

# Digital sikkerhed 2019: Trusler, tendenser og strategi

31. januar - Comwell Hotel Aarhus, Aarhus

---

- 08:30 - 08:55 **Morgenmad & Registering**
- 08:55 - 09:00 **Velkomst**  
Dan Jensen, redaktionschef, Computerworld
- 09:00 - 09:35 **DEN SURE GAMLE IT-SIKKERHEDSCHEF ER NU MERE BEKYMRET END SUR...**  
Ken Bonefeld Nielsen, Sikkerhedsekspert
- 09:40 - 10:10 **Analyse af sårbarheder fundet i 2018**  
Mikkel Holm Brøndum, CEH, OSCP, OSWP – senior analyst, CGI
- 10:15 - 10:40 **Sikkerhed med brugeren i centrum**  
Søren Linde, Senior Mobility Consultant & Team Lead, Conscia
- 10:45 - 11:15 **Pause**
- 11:15 - 11:40 **Hvordan kommunikerer du it-sikkerhed og KRI til ledelsen? (Scene - SPOR 1)**  
Christian Schmidt, Direktør, Dediko
- 11:15 - 11:40 **Cyber crisis management kræver struktureret forberedelse og uddannelse (Scene - SPOR 2)**  
Christian Thygesen, partner, Rezilienze
- 11:45 - 12:10 **Vigtigheden af sikkerhed forankret i hardware**  
Flemming Pregaard, chief technologist, HP
- 12:15 - 13:00 **Frokost**
- 13:00 - 13:25 **Hvem roder rundt i dit datacenter. Du aner det ikke, vel? (Scene - SPOR 1)**  
Claus Jensen-Fangel, Security Evangelist, Atea A/S
- 13:00 - 13:25 **Humor mod hacking (Scene - SPOR 2)**  
Lis Kelså, Direktør, Humor mod hacking | Kelsa Media ApS  
Kim Larsen, GDPR / Compliance Manager, EG A/S  
Morten Eskildsen, datalogistuderende og whitehat-hacker, Humor mod hacking
- 13:30 - 13:55 **Fremtidens hackere er allerede i din hardware (live demo) (Scene - SPOR 1)**  
Keld Norman, IT sikkerhedskonsulent
- 13:30 - 13:55 **Sådan opdager du hackeren (Scene - SPOR 2)**  
Jonas J. Jacobsen, sales director, partner, GlobalSequor
- 14:00 - 14:25 **Brug et årshjul til at spise sikkerhedselefanten**  
Louise Bøttner, kundeansvarlig, Neupart  
Jakob Holm Hansen, CEO, Neupart
- 14:30 - 14:55 **Beskyt den digitale verden**  
Jacob Lie Vuust, Head of Public Sales, Fortinet  
Dennis Ladefoged, Manager System Engineering, Enterprise, Fortinet
- 15:00 - 15:20 **Pause**

- 15:20 - 15:45 **Hør erfaringerne fra CIO hos Farvskov kommune**  
Henrik Brix, It- og digitaliseringschef og Formand for de kommunale it-chefer, Farvskov kommune
- 15:50 - 16:20 **Den aktuelle cybertrussel mod Danmark**  
Peter Kruse, CISO, Clever
- 16:20 - 16:20 **Tak for i dag**

## 08:30 - 08:55: Morgenmad & Registering

## 08:55 - 09:00: Velkomst



**Dan Jensen**  
redaktionschef  
Computerworld

## 09:00 - 09:35: DEN SURE GAMLE IT-SIKKERHEDSCHEF ER NU MERE BEKYMRET END SUR...



**Ken Bonfeld Nielsen**  
Sikkerhedseksperter / Keynote

*Han har nemlig brugt jule og nytårsferien til at gruble over hvor vi og verden er på vej hen og hvad indflydelse det får på den moderne infrastruktur og hvilke scenarier der evt. kan komme til at udspille sig om en konsekvens af den storpolitiske kamp mellem Trump, Putin og den kinesiske præsident.*

