IT-sikkerhed 2019

Onsdag den 23. januar

08.30	**Registrering**	
09.00	**Velkommen på IT-sikkerhed 2019**	
09.10	**Protecting the Swedish election 2018 against foreign influence campaigns** *Mikael Tofvesson, Chef, Enheten för omvärld och beredskap – (MSB)* This year, in May there will be an election to the European Parliament and before 17 June there will be a general election in Denmark. There have been several cases of foreign interference of elections in recent years. This presentation will highlight the systematic work of MSB and some lessons identified on how to protect elections against foreign influence campaigns.	
09.50	**Er din virksomhed klar til at blive hacket? - Vejledning fra NC3 og DANSK IT** *Rasmus Riis Kristensen, 'technical group lead'Nationalt Cyber Crime Center, NC3* NC3 og DANSK IT har udgivet en vejledning i, hvordan man bør forholde sig før og efter et sikkerhedsbrud. Få nogle klare anbefalinger til hvordan du bedst sikrer dine IT-systemer. Anbefalingerne går både på at holde hackerne ude, men også hvordan man undgår, at vigtige beviser bliver ødelagte, såfremt skaden allerede er sket.	
10.30	**Speeddating**	
10.55	**Pause**	
11.20	**Trusselsbilledet anno 2019** *Jens Christian Høy Monrad, Senior Analytiker, FireEye* Du vil blive præsenteret for en række hændelser i 2018, samt få et indblik i hvordan storpolitik har en direkte linje til hvordan visse stater udfører cyberangreb mod private virksomheder og lande.	**IoT kan forbedre sikkerheden** *Christian Damsgaard Jensen, Associate Professor, Head of Cyber Security Section, DTU* Introduktionen af IoT teknologi forbindes ofte med forringet sikkerhed, hvilket hovedsageligt skyldes producenterne af IoT udstyrs primære fokus på pris på bekostning af sikkerhed, men det skyldes også den øgede angrebsoverflade som introduktionen af IoT teknologi

		indebærer. IoT teknologi kan imidlertid også forbedre sikkerheden og hjælpe med at løse problemer der ellers er vanskelige at løse med teknologi, såsom "tailgating" og "shoulder surfing". Denne præsentation gennemgår eksempler på hvordan en sikret infrastruktur af IoT teknologi kan benyttes til at etablere konteksten for sikkerhedsrelaterede beslutninger, hvorved den generelle sikkerhed kan forbedres.
11.55	**Dilemma games** Vi stiller aktuelle IT sikkerhedsproblematikker på spidsen og tvinger dig til at tage stilling. Dilemmaspillet tester din intuition og udfordre dine beslutninger. Du vil komme hjem med finpudsede argumenter og være forberedt på modargumenterne for dine valg.	**Dilemma games** Vi stiller aktuelle IT sikkerhedsproblematikker på spidsen og tvinger dig til at tage stilling. Dilemmaspillet tester din intuition og udfordre dine beslutninger. Du vil komme hjem med finpudsede argumenter og være forberedt på modargumenterne for dine valg.
12.30	**Frokost**	
13.30	**BeyondCorp – brugere som den nye security perimeter** *Jesper Frederiksen, General Manager, EMEA, Okta Inc.* Gone are the days when all of your data was stored on servers in a room within your office building. Today, people are accessing data from outside the corporate firewall – working across a variety of cloud and on-prem apps, on a multitude of devices, from all over the world. The only consistent control point today is the user, and every person in your business is a potential target for a threat actor. Today, with more than 80% of all hacking-related breaches caused by compromised or poor credentials, it's critical for organizations to protect their users and, by extension, their sensitive data. Zero Trust and Google's BeyondCorp are security frameworks that take in this new threat landscape and say no user should be assumed to be trusted: everyone is a potential weak link in the system. In this talk, Jesper Frederiksen, Okta General Manager, EMEA, will explore what a Zero Trust framework	***Cyber Security – en kombination af præventive kontroller og aktivt forsvar.*** *Michael Weng, Senior OT/ICS/SCADA, Cyber Security Advisor & Threathunter/NSM Evangelist, ics2secure.com* 'Threathunting' og 'Cyber Threat Intelligence' er nogle af de nye ord, der har fået plads i medierne, men hvad dækker de over? Og hvad er baggrunden for dem? Kom og hør om forskellen på Cyber Security i IT og OT og få et bud på nogle simple retningslinjer, der kan hjælpe med at hæve Cyber Security niveauet betragteligt i både IT og OT. Og hør om hvad Threat Modelling er i den forbindelse.

	looks like, share insight into Okta's approach to identity-driven security as the foundation to a Zero Trust approach, and talk through example applications of Zero Trust in organizations today – showing how, with Okta, these companies can ensure that the right people have access only to the right information, and at the right time.	
14.05	**Transit**	
14.15	**GDPR – en fortælling der starter 25. maj 2018** *Allan Frank, IT-sikkerhedsspecialist, Datatilsynet* Nationale tilsyns brug af Forordningen til indgreb, bøder og kritik både i Danmark og resten af Europa. Vi tager et kig på erfaringerne med persondatasikkerheden siden forordningen trådte i kraft i maj sidste år. Du vil få indblik i tilsynets arbejde, klagesager og sikkerhedsbrud.	**Building Zero Trust networks with Microsoft 365** *Ken Hyld, Lead Technology Architect, Microsoft Technology Center*
14.50	**Pause**	
15.10	**Hackathon**	
15.25	**AI som sikkerhedskonsulent** *Martin Börjesson, Partner, 2021.ai* AI og Machine Learning, hvordan får vi skabt de rigtige retninger indenfor Data Sikkerhed, men samtidigt maksimeret værdien?	
16.05	**Reception**	
17.00	**Tak for i dag**	

