

Datasikkerhed

26. marts - Radisson Blu Scandinavia Hotel, Aarhus, Århus C

08:30 - 08:55	Morgenmad og registrering
08:55 - 09:00	Velkomst
09:00 - 09:40	De største trusler netop nu
09:45 - 10:10	Enabling a secure mobile organization
10:15 - 10:40	Privacy og datasikkerhed
10:45 - 11:00	Kaffepause
11:00 - 11:25	Beskyt dine identiteter
11:30 - 11:55	Datalækager - en af vor tids største digitale udfordringer
12:00 - 12:25	Overvågning er dit bedste sikkerhedsværktøj
12:30 - 13:15	Frokost
13:15 - 13:40	Spotting Security-Minded Solutions
13:45 - 14:10	Human Behaviour: The Final Frontier?
14:15 - 14:55	2014: Danmark under angreb
15:00 - 15:00	Afslutning på dagen, kaffe og kage

08:30 - 08:55: Morgenmad og registrering

08:55 - 09:00: Velkomst

09:00 - 09:40: De største trusler netop nu

Det vælter dagligt ud med nyheder om nye trusselsformer, APT-angreb, avanceret malware, forskellige sikkerheds-riscici og mange andre ting, som man skal passe på.

De store mængder informationer kan gøre det svært at prioritere, hvad man egentlig skal satse på, ligesom det er et tilbagevendende spørgsmål til sikkerheds-firmaerne, hvad vi egentlig kan forvente i fremtiden.

Men spørgsmålet er grundlæggende forkert, og det viser, at vi har en forkert tilgang, når vi tænker på og drøfter it-sikkerhed.

Kaspersky-ekspert David Jacoby ridser billedet klart op på sin morsomme og provokerende facon: Det egentlige sikkerhedsproblem ligger faktisk et helt andet sted. Kom og få smasket lige i fjæset, hvad tidens største sikkerhedsproblem egentlig er for dig og dit firma.

09:45 - 10:10: Enabling a secure mobile organization

- Gain insight into the risks and evolving attack vectors challenging the mobile organization*
- Find out why it is important to define guidelines that will balance security and operations to usability and business continuity*
- Get an overview to solutions and security guidelines that protect the users, data and assets of the mobile organization*

10:15 - 10:40: Privacy og datasikkerhed

Privacy og datasikkerhed optager med god grund alle i it verdenen i disse år. Med potentielle sikkerhedsmæssige udfordringer som følge af bring your own device, big data for eksempel, og senest med den massive pressedækning af Edward Snowden-dokumenterne, er også mange almindelige borgere blevet gjort interesserede i emnet.

Naturligvis befinder en lang række store it firmaer sig midt i stormens centrum, men emnet er absolut ikke nyt for Microsoft. Siden firmaet blev stiftet i 1975 er der proaktivt blevet arbejdet med sikkerhed. Arbejde blev kraftigt intensiveret i 2003, hvor emnet blev gjort højaktuelt af de første brede udfordringer med cybersikkerhed på grund af blandt andet Blaster og Slammer-vira.

Privacy og datasikkerhed gennemsyrrer al produktudvikling, forskning, drift og generel forretningsførsel i Microsoft. Og på det seneste har en række juridiske og politiske tiltag også fundet vej i arbejdet og endda skabt en alliance mellem ellers konkurrerende virksomheder i branchen.

I denne session vil Ole Kjeldsen, som er national technology officer i Microsoft Danmark, give et indblik i, hvordan Microsoft arbejder med privacy og datasikkerhed i de mange forskellige dimensioner og ikke mindst fremvise hvordan firmaet forholder sig til og arbejder med verserende sager.

10:45 - 11:00: Kaffepause

11:00 - 11:25: Beskyt dine identiteter

Hacking og tyveri af bruger-identiteter er fortsat en af de hurtigst voksende måder at kompromittere bruger-identiteter og dermed også vores organisationer på. SMS PASSCODE vil i dette indlæg se på de seneste tendenser samt på de muligheder, der ligger i beskyttelsen af identiteterne uden at gå på kompromis med de fortsat stigende krav fra brugerne om fleksibel adgang til it-systemer.