*Hvad betydning kan fængslingen af en kinesisk CFO få for infrastrukturen i den vestlige verden og hvor kommer IOT ind i billedet? Scenen bliver sat for dagens øvrige indlæg med overordnede tanker om den særdeles vigtige digitale sikkerhed - som vi alle er afhængige af bliver kraftigt forbedret...*

## 09:40 - 10:10: Analyse af sårbarheder fundet i 2018



**Mikkel Holm Brøndum**  
CEH, OSCP, OSWP – senior analyst  
CGI / Partner

*I dette oplæg gennemgår penetrationstester Mikkel Brøndum, hvilke fejl og mangler han ofte stødte på under sine opgaver i 2018. Det gælder både organisatoriske, applikationsmæssige, driftsmæssige og netværksmæssige sårbarheder.*

*En af overskrifter er bl.a. at teknologien og dygtige serviceudbydere - på godt og ondt - lader os abstrahere fra sikkerhedsmæssige detaljer i temmelig mange sammenhænge, hvilket kan resultere i sårbare produkter, svage perimetere, underminering af sikkerhedsmodeller og falsk tryghed.*

*Hvis tiden tillader det, vil Mikkel vise, hvor let det er at identificere og delvist kompromittere IoT-enheder i nærheden af konferencen.*

## 10:15 - 10:40: Sikkerhed med brugeren i centrum



**Søren Linde**  
Senior Mobility Consultant & Team Lead  
Conscia / Partner

*Vi giver et bud på, hvordan din organisation kan øge it-sikkerheden og samtidig få mere tilfredse brugere.*

## 10:45 - 11:15: Pause

## 11:15 - 11:40 - Hvordan kommunikerer du it-sikkerhed og KRI til ledelsen? (Scene - SPOR 1)



**Christian Schmidt**  
Direktør  
Dediko / Partner

*Vurdering af den strategiske it-sikkerhed bygger på begreber som MÅLBAR it-sikkerhed og kommunikerbar it-sikkerhed. For at nå i mål med denne proces er det nødvendigt at sammenkæde bedste praksis med ressourcer i form af budget, personer og viden.*

*Kombinationen skal kunne kommunikeres til hele organisationen og til ledelsen, som skal tage ejerskab af den ACCEPTEREDE risiko. Sikkerhedsporofilen fra Drawares Dansk IT-Sikkerhedsbarometer™ er hjørnестenen i dette initiativ.*

*Her vil du lære, hvordan man bruger dette koncept til håndtering af strategisk it-sikkerhed.*

## 11:15 - 11:40 - Cyber crisis management kræver struktureret forberedelse og uddannelse (Scene - SPOR 2)



**Christian Thygesen**  
partner  
Rezilienze / Partner

Mange ledelser og itafdelinger undervurderer betydningen af konkret og professionel forberedelse, inden krisen slår ned som lyn fra en klar himmel.

Indlægget vil tage udgangspunkt i best practice og standarder, men hurtigt blive drejet over på, hvad der i praksis bør gøres før og under en alvorlig hændelse og igangsættelsen af en større krise, der kan smadre forretningen, hvis der ikke gennemføres en fornuftig kriseledelse...

## 11:45 - 12:10: Vigtigheden af sikkerhed forankret i hardware



**Flemming Pregaard**  
chief technologist  
HP / Partner

*Er dine pc'er og printere en del af virksomhedens samlede sikkerhedsstrategi? Mange virksomheder fokuserer deres indsats på datacenteret og antivirus, mens resten efterlades med kun grundlæggende beskyttelse og uden monitorering, hvilket gør dem sårbare overfor cyberangreb.*

*Flemming Pregaard viser med konkrete eksempler, hvorfor pc'er og printere bør være en del af den samlede sikkerhedsstrategi, og hvad din virksomhed kan gøre for at sikre sig endnu bedre og hurtigt komme videre, hvis du bliver angrebet.*