IT-sikkerhed 2019

torsdag den 24. januar

08.30	**Morgenkaffe**
09.00	**Velkommen dag 2**

09.10	**Privacy, surveillance and hacking, protect yourself** *Henrik Lund Kramshøj, sikkerhedskonsulent Zencurity Aps* Do you think like an attacker? Why not. This talk will try to convince you to start attacking yourself, your company, your life. We will start to discuss your laptop security stance, the apps you use and the breadcrumbs you and your use of the internet leaves all over the place.	
09.50	**Transit**	
10.00	**Fokus på intern svindel - En måde at gribe det an på.** Tom Engly, Director, Chief Security Officer, Tryg Vi **skal** have tillid til vores medarbejdere, men må heller ikke være blinde overfor, at enkelte ikke altid gengælder den tillid. Derfor er det afgørende, at vi også gør en indsats for fokusere på dem der ikke gengælder den – både af hensyn til ejere og aktionærer, men ikke mindst overfor de ærlige medarbejdere, som der heldigvis er flest af. Indlægget giver et bud på, hvordan vi i Tryg har valgt at gribe dette an.	**National Cyber Information Strategy** **Decentrale cyber enheder** *Poul Thorlacius-Ussing, Overingeniør, Center for Cybersikkerhed* DCIS'erne rolle og forventningerne til dem i rammen af cyber – og informationssikkerhedsstrategien
10.35	**Pause**	
11.05	**Security Nudging** -3 eksempler på nudges, der hjælper brugerne i den rigtige retning *Sarah Aaalborg, Information Security Risk Manager, Novozymes* Har du overvejet at indføre nudging i din security awareness plan? Med enkle tiltag på det rigtige tidspunkt, kan du ændre dine brugeres adfærd. Kom og se tre enkle eksempler på nudges, der får brugerne til at være mere sikkerhedsbevidste - og som du måske allerede har teknikken til at udføre	**SAC Intro - Hvorfor, Hvordan, Hvad** *Marc Andersen, Incident Responder/Analytiker, NIL815* At bygge en enhed, der varetager monitorering og Incident Response er ikke noget småt foretagende. Enheden skal kunne håndtere ekstreme mængder af data, finde meningen i den samlede støj, reagere når truslerne manifesterer sig....og samtidig bevare et koldt hoved. En kort gennemgang vil belyse de fundamentale byggesten i et Security Analytics Center og de faldgruber der uvægerligt opstår.
11.40	**IOT: Hvor avanceret er APT angreb egentlig?** *Søren Egede Knudsen, Chefkonsulent, Energistyrelsen* På konferencer hører men ofte om APT (Advanced Persitent Threat) angreb og nogle	**Hackerlandsholdet**

	gange bliver det sagt at dem kan man ikke stoppe! Men, hvor avancerede er de egentlig? I denne præsentation vil tages et retrospektivt billede af nogle ATP angreb i OT miljøer. I dette vil jeg gennemgå nogle detaljer om udvalgte APT-angreb. Dette både om selve angrebet/malwaren men også nogle strategier, der kan bruges for at opdage et angreb, samt beredskabet organisationen bør have. Sessionen vil indeholde tekniske og organisatoriske behov for at have et godt beredskab, og hvordan disse skal arbejde sammen for at få en mere effektiv plan mod cyberangreb.	
12.15	**Frokost**	
13.15	**Internet of things - trojansk hest eller civilsationens St. Bernard hund** Hvad betyder IoT i forhold til private og virksomheders effektivitet, fortrolighed og sikkerhed *Per Ahlmann Andersen, Bestyrelsesmedlem DANSK IT, Founder og CEO, BIEXA.COM* Med Internet of Things står vi overfor et tipping point i forhold til adoption og hvilken værdi kan vi få ud af teknologierne. Tech giganterne kæmper lige nu en vigtig kamp på området, men hvorfor og hvordan? Dette vil Per give dig et indblik i samt komme ind på, hvad vi alle bør være opmærksomme på. Herunder - Hvor godt er virksomheder og forbrugere beskyttet af standarder og hvad kan og bør der gøres på IT Sikkerhedsområde.	**Sikkerhedshændelser - hvad gør man når man får opkaldet? -** Erfaringer fra et liv i den skarpe ende *Lars Borgeskov, Politiet Lars Borgeskov, sektionsleder, Rigspolitiet Koncern IT Sikkerhed*

13.50	**Pause**	
14.10	**Nyt fra det digitale domæne** *Flemming Splidsboel Hansen, Seniorforsker, Dansk Institut for Internationale Studier* Stater har i stigende grad fokus på det digitale domæne som en særskilt arena og som en enabler for operationer i de fysiske og kognitive domæner. Udviklingen giver en masse muligheder men medfører også helt nye trusler.	
15.00	**Afrunding og tak for i år**	