Cyber Security

I dag handler cybersikkerhed ikke kun om at forhindre angreb.
Det handler om at kunne stå oprejst, når angrebet rammer.

PROGRAM: TORSDAG DEN 1. OKTOBER 2026

CLASSIC CAR HOUSE, KØBENHAVN

LOKALE: AMAILE

8.30 - 9.00 **Registrering og let morgenmad**

9.00 - 9.10 **Velkomst**
** Torben Jørgensen, owner, InfoSec Partner Aps og forperson for Dansk IT's fagråd for Informationssikkerhed*
** Kim Stensdal, chef for kommunikation og viden, Dansk IT*

9.10 - 9.50 **Hybridkrigen er her: Hvordan navigerer du din organisation sikkert videre?**
* *Jacob Kaarsbo, uafhængig sikkerhedspolitisk rådgiver og tidligere chefanalytiker, Forsvarets Efterretningstjeneste*

Cybertruslen er ikke længere kun teknisk. Når organiserede kriminelle, statslige aktører, sabotage og påvirkningsoperationer smelter sammen, bliver cybersikkerhed et strategisk ledelsesansvar.

Jacob Kaarsbo giver et skarpt perspektiv på hybridkrigen, all-domain warfare og det nye trusselsbillede, danske organisationer skal navigere i.

Oplægget viser, hvorfor der er brug for rådgivning, der ikke bare rapporterer hændelser, men fortolker udviklingen og oversætter risiko til beslutninger i direktion og bestyrelse.

9.50 - 10.20 **NATO: Cyber Deterrence – Defending in a World of Hybrid Threats**
** Colonel Mietta Groeneveld, MSc Director, NATO Command and Control Centre of Excellence, NATO*

Cyber attacks now move at algorithmic speed. A drone swarm cannot be stopped one drone at a time, and neither can an AI enabled intrusion. Colonel Mietta Groeneveld, Director of the NATO Command and Control Centre of Excellence, brings a military perspective on resilience, layered defense, and the command decisions organizations must agree before the next incident, not during it.

Drawing on NATO exercises such as Locked Shields, she will discuss how to move from a conventional, symmetric mindset to one built for the speed of modern threats, across the cyber, physical, and cognitive domains at once.

10.20 - 10.50 **Kaffepause**

dansk·it

Cyber Security

	LOKALE: AMAILE	LOKALE: V16
10.50 - 11.30	**Erfaringer fra virkelige cyberangreb** ** Jan Kaastrup, Chief Innovation officer & partner, CSIS Security Group* Cyberangreb rammer ikke kun "de andre". Som digital efterforsker hos CSIS er Jan Kaastrup den, danske virksomheder og organisationer ringer til, når skærmene går i sort og krav om løsepenge lander i indbakken. Med mere end 200 efterforskede angreb bag sig tager han dig med bag facaden på konkrete hackersager – hvordan de udfoldede sig, hvilke beslutninger der blev afgørende i de kritiske timer, og hvordan driften blev sikret igen. Du får et skarpt billede af det aktuelle trusselsbillede, de fejl mange gør i forbindelse med et angreb, og hvorfor et cyberangreb sjældent bare er et IT-problem, men en ledelseskrise. Vigtigst af alt: konkrete lessons learned, du kan bruge i din egen organisation – før det er dig, der får mailen eller opkaldet om et hackerangreb.	**Livehacking med cyberlandsholdet: Se din organisation med angriberens øjne** ** Jens Myrup Pedersen, professor i cybersikkerhed, Aarhus Universitet og landstræner for det danske Cyberlandshold* ** Sebastian Bach, repræsentant, Cyberlandsholdet* Hvordan tænker en hacker, og hvad kan din organisation lære af de unge cybertalenter der træner cybersikkerhed på eliteniveau? Jens giver sammen med en repræsentant fra Cyberlandsholdet et konkret indblik i, hvordan Capture The Flag-formatet kan bruges til at træne både offensive og defensive cyberkompetencer. Oplægget viser, hvordan erfaringer fra Cyberlandsholdet og de danske cybermesterskaber kan omsættes til kompetenceudvikling, beredskab og hurtig opkvalificering, når nye sårbarheder opstår, og tiden er knap.
11.30 - 11.45	**Transit**	
11.45 - 12.25	**Nu rammer NIS2 driften: Hvad skal du konkret gøre?** ** Emil Bisgaard, partner og juridisk ekspert i cyberregulering, Poul Schmidt/Kammeradvokaten* Cybersikkerhed er rykket helt ind på den politiske dagsorden, og med NIS2 er kravene blevet mere konkrete for både virksomheder, myndigheder og kommuner. I dette oplæg giver Emil Bisgaard en praksisnær status på NIS2 efter det første år i Danmark. Hvad har været de største udfordringer? Hvordan går implementeringen i resten af Europa? Og hvad kan EU-Kommissionens omnibusforslag komme til at betyde? Oplægget ser også frem mod den næste bølge af cyberregulering, blandt andet Critical Entities Resilience, Cyber Resilience Act, en opdateret Cybersecurity Act. Du får et klart overblik over, hvad der er vigtigst lige nu, hvad der er på vej, og konkrete anbefalinger ift. hvordan cyberansvarlige kan navigere i reguleringen uden at drukne i jura.	**Tutorial: De 7 enkle greb, der styrker cybersikkerheden markant** ** Leif Jensen, sikkerhedsekspert, ESET og medlem af Dansk IT's fagråd for Informationssikkerhed* God cybersikkerhed behøver ikke altid begynde med store investeringer, avancerede løsninger eller hundedyre konsulentforløb. I denne tutorial får du en konkret gennemgang af 7 vigtige skridt, der kan styrke sikkerheden markant i din organisation. Leif Jensen viser, hvilke tiltag der ofte bliver overset i hverdagen, men som kan gøre en reel forskel for både drift, beredskab og modstandsdygtighed. Du får et praktisk overblik over, hvor du kan starte, hvad du bør prioritere, og hvordan du med relativt enkle greb kan løfte sikkerhedsniveauet i den organisation.
12.25 - 13.25	**Frokost**	

