Cyber Security 2025

TORSDAG D. 20. NOVEMBER 2025
AI INNOVATION HOUSE, VEJLE

dansk•it

08.30 - 09.00 **Ankomst, registrering, og morgenmad**

09.00 - 09.10 **Velkomst**
* *Torben Jørgensen Owner, InfoSec Partner Aps*
* *TBA*

09.10 – 09.50 **Trusselsbilledet i det geopolitiske lys**
* *Peter Kruse, CISO, Clever*

I en verden præget af globale spændinger, hybridkrigsførelse og statssponsorerede cyberangreb bliver cybersikkerhed i stigende grad en integreret del af det geopolitiske spil. Peter stiller derfor skarpt på, hvordan internationale konflikter, teknologisk rivalisering og politiske magtkampe er med til at forme og intensivere trusselsbilledet for it-sikkerhed.

Ondsindede stater anvender i stigen grad cyberspace som en strategisk arena til at fremme deres interesser – ofte gennem sofistikerede og målrettede angreb rettet mod både kritisk infrastruktur, myndigheder og private virksomheder. Samtidig ser vi nærmere på de metoder, værktøjer og taktikker, der kendetegner nutidens trusselsaktører, samt hvordan cybersikkerhed i stigende grad kobles til både national sikkerhed og udenrigspolitik.

Du får en analytisk indsigt i de geopolitiske drivkræfter bag nutidens cybertrusler og samtidig indsigt nødvendigheden af både tekniske, strategiske og diplomatiske tilgange til forsvar og risikohåndtering i en kompleks og foranderlig verdensorden.

09.50 – 10.30 **Status på NIS2, CER og den kommende EU lavine af forordninger**
* *Mikkel Friis Rossa, partner, Bech Bruun*
* *Kasper Bilde Nielsen, senioradvokat, Bech Bruun*

EU skruer markant op for de regulatoriske krav til cybersikkerhed og risikostyring – og det har vidtrækkende konsekvenser for både offentlige og private organisationer. I dette oplæg giver vi en opdateret status på NIS2 og CER-direktivet samt et overblik over de mange forordninger, der er på vej fra Bruxelles.

Vi ser nærmere på, hvad der allerede gælder, hvad der er på trapperne, og hvordan organisationer bør forberede sig strategisk og praktisk. Fokus er ikke kun på overholdelse, men på hvordan compliance kan bruges som løftestang til styrket robusthed og forretningsværdi i en tid, hvor cybersikkerhed ikke længere kun er et teknisk anliggende – men et forretningskritisk ledelsesansvar.

10.30 – 10.50 **Pause og netværk**

10.50 – 11.30 **Plan B for cybersikkerhed: Beskyt din organisation uden afhængighed af amerikanske techgiganter**
* *Thomas Kristmar, områdechef, Statens IT*

I takt med at digital suverænitet og open source fylder stadig mere i debatten, bliver det afgørende også at tænke cybersikkerhed ind som en central del af ligningen. For hvad kræver det egentlig, hvis danske organisationer vil opretholde et højt sikkerhedsniveau uden at være afhængige af amerikanske cloud- og softwareleverandører?
Der stilles skarpt på, hvordan man bygger en robust og realistisk plan B. Vi undersøger, hvilke krav man bør stille til alternative løsninger – særligt de europæiske og open source-baserede – og hvordan deres sikkerhedsniveau kan måle sig med de standarder, som amerikanske aktører har udviklet gennem årtiers investeringer i cybersikkerhed.
Du får et nuanceret og praksisnært blik på, hvad et skifte væk fra de amerikanske platforme indebærer – både risici og muligheder – og hvordan organisationer kan bevæge sig sikkert mod større digital uafhængighed uden at gå på kompromis med deres it-sikkerhed

Cyber Security 2025

TORSDAG D. 20. NOVEMBER 2025
AI INNOVATION HOUSE, VEJLE

dansk•it

11.30 – 12.10

Cybersikkerhed i SMV'er – styrket gennem offentlig-privat samarbejde

* Peer H. Kristensen, Direktør, Security Tech Space

Små og mellemstore virksomheder er særligt udsatte for cyberangreb, hvilket kan få alvorlige konsekvenser. Indlægget præsenterer et nyt initiativ, hvor offentlige og private aktører samarbejder om at styrke cybersikkerheden i SMV'er gennem fælles løsninger, teknologi og best practices. Målet er at skabe en praktisk og bæredygtig model, der styrker robustheden i dansk erhvervsliv.

