IT-SIKKERHED 2016

Konference i København 3. og 4. februar 2016

Program 3. februar 2016

08.30	**Registrering og morgenmad**
09.00	**Velkommen**
09.10	**Keynote: It-sikkerhed - Topledelsens ansvar** Lars Mikkelgaard-Jensen, bestyrelsesformand, IBM Danmark Sikkerhedsfolk oplever ofte, at det er svært at få ledelsen i tale, og når det så lykkedes, så er det ikke altid ledelsen eller forretningen forstår dem. Som en følge heraf får sikkerhed ikke nødvendigvis den 'rigtige' eller nødvendige prioritet i hverdagen. I dette indlæg kommer Lars Mikkelgaard-Jensen med tips til hvad du som sikkerhedsfaglig kan gøre for at målrette din kommunikation med henblik på at sælge sikkerhed til forretningen.
09.55	**Virksomhedskulturs påvirkning af sikkerhedskultur** Martin Warming, CISO, DONG Energy Hvordan har DONG Energy brugt den eksisterende virksomhedskultur til at sikre forankring af informationssikkerhed og derved sikre opbakning til den rejse, vi er på.
10.30	**Speed dating**
10.45	**Pause**
11.10	**Indfrielse og omlægning af teknisk gæld** Kerny Ustrup, it-direktør, MT Højgaard Med baggrund i en tværgående risikoanalyse inden for IT-området besluttede MT Højgaard at sætte gang i en modernisering af både processer, applikationer og infrastruktur. Formålet med øvelsen var at reducere den tekniske gæld, så virksomheden it-mæssigt bedre kunne understøtte et vækstscenarie, udløse koncernsynergier og desuden reducere de it-mæssige sikkerhedstrusler.

11.45	**10 teser om sikkerhed i balance** Rasmus Theede, formand, Rådet for Digital Sikkerhed De seneste år har en række offentlige myndigheder og private virksomheder været ramt af alvorlige hackerangreb og brud på it-sikkerheden. Hidtil har indsatsen været primært rettet mod centrale offentlige myndigheder og udvalgte store virksomheder. Men alle virksomheder og offentlige organisationer risikerer at blive udsat hackerangreb eller miste kritiske data, hvis de ikke har styr på deres sikkerhedsprocesser. Rasmus Theede, formand for Rådet for Digital Sikkerhed, kommer med sine 10 bud på hvordan man imødegår den stigende sikkerhedstrussel i balance med interne og eksterne krav.
12.20	**Frokost**
13.20	**From Words to Action** Patrik Håkansson, Group Security Advisor, Ericsson In a bid to ensure none of its 114,000 staff worldwide were using company equipment to view illegal content, in 2011 Ericsson started to install a CAM (child abuse material) detection software on its computer assets globally. Patrik Håkansson, one of the primary drivers behind the initiative, tells the inside story and the challenges behind launching a global corporate program to protect the most vulnerable in society. Patrik touches on a number of areas to consider; legal and technical challenges, cultural differences, attention by law enforcement, corporate prerequisites, internal and external communication. Patrik Håkansson is one of the primary drivers of the company's Action against Child Sexual Abuse (CSA) program and specialised in coordination and execution of internal investigations of CSA related cases and other corporate investigations globally.
13.55	**Truslen fra internettet fra Trusselsvurderingsenheden i Center for Cybersikkerhed** Thorsten Foldager Johnsen, sektionschef, Center for Cybersikkerhed I dette indlæg orienteres om enhedens virke og sammensætning, og Thorsten gennemgår enhedens seneste generelle trusselsvurdering.
14.30	**Pause**

14.55	**Hvorfor har vi stadig sikkerhedsproblemer? Et nostalgisk tilbageblik på de gode gamle dage og hvad vi måske stadig kan bruge erfaringerne til i det 21. århundrede.** Ole Stampe Rasmussen, tidligere PBS (Pengeinstitutternes Betalings Systemer) I databehandlingens barndom i 1960'erne og 70'erne handlede it-sikkerhed primært om at holde maskinerne i gang. Vi var rigtig gode til at tage back-up og restarte, for alle opgaver kørte som timelange batches, hvor man kunne risikere at skulle starte forfra, hvis maskinen brød sammen. Og det gjorde de jævnligt! Svindel og misbrug var meget sjældent og involverede altid egne medarbejdere, så det havde man simple interne kontroller til at forhindre. Ingen havde nogensinde hørt om computervirus og hacking. I starten af 1980'erne var pengeinstitutterne ved at drukne i papirchecks, og man erkendte, at den eneste økonomiske løsning ville være et realtidssystem med datafangst ude i butikkerne. Det indebar et helt nyt risikobillede for it-sikkerheden. 25.000 terminaler ude i et helt ukontrollerbart "fjendeland" med opkobling til en central computer via ukontrollerbare kommunikations-forbindelser gav nogle hidtil usete udfordringer. Det lykkedes at få løst disse udfordringer, og i 1984 kunne den første Dankort-transaktion køre igennem systemet. Siden da er milliarder af transaktioner kørt igennem, og ingen har været i stand til at bryde den grundliggende sikkerhed i systemet. Der har imidlertid været utallige andre sikkerhedsbrud siden 1984. Indlægget vil forsøge at belyse nogle af årsagerne til disse brud.
15.30	**Overrækkelse af Cybersikkerhedspris og præsentation af idé**
16.05	**Reception med drikkevarer og snacks**
17.00	**Tak for i dag**