Cyber Security

13.25 – 14.05

Building Resilient Digital Infrastructure: Perspectives from X-Road for Denmark
** Ville Sirviö, Chief Executive Officer, Nordic Institute for Interoperability Solutions (NIIS), Estonia*

As societies become increasingly reliant on digital services, resilience has become a fundamental requirement for digital public infrastructure. This presentation explores how X-Road's distributed architecture strengthens resilience by eliminating single points of failure, enabling secure, trusted data exchange, and supporting operational continuity even during disruptions.

Drawing on real-world deployments across multiple countries, it demonstrates how interoperability, modularity, decentralisation, and security-by-design contribute to more resilient digital governments and societies.

De første 24 timer: Hvad gør du, når cyberangrebet rammer?
** Frederik Helweg-Larsen, partner, Rethink Cybersecurity Advisory*

Når et cyberangreb rammer, er det for sent at begynde at diskutere roller, ansvar og beslutningsveje. Så handler det om at kunne handle hurtigt, klogt og koordineret – på tværs af teknik, ledelse, jura, kommunikation og forretning. Men hvordan sikrer man, at beredskabsplanen faktisk virker i virkeligheden – og ikke bare ligger og støver i en mappe?

I denne session får deltagerne rig mulighed for at stille spørgsmål, dele konkrete erfaringer og diskutere, hvordan man som sikkerhedsansvarlig kan styre processen, når krisen rammer. Vi ser på typiske faldgruber, vigtige afklaringer og lavpraktiske greb, der kan gøre organisationen bedre rustet til at stå oprejst, når cyberangrebet rammer.

14.05 - 14.35 Kaffepause

14.35 - 15.05

Det menneskelige aspekt af Cyber Security: Hvorfor selv kloge mennesker åbner døren for hackere
** Sarah Aalborg, specialist i informationssikkerhed og Human Risk, Secure by Choice*

De fleste cyberangreb lykkes ikke, fordi teknologien fejler. De lykkes, fordi de udnytter helt almindelige menneskelige mekanismer som tillid, nysgerrighed, tidspres og ønsket om at hjælpe andre.

I dette oplæg ser Sarah Aalborg nærmere på, hvorfor selv intelligente og erfarne mennesker træffer usikre beslutninger, og hvordan viden om psykologi og adfærd kan bruges til at designe sikkerhed, der fungerer i virkeligheden.

Deltagerne får et nyt perspektiv på human risk og inspiration til at tænke mennesket ind som en aktiv del af sikkerhedsarkitekturen frem for blot at betragte det som det svageste led.

15.05 - 15.50

AI mod AI: Hvem vinder cyber-oprustningskapløbet?
** Peter Kruse, Security Researcher and Malware Analyst, Kruse Industries ApS*

AI er i fuld gang med at ændre cybersikkerhed. Kriminelle aktører bruger teknologien til phishing, deepfakes, automatisering og hurtigere jagt på sårbarheder. Samtidig bliver AI et stadig vigtigere værktøj for forsvarerne, blandt andet til detektion, analyse, prioritering, hændelseshåndtering og patching.

Men hvem får mest ud af teknologien først, angriberne eller forsvarerne?
Hvem vinder cyber-oprustningskapløbet?

I dette oplæg giver Peter Kruse, en af Danmarks mest erfarne profiler inden for cybersikkerhed og cybertrusler, et praksisnært og nøgternt blik på, hvordan AI allerede bruges i cyberkriminalitet, hvor teknologien kan styrke organisationens forsvar, og hvad CISO'er, sikkerhedsansvarlige og ledere bør forberede sig på nu.

15.50 - 16.00

Opsamling og tak for denne gang
** Kim Stensdal, chef for kommunikation og viden, Dansk IT*