## 12:15 - 13:00: Frokost

## 13:00 - 13:25 - Hvem roder rundt i dit datacenter. Du aner det ikke, vel? (Scene - SPOR 1)



**Claus Jensen-Fangel**  
Security Evangelist  
Atea A/S / Partner

*Ikke mange har et godt svar på, hvordan man sikrer synligheden og sikkerhed i datacenteret, når en hacker er kommet uden om den dyre perimeter-sikkerhed.*

*Ofte bliver pengene brugt på at bygge mur og grave voldgrav, så fjenden ikke kan komme ind.*

*Mange er allerede kompromitteret. Fjenden har allerede agenter på indersiden. Hvad kan du så gøre?*

*Du skal ændre måden, som du tænker sikkerhed på!*

*Atea fortæller, hvordan man opnår synlighed og automatiseret trusselshåndtering i et datacenter med Palo Alto Networks og VMware NSX.*

## 13:00 - 13:25 - Humor mod hacking (Scene - SPOR 2)



**Lis Kelså**

Direktør

Humor mod hacking | Kelsa Media ApS / Partner



**Kim Larsen**

GDPR / Compliance Manager

EG A/S / Partner



**Morten Eskildsen**

datalogistuderende og whitehat-hacker

Humor mod hacking / Partner

*De fleste medarbejdere synes, at it-sikkerhed og GDPR er uinteressant og uvedkommende.*

*Men medarbejdernes adfærd er helt afgørende for organisationens it-sikkerhed. Derfor skal historier om it-sikkerhed og persondata fortælles, så medarbejderne bliver inddraget, involveret og inspireret.*

*Det er udgangspunktet i kampagnen 'Humor mod hacking' fra Kelsa Media, som har været en af ingredienserne i en vellykket awareness-kampagne i it-virksomheden EG de seneste måneder.*

*Kim Larsen fra EG, Morten Eskildsen fra Humor mod hacking og Lis Kelså fra Kelsa Media fortæller om awareness-kampagnens tilblivelse og anvendelse, og om erfaringerne fra udrulningen i en organisation med 1.900 medarbejdere fordelt på mere end 30 lokationer i flere lande.*

## 13:30 - 13:55 - Fremtidens hackere er allerede i din hardware (live demo) (Scene - SPOR 1)



**Keld Norman**

IT sikkerhedskonsulent / Keynote

*Telefonladeren, der overvåger dig. USB sticket, der slår din computer ihjel. Supply Chain Attacks kaldes det, når man installerer bagdøre i hardwaren, inden det kommer ud til forbrugeren. Se de vilde eksempler på virkelige hændelser.*

## 13:30 - 13:55 - Sådan opdager du hackeren (Scene - SPOR 2)



**Jonas J. Jacobsen**  
sales director, partner  
GlobalSeQur / Partner

*Vi ved, at hackerne kommer ind i virksomheders netværk. Så udover at prøve at forudsige og forhindre, så skal der fremover være mere fokus på at opdage og reagere.*

*Det er her, at SIEM er den centrale brik. Processen handler om områderne:*

- Compliance.
- Sikkerhed.
- Operations.

*Målet med præsentationen er at give deltagerne en forståelse af de forskellige elementer såsom:*

- Log management.
- SIEM.
- Analytics.