12.10 – 13.00

Frokost og netværk

13.00 – 13.40

AIs betydning for cybersikkerheden nu og i fremtiden

* Simon Simonsen, Lead Security Specialist, Systematic

Kunstig intelligens er godt på vej til at ændre spillets regler i cybersikkerhed – både på forsvars- og angrebssiden.Derfor ser vi nærmere på, hvordan AI allerede i dag bruges til at opdage trusler hurtigere, automatisere reaktioner og analysere enorme mængder sikkerhedsdata med en præcision, mennesker ikke kan matche.

Men udviklingen har også en skyggeside: AI er i stigende grad et værktøj for trusselsaktører, som bruger teknologien til at udvikle mere avancerede og målrettede angreb. Og fremtiden byder på både større potentiale og større risici.

Hvordan skal organisationer forholde sig til AI i deres sikkerhedsstrategi? Hvad kan teknologien allerede nu – og hvad skal vi forberede os på? Oplægget giver et overblik over den aktuelle status, fremtidsperspektiver og centrale overvejelser for både beslutningstagere og sikkerhedsfaglige.

13.40 – 14.20

Er amerikansk cloud dømt ude?

* Lone Juric Sørensen, Chef for Fælles IT & Digitalisering, Aarhus Kommune

Med øget fokus på datalovgivning, Schrems II og krav til digital suverænitet har flere danske offentlige aktører taget kritiske cloudvalg.

Århus Kommune er blandt dem og har flyttet dele af deres data fra amerikanske Azure til tyske Hetzner. I dette oplæg ser vi nærmere på bevæggrunden, erfaringerne – og det større spørgsmål: Er amerikansk cloud stadig en realistisk løsning i det offentlige Danmark?

14.20 – 14.40

Pause og netværk

14.40 – 15.20

Klar til kaos? I Sorø har de stresstestet deres IT-redskab

* Emil Nygaard, Leder af IT-Drift, Sorø Kommune

Hvordan reagerer man, når det virkelig gælder? I Sorø Kommune har man valgt at finde ud af det, før en reel krise opstår. Gennem en omfattende stresstest af deres IT-beredskab har kommunen sat fokus på, hvordan man bedst forbereder sig på det uforudsigelige – og hvad man lærer, når teorien møder praksis.

Emil Nygaard, leder af IT-drift i Sorø deler erfaringerne med at øve sig på det værste. For trusselsbilledet er ikke længere noget, man kan se bort fra: Center for Cybersikkerhed vurderer truslen fra cyberkriminalitet som meget høj, og selvom kommunerne hidtil er sluppet relativt billigt, kan held ikke være en strategi.

Hvordan ruster man en kommune – teknisk, organisatorisk og mentalt – til at håndtere alt fra ransomware til nedbrud og destruktive angreb? Og hvad gør man, når det uforudsete alligevel indtræffer?

Cyber Security 2025

TORSDAG D. 20. NOVEMBER 2025
AI INNOVATION HOUSE, VEJLE

dansk•it

15.20 – 16.00

Vejen til en moderne sikkerhedskultur

* Roel Schouten, Vice President Information Security, Trivium Packaging

Når en organisation rammes af et cyberangreb, er det naturligt at reagere med forsigtighed, kontrol og begrænsninger. Men krisemode kan ikke være en varig tilstand. På et tidspunkt skal man ikke bare tilbage til normal drift – sikkerhedsteamet skal igen tage en proaktiv rolle og støtte forretningen fremadrettet.

I dette oplæg tager jeg udgangspunkt i en konkret cyberkrise i 2021, hvor den umiddelbare reaktion var at sige nej til alt. Det gav kortvarig tryghed, men hæmmede samarbejde og fremdrift. Erfaringen viser, hvor vigtigt det er at balancere beskyttelse med fremdrift – og at sikkerhed skal ses som en partner, ikke en bremseklods.

Derfor sætter jeg fokus på, hvordan vi som sikkerhedsprofessionelle kan bidrage til at forme en moderne sikkerhedskultur, hvor medarbejdere opfattes som en del af løsningen – ikke som risici. Alt for ofte præges feltet af en "os og dem"-mentalitet, som skaber afstand og modstand, og i sidste ende undergraver vores fælles mål: en stærk, tryg og modstandsdygtig organisation.

Hvordan skaber vi en kultur, hvor samarbejde, respekt og fælles ansvar bliver fundamentet for god sikkerhed? Det er det spørgsmål, jeg vil dykke ned i.

16.00 – 16.05

Opsummering og farvel og tak