11:30 - 11:55: Datalækager - en af vor tids største digitale udfordringer

Kim Aarenstrup, der er bestyrelsesformand for det internationale Information Security Forum og fhv. it-sikkerhedsdirektør i Mærsk, fortæller om udfordringerne omkring datalækager, og hvilke aspekter man skal være opmærksom på.

Garneret med et par praktiske eksempler fortæller Kim om hvilke metoder man bør overveje i forhold til at få disse ting under kontrol.

12:00 - 12:25: Overvågning er dit bedste sikkerhedsværktøj

De seneste år har vist os, at virksomheder opdager alvorlige hændelser i deres netværk alt for sent - hvis de da overhovedet opdager dem. Resultatet er, at store mængder kritiske data mistes, hvilket medfører store omkostninger og tab for virksomhederne: Konkurrencemæssige forspring mistes, brugerne mister tilliden, og der skal bruges mange ressourcer på oprydning.

Efterhånden som angrebene bliver mere avancerede og infrastrukturen mere kompleks, er sikkerhedsovervågning vores vigtigste værktøj til at kunne opdage og reagere på sikkerhedsbrister i tide. Sikkerhedsovervågning trækker på data fra forskellige systemer og er et redskab til at prioritere indsatsen i forbindelse med kritiske sikkerhedsbrud på infrastrukturen.

Dette indlæg omhandler, hvorfor overvågning er vigtig, og hvordan man kan skabe værdi ud fra viden om og overblik over aktiviteten på ens netværk.

12:30 - 13:15: Frokost

13:15 - 13:40: Spotting Security-Minded Solutions

CIO'er, it-chefer og sikkerhedschefer skal træffe vanskelige beslutninger, når de står over ny-indkøb af it-sikkerheds-systemer.

Nye løsninger skal understøtte de nuværende forretningsprocesser og ikke gøre, at du er nødt til at udvikle nye.

Her præsenterer vi en smart måde til at få overblik og overskud på baseret på en lang liste af features og karakteristika, ligesom vi kommer nærmere ind på forskellen mellem teknologisk- og sikkerhedsorienterede løsninger og hvordan de forskellige løsninger vil kunne påvirke dine forretningsprocesser og din ROI.

Og så har vi en tjekliste til at evaluere nye løsninger helt i bund.

13:45 - 14:10: Human Behaviour: The Final Frontier?

Interne datalækager er en udfordring i mange organisationer, og skylden skal ofte findes i social engineering, lækager hos interne folk samt øvrig, generel menneskelig adfærd.

Pilen peger med andre ord næsten altid i retning af menneskelig adfærd, når det gælder datalækager i organisationerne.

I fremtiden vil det være vigtigt at få totalt styr på disse mulige datalækager. Det arbejder blandt andet forskningsprojektet TRESPASS på via avancerede modellerings- og analyseteknikker, som skal gøre det muligt at spotte datalækager meget tidligt.

Hør om udfordringerne ved internedatalækager, og hvordan forskerne forestiller sig, at man kan tackle problemet.

14:15 - 14:55: 2014: Danmark under angreb

Flere end 100.000 PC'ere i Danmark er inficeret med virus/malware. Og endnu værre en type virus/malware som har dataindsamlende egenskaber, hvilket betyder at bagmændene systematisk høster følsomme data fra de mange systemer. Der er tale om inficerede PC'ere som befinder sig hos offentlige myndigheder og institutioner, private virksomheder og almindelige slutbrugere. Præsentationen vil blive krydret med eksempler på hvordan denne type angreb udføres og hvordan de it-kriminelle med stor lethed kan fjernkontrollere i tusindvis af systemer på samme tid.

15:00 - 15:00: Afslutning på dagen, kaffe og kage