*Samtidig demonstrerer vi, hvordan andre teknologier fra RSA som playbooks, UEBA, packet inspection og endpoint detection & response kan bidrage til beredskabet. V*

## 14:00 - 14:25: Brug et årshjul til at spise sikkerhedselefanten



**Louise Bøttner**  
kundeansvarlig  
Neupart / Partner



**Jakob Holm Hansen**  
CEO  
Neupart / Partner

*Et voksende trusselsbillede. Nye og flere sikkerhedskrav. Øget bevågenhed fra ledelse, kunder og offentligheden. Det kan være en stor og kompleks opgave at holde styr på informationssikkerheden – især hvis der kun er få ressourcer til rådighed. Ved hjælp af et årshjul til implementering og vedligeholdelse af informationssikkerheden kan man effektivisere arbejdet og frigøre mere tid til at levere værdiskabende rådgivning til ledelsen.*

*Louise Bøttner og Jakob Holm Hansen viser, hvordan man etablerer et årshjul og kommer med smagsprøver på et helt nyt projektstyringsværktøj, der kan automatisere compliance-programmet, så den berømte elefant kan deles op og spises i små bidder.*

## **14:30 - 14:55: Beskyt den digitale verden**



**Jacob Lie Vuust**  
Head of Public Sales  
Fortinet / Partner



**Dennis Ladefoged**  
Manager System Engineering, Enterprise  
Fortinet / Partner

*Nutidens netværk er uden grænser og med en støt stigende kompleksitet. On-demand infrastruktur, cloud-baseret tjenester, software-defineret infrastruktur og de ikke-så-håndterbare IoT enheder, kræver en ny tilgang for at beskytte disse nye miljøer.*

*I mange år har anden-generations Firewalls, beskyttet infrastrukturen med indsigt i applikations-laget. Denne generation af firewalls er bygget til at fokusere på indhold, men mangler indsigt i nutidens komplekse netværk.*

*I dag ser vi begyndelsen af tredje-generation firewalls, hvor der fokuseres på hensigt i trafikken. Data er ikke længere på indersiden af den traditionelle perimeter, den er praktisk talt overalt og derfor er det blevet vigtigt at beskytte ens infrastruktur end-to-end. Data skal beskyttes lige meget om den i skyen, på en mobil eller på indersiden og sammenkobles med adfærds analyse for at kunne bestemme en hackers hensigt.*

*Derfor har vi skabt Fortinet Security Fabric med en integreret tilgang til nutidens infrastruktur. Kernen af Security Fabric'en er simpel. Sikkerhedsværktøjer er dybt integreret i netværket, mens de stadig operere i en bred vifte af miljøer fra cloud til IoT. De er vævet sammen i en fabric-baseret framework der tillader dem at indsamle, dele og korrelere trussels information mellem sikkerheds og netværks enheder. Politikker kan orkestreres og styres centralt mens en respons til trusler overalt på netværket kan automatiseres og koordineres.*

## **15:00 - 15:20: Pause**

## 15:20 - 15:45: Hør erfaringerne fra CIO hos Favrskov kommune



**Henrik Brix**

It- og digitaliseringschef og Formand for de kommunale it-chefer  
Favrskov kommune / Partner

## 15:50 - 16:20: Den aktuelle cybertrussel mod Danmark



**Peter Kruse**

CISO  
Clever / Keynote

*Cybercrime og avancerede digitale angreb fra organiserede kriminelle grupperinger samt statsaktører præger fortsat trusselsbilledet mod Danmark. Vi har aldrig tidligere været under et så vedvarende og konstant digitalt bombardement som i det forløbne år, og alle tal og tendenser fremskriver en fortsat stigning.*

*Med denne præsentation sættes der skarpt på de aktuelle og mest alvorlige trusler samt teknisk detaljer fra angreb med afsæt i et par konkrete case stories. Præsentationen vil blive krydret med tekniske demonstrationer af Crime as a Service værktøjer og paneler misbrugt af it-kriminelle i både globale og mere geografisk målrettede angreb.*

*Og endeligt skal vi kigge ned i den omfattende telemetri af threat intelligence som CSIS dagligt samler ind, både selv via vores mange services, og via betroede samarbejdspartnere. Dette telemetri kan hjælpe til at give et billede af hvilke aktører og lande som har mest fokus på at angribe mål i Danmark.*

## 16:20 - 16:20: Tak for i dag