TechFront: Sikkerhed i det offentlige

3. december - Kosmopol, København

08:30 - 09:00	**Registrering og morgenmad**
09:00 - 09:05	**Velkomst** Lars Jacobsen, Chefredaktør og moderator, Computerworld
09:05 - 09:35	**Når velfærden er målet: Sådan bygges et fælles cyberforsvar for kommunerne** Kristian Vengsgaard, CEO, KOMBIT
09:35 - 10:00	**Fra panik til parathed: Kunsten at være et skridt foran hackerne** Koen Maris, Head of Cybersecurity advisory, Atos
10:00 - 10:15	**Diskussion og erfaringsudveksling**
10:15 - 10:40	**Pause**
10:40 - 11:10	**Robusthed og redundans - en forudsætning for effektiv it-drift** Aino Olsen, Direktør, Cyberdivisionen, FMI
11:10 - 11:35	**Robust cybersikkerhed – har vi den, eller tror vi bare, vi har den?** Christian Schmidt, Compliance specialist, Dediko
11:35 - 11:50	**Diskussion og erfaringsudveksling**
11:50 - 12:40	**Frokost**
12:40 - 13:05	**Cybersikkerhed starter med data: Find dem. Forstå dem. Beskyt dem.** Kaare Mortensen, Pre-Sales Consultant, Thales
13:10 - 13:35	**Taler kommer snart**
13:35 - 14:05	**Ét samlet værn: Indenfor Aarhus Havns nye Security Center** Laura Thomsen, Cyber Security Specialist, Aarhus Havn
14:05 - 14:10	**Opsummering v. dagens moderator** Lars Jacobsen, Chefredaktør og moderator, Computerworld
14:10 - 14:30	**Kaffe, kage og netværk**
14:30 - 14:30	**Tak for i dag**

08:30 - 09:00: Registrering og morgenmad

09:00 - 09:05: Velkomst



Lars Jacobsen
Chefredaktør og moderator
Computerworld

09:05 - 09:35: Når velfærden er målet: Sådan bygges et fælles cyberforsvar for kommunerne



Kristian Vengsgaard
CEO
KOMBIT / Keynote

Kommunernes digitale infrastruktur understøtter nogle af samfundets mest centrale velfærdsydelser. Et alvorligt cyberangreb kan derfor hurtigt få konkrete konsekvenser for både borgere og kommunal drift.

Samtidig er ansvar, kompetencer og ressourcer fordelt mellem 98 kommuner, fælleskommunale løsninger, myndigheder og leverandører. Kristian Vengsgaard sætter fokus på de største fælles sårbarheder og afhængigheder – og giver sit bud på, hvordan et sammenhængende cyberskjold omkring den kommunale sektor skal bygges.

09:35 - 10:00: Fra panik til parathed: Kunsten at være et skridt foran hackerne



Koen Maris
Head of Cybersecurity advisory
Atos / Partner

AI-trusler og zero-days kræver mere end hurtig reaktion. Koen Maris fra Atos viser, hvordan Prepare – Respond – Adapt (PRA) gør cyberforsvaret mere proaktivt og tilpasningsdygtigt.

Med medarbejdere som aktive medspillere og agentisk AI til hurtige undersøgelser kan I opdage trusler tidligere, lære af hændelser og dokumentere værdien af forebyggelse over for bestyrelsen.

Dette oplæg afholdes på engelsk

10:00 - 10:15: Diskussion og erfaringsudveksling

10:15 - 10:40: Pause

10:40 - 11:10: Robusthed og redundans - en forudsætning for effektiv it-drift



Aino Olsen
Direktør
Cyberdivisionen, FMI / Keynote

Cyberangreb udgør en konkret trussel mod samfundskritiske institutioner, og Forsvarets it-organisation er også omfattet af det skærpede sikkerhedsniveau. Robust it-drift kræver øget agtpågivenhed, træning i systemgenopretning og evnen til at opretholde driften og handle effektivt under nedbrud.

Digital robusthed kræver investeringer i redundans, ligesom fysiske lagre kræver ressourcer. Oplægget giver indsigt i, hvordan Forsvarets it-organisation kan styrke sin robusthed over for cyberangreb, sikre driften under nedbrud og prioritere investeringer i digital redundans. Investeringerne koster, men er en forudsætning for sikker og effektiv it-drift i en skærpet sikkerhedssituation.

11:10 - 11:35: Robust cybersikkerhed – har vi den, eller tror vi bare, vi har den?



Christian Schmidt
Compliance specialist
Dediko / Partner

Mange organisationer investerer betydeligt i cybersikkerhed, implementerer kontroller og arbejder med NIS2, ISO 27001 og CIS 18. Men hvordan ved vi egentlig, om sikkerheden virker – og om organisationen kan modstå, håndtere og komme sig efter et alvorligt cyberangreb?

I dette indlæg udfordrer vi forskellen mellem at ***have cybersikkerhed på papiret og at være robust i praksis****.*

Vi ser på, hvad der reelt skaber cyberrobusthed, hvorfor compliance og teknologiske investeringer ikke er tilstrækkelige, og hvordan ledelsen kan måle sikkerhedens effekt frem for blot at måle aktiviteter.

Med konkrete eksempler og praktiske målepunkter viser vi, hvordan organisationer kan omsætte sikkerhedskrav til dokumenteret evne til at beskytte og opretholde deres kritiske funktioner – også når angrebet lykkes.

11:35 - 11:50: Diskussion og erfaringsudveksling

11:50 - 12:40: Frokost

12:40 - 13:05: Cybersikkerhed starter med data: Find dem. Forstå dem. Beskyt dem.



Kaare Mortensen
Pre-Sales Consultant
Thales / Partner

Sikkerhedsansvarlige står til ansvar ved sikkerhedsbrud, men mangler ofte overblik over, hvor organisationens kritiske data befinder sig, og hvem der har adgang til dem.

Samtidig skaber fragmenterede værktøjer, manuelle processer og stigende compliancekrav stadig større kompleksitet.

Udfordringen er ikke manglen på alarmer, men evnen til hurtigt at forstå, prioritere og håndtere de reelle risici.

Indlægget viser, hvordan en Data Security Posture Management (DSPM)-tilgang kan skabe overblik, kontrol og konkret beskyttelse af de data, organisationen ikke kan undvære.

13:10 - 13:35: Taler kommer snart

13:35 - 14:05: Ét samlet værn: Indenfor Aarhus Havns nye Security Center



Laura Thomsen
Cyber Security Specialist
Aarhus Havn / Keynote

Et cyberangreb på en havn kan hurtigt få fysiske konsekvenser og forstyrre både varestrømme og forsyningskæder. Aarhus Havn har derfor samlet den fysiske og digitale sikkerhed i én organisation. Laura Thomsen fortæller, hvordan havnen skaber et fælles risikobillede, forbereder organisationen på alvorlige hændelser og prioriterer de funktioner, der skal holdes i gang – også når systemer eller infrastruktur bliver ramt.

14:05 - 14:10: Opsummering v. dagens moderator



Lars Jacobsen
Chefredaktør og moderator
Computerworld

14:10 - 14:30: Kaffe, kage og netværk

14:30 - 14:30: Tak for i dag