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 cybertrusler bliver forretningstruende – sådan skal du reagere** Henrik Christiansen, Crisis Negotiator, Delta Crisis Management
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, Compliance specialist, Dediko
10:50 - 11:15	**Fra reaktiv cybersikkerhed til cyberresiliens** Karsten Dreyer Lund, Solution Engineer, Commvault
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	**Når cyberangreb rammer: Hvor hurtigt – og sikkert – kan din organisation komme sig?** Henrik Thorsøe Pedersen, Enterprise Account Manager, Cohesity
13:20 - 13:40	**Pause & netværk**
13:40 - 14:10	**AI i praksis: Hvilke cyberopgaver blev lettere – og hvilke blev ikke?** Olivia Wenya Chen, Challenge Author, Cyberlandsholdet og Campfire Security
14:10 - 14:40	**Moderne dusørjægere: Hvordan venlige hackere hjælper med at styrke virksomheders IT-sikkerhed** Emil Hørning, Head of Hackers, Defend Denmark
14:40 - 14:45	**Opsummering v. dagens moderator**
14:45 - 14:45	**Tak for i dag**

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 cybertrusler bliver forretningstruende – sådan skal du reagere



Henrik Christiansen
Crisis Negotiator
Delta Crisis Management / Keynote

Når cybertrusler går fra IT-udfordring til forretningskritisk risiko, kræver det hurtig og målrettet handling. I dette indlæg deler Henrik Christiansen erfaringer med, hvordan organisationer bør reagere, når angreb rammer drift, data og omdømme.

Med konkrete eksempler og best practice får deltagerne indsigt i effektiv krisehåndtering, beslutningstagning under pres og samspillet mellem IT, ledelse og forretning. Fokus er på at styrke beredskabet og sikre en hurtig, forretningsmæssig genopretning.

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
Compliance specialist
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: Fra reaktiv cybersikkerhed til cyberresiliens



Karsten Dreyer Lund
Solution Engineer
Commvault / Partner

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. 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: Når cyberangreb rammer: Hvor hurtigt – og sikkert – kan din organisation komme sig?



Henrik Thorsøe Pedersen
Enterprise Account Manager
Cohesity / Partner

Cyberangreb er ikke længere et spørgsmål om hvis, men hvornår. For ledelsen betyder det, at parathed ikke kun handler om forebyggelse, men om evnen til at komme sig sikkert, når en hændelse indtræffer.

I dette indlæg udforsker vi, hvorfor traditionelle gendannelsesmetoder ofte fejler under ransomware-angreb, og hvad der skal til for at opnå en ren gendannelse uden at genindføre kompromitterede data. Med konkrete eksempler deler Cohesity indsigter i, hvordan organisationer kan styrke deres cyberresiliens, minimere nedetid og genvinde kontrollen over forretningen – selv i de mest kritiske situationer.

13:20 - 13:40: Pause & netværk

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

13:40 - 14:10: AI i praksis: Hvilke cyberopgaver blev lettere – og hvilke blev ikke?



Olivia Wenya Chen
Challenge Author
Cyberlandsholdet og Campfire Security / Keynote

Hvad sker der når Cyberlandsholdet giver deltagere adgang til AI-værktøjer i konkurrencens sidste tre timer? Olivia Wenya Chen præsenterer anonymiseret data fra deltagere på tværs af junior- og seniorkategorien og viser, hvordan AI påvirkede løsningen af konkrete cyberopgaver.

Oplægget giver indblik i, hvilke opgavetyper AI kunne løfte, hvor teknologien ikke gjorde en forskel, og hvad resultaterne siger om cybersikkerhedskompetencer i Danmark. Samtidig sætter Olivia fokus på den rolle, AI kommer til at spille i fremtidens cyberforsvar.

14:10 - 14:40: 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".

14:40 - 14:45: Opsummering v. dagens moderator

14:45 - 14:45: Tak for i dag