlig? (tip: CIS18 IG2)

En central pointe er, at compliance alene ikke skaber sikkerhed. Sponsorering opnås ved at oversætte tekniske sårbarheder til forretningsrisici: driftstab, omsætningspåvirkning, regulatoriske sanktioner og personligt ledelsesansvar.

Ledelser investerer ikke i kontroller – de investerer i risikoreduktion og kontinuitet. Effektiv kommunikation kræver scenariebaserede analyser, kvantificering af risiko og klare beslutningsoplæg med konsekvensvurderinger. Fokuser på de 10 mest effektive tiltag, mål risikoreduktion frem for aktivitet – og gør Cyber til et strategisk ledelsesanliggende, ikke et IT-projekt.

På 25 minutter får du et indspark til hvordan du skal gribe dette an i praksis.

10:50 - 11:15: Commvault - Taler kommer snart

11:15 - 11:30: Erfaringsudveksling og diskussion v. borde

11:30 - 12:25: Frokost & netværk

Nyd en lækker frokostbuffet og sodavand, som serveres sidende i festsalen. Sæt dig gerne sammen med nogen du ikke kender.

12:25 - 12:55: Operation Endgame: Hvordan politiet går efter infrastrukturen bag global cybercrime

Mathias Andersen
Fungerende politikommissær
National enhed for Særlig Kriminalitet / Keynote

National enhed for Særlig Kriminalitet arbejder hver dag for at gøre livet sværere for cyberkriminelle – blandt andet ved at nedtage central infrastruktur. NSK har deltaget i Operation Endgame i flere år og har deltaget i flere nedtagninger. Nicklas Fallesen og Mathias Andersen giver et indblik i, hvordan der ser ud operationsrummet, når interventioner mod servere, domæner og paneler planlægges, udføres og resultaterne analyseres.

12:55 - 13:20: Cohesity - Taler kommer snart

13:20 - 13:35: Erfaringsudveksling og diskussion ved borde

13:35 - 13:55: Pause & netværk

Få en kop kaffe, et stykke kage og få connectet med dem du har netværket med gennem dagen.

13:55 - 14:20: Taler kommer snart

14:20 - 14:50: Moderne dusørjægere: Hvordan venlige hackere hjælper med at styrke virksomheders IT-sikkerhed

Emil Hørning
Head of Hackers
Defend Denmark / Keynote

Hver dag hjælper venlige etiske hackere tusindvis af virksomheder med at finde kritiske sårbarheder I bytte for dusører. Dette økosystem hedder "Bug Bounty" og omfatter, at hackere kan blive belønnet for at afdække, hvordan de har kunnet hacke en virksomhed.

Dette indlæg vil give indsigt I bug bounty økosystemet I 2026, vise hvordan en etisk hacker bruger sine værktøjer og give konkrete råd til hvordan IT-afdelingen kan arbejde mere omkostningsbevidst med "The power of the crowd".

14:50 - 14:50: Opsummering og tak for idag