Program 4. februar 2016

08.30	**Registrering og morgenmad**
09.00	**Velkommen til dag 2 - opsamling på dag 1**
09.10	**Securing DNS against malware threats & the importance of an integrated security ecosystem** Richard Langston, Senior Product Manager Security, Infoblox Today's targeted attacks pose a threat to both data and infrastructure in an enterprise. Cyber criminals constantly create new infrastructure to launch DNS attacks, infiltrate a network and use DNS as a pathway for data exfiltration. Learn how to defend against DNS threats and prevent data exfiltration while leveraging the benefits of an integrated security ecosystem.

09.45	**Outsourcing og sikkerhed** Poul Otto Schousboe, Head of Group IT Security, Danske Bank
10.20	**Pause**
10.45	**Informationssikkerhed i Københavns kommune** Andreas Hare, centerchef, it driftscenter, Københavns kommune Københavns Kommune oplever som alle andre myndigheder et stigende pres fra IT kriminelle, herunder angreb med Ransomware.Hør hvordan Københavns Kommune har optrappet sin fokus på IT-sikkerhed på en række parametre: Proces, Ledelse, Awareness, Monitorering og Protection.
11.20	**Sikring af kritisk (IT-)infrastruktur** Christian Damsgaard Jensen, Ph.D., Applied Matemathics & Computer science, DTU Kritisk infrastruktur overvåges og kontrolleres i stigende grad gennem åbne netværk, såsom Internettet, hvilket åbner mulighed for at kriminelle eller fremmede magter kan forstyrre eller overtage kontrollen med dele af den kritiske infrastruktur. Dette indlæg ser på nogle af de udfordringer der opstår når man ønsker at styre og koordinere kritisk infrastruktur ved hjælp af COTS-komponenter gennem Internettet.
11.55	**Frokost**
12.55	**Cyberintelligence - fundamentet for en proaktiv indsats** Jakob Scharf, Executive Director/ Co-founder, CERTA Intelligence & Security Et effektivt cyber-forsvar forudsætter, at den enkelte organisation kan agere proaktivt i forhold til konkrete trusler, og at organisationen er i stand til hurtigt at erkende, afdække samt afværge konkrete angreb og derved begrænse eventuelle skadevirkninger mest muligt. Brugen af cyber-intelligence udgør fundamentet for en proaktiv indsats og indebærer, at der løbende indsamles og bearbejdes internetbaserede efterretninger om konkrete angrebsplaner mod organisationen - herunder om angriberne, deres metoder og fremgangsmåder - lækkede oplysninger samt tekniske forhold og andre sårbarheder i forhold til organisationen, der vil kunne udnyttes i forbindelse med et cyber-angreb. Jakob Scharf giver en introduktion til cyber-intelligence og vil i forbindelse med sit indlæg gennemgå en række cases inden for cyberintelligence.

13.30	**Identitetstyveri - nyt begreb, gammel forbrydelse?** Anders Young Rasmussen, konsulent, Det Kriminalpræventive Råd og Philip Lundsgaard, offer for identitetstyveri Forskellige undersøgelser viser, at identitetstyveri er en af de typer forbrydelser, som folk er mest bekymrede for. Der er findes talrige historier om, hvordan ofre har opdaget, at de har været udsat for identitetstyveri, fordi regninger og rykkere har hobet sig op i postkassen. Men hvad er identitetstyveri egentlig, og kan man forebygge det? Konsulent i Det Kriminalpræventive Råd Anders Rasmussen, vil belyse begrebet nærmere og fortælle om, der egentlig er grund til bekymring. Herudover kan du møde Philip Lundsgaard, der har været udsat for identitetstyveri, og høre hans personlige beretning om de konsekvenser, som identitetstyveriet har haft for ham.
14.05	**Pause**
14.30	**Datatilsynets tilsynsvirksomhed** Cristina Angela Gulisano, direktør, Datatilsynet I dette indlæg vil Datatilsynets direktør Cristina Angela Gulisano fortælle om tilsynets virksomhed og fokusområder. Herudover til vil Cristina orientere om de dele af myndigheders og virksomheders varetagelse af persondatabeskyttelsen som oftest giver anledning til kritik.
15.05	**Hackernes mange muligheder - fokus på Ransomware og andre aktuelle angreb** Jacob Herbst, Chief Technology Officer, Dubex
15.40	**Afrunding**
15.45	**Tak for i år**

DANSK IT tager forbehold for ændringer i programmet

Senest opdateret 26. januar 2016