Opdatér din viden om trusler og

datasikkerhed

Guldpartnere:

CHECK POINT Software Technologies Ltd. ezenta

PROGRAM - PLENUM

08:30 **Morgenmad og registrering**

09:00 **Velkomst**

v/Kim Stensdal, teknologiredaktør, Computerworld.

09.05 **Privacy og datasikkerhed**

v/Ole Kjeldsen, national technology officer, Microsoft

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 gennemsyrer 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.

09:45 **Sådan beskytter du store mængder kritiske data**

v/Peter Sandkuijl, Europe network security se manager, Check Point

The targeted attacks towards large corporate, national- and state databases containing sensitive data are rapidly increasing. Are you ready for increased hacker activity threats that cannot be detected by ordinary security controls?

Gain insight to the hackers secrets and dissect the invasion techniques behind using practical examples.

Find out how to select countermeasures and provide proper mitigation security controls and detection tools.
Learn how to balance business assets and risk mitigation investments.

10:15 **Kaffepause, networking**

10:30 **OPDELING I SPOR - SE SIDE 2**

12:30 **Frokost og networking**

13:15 **De største trusler netop nu**

v/David Jacoby, senior security researcher, Kaspersky

The security industry is constantly written about new threats, APT attacks, advanced malware and security risks. This information can be quite difficult to grasp and prioritize. Also, as security analysts we often get asked the question: “What threats and vulnerabilities do you expect we will see in the future?” This is a very interesting question but also an indication that the way we think about and discuss IT security is fundamentally wrong.

Let me tell you a story that hopefully will help you understand what we are actually vulnerable against, and also learn about some of the largest security threats out there in a funny but provocative presentation.

14:00 **Roundtable**

15:00 **Tak for i dag**

Opdatér din viden om trusler og

datasikkerhed

OPDELING I SPOR

OVERVÅGNING

10.30 **Sådan får vi bugt med de cyberkriminelle**

v/Mr. Jean-Dominique Nollet, head of Laboratory European Cybercrime Centre

I øjeblikket er der nærmest frit lejde for it-kriminelle. Det skal der naturligvis laves om på. Det skal ikke være attraktivt at bruge nettet til kriminalitet. Det er en svær opgave at vende billedet, men den er ikke umulig.

Hør hvad European Cybercrime Centre gør for at løse disse problemer.

11.00 **Overvågning der virker**

v/Ken Willen | security business manager, Ezenta

Overvågning har fået en negativ klang - i 2013 ikke mindst med Edward Snowdens afsløringer af NSA's omfattende overvågning af fjender og "venner". Det har blandet andet givet en debat om virksomheders overvågning af medarbejdere.

I Ezenta får vi i stigende grad henvendelser fra virksomheder, der ønsker at beskytte sig mod konkrete hændelser, der omfatter læk af følsom information. Flyttes fokus af Edward Snowdens afsløringer fra krænkelse af den personlige frihed til konsekvenserne for berørte virksomheder af, at fremmede magter og konkurrenter har adgang til virksomhedernes følsomme informationer, så kræver det handling.

Set fra et it-sikkerhedsmæssigt perspektiv er virksomheders overvågning et must for at afværge, at trusler kommer ind i virksomheden, og følsom information lækkes fra virksomheden.

I dette indlæg gives et indblik i, hvad overvågning kan indbefatte, hvordan det kan implementeres uden at kompromittere den enkelte medarbejders fortrolighed, samt hvordan man med en analyse kan få et overblik over, hvor man først bør sætte ind med ekstra it-sikkerhedskontroller.

HACKING

10.30 **2014: Danmark under angreb**

v/Peter Kruse, head of CSIS eCrime Unit

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

11.00 **Live hacking**

v/Jesper Mikkelsen, security expert, certified ethical hacker, Trend Micro

Demo af hvorledes en hacker kan kompromitere blandt andet en web-server via SQL-injections og code-injections.

Oplev hvordan en brugers browser bliver hooked, og hvad hackeren efterfølgende kan gøre ved det inficerede system.

Traditionelle sikkerhedsforanstaltninger er ikke længere nok, så hvad kan vi gøre mod targeted attacks?

INTERNE DATALÆKAGER

10.30 **Poul Otto Schousboe, CSO, Danske Bank**

11.00 **Data loss prevention**

v/Peter Schjøtt, sikkerhedsspecialist, Symantec

Alle organisationer har data, der ikke skal slippe ud af organisationen til uvedkommende. Det kan foreksempel være børsmeddelelser (for tidligt), patenter, nye produkter, patientdata eller andre personlige oplysninger. Langt de fleste organisationer kæmper med, hvordan de undgår at disse oplysninger skal slippe ud enten ved fejl eller forsætligt. Det er ikke gjort med at skrive et par linier i en sikkerhedspolitik, når det gælder om at styre, hvilke data der må distribueres, sendes og gemmes til hvem og hvordan.

Data Loss Prevention (DLP) er et koncept, som kan hjælpe virksomhederne med at finde fortrolige data, afgøre hvordan de behandles korrekt, uddanne brugerne i hvad der er rigtigt og forkert og så videre.
Men DLP griber også grundlæggende ind i organisationens processer og forretningsgange. DLP er ikke bare et værktøj it-afdelingen skal implementere, men griber langt bredere ind. Derfor er det vigtigt at finde ud af, hvad man vil med DLP og hvordan man vil begynde med at implementere DLP.

Sessionen vil give en high-level introduktion til DLP, og de tanker, man skal gøre sig, hvis man overvejer at implementere DLP. Sessionen er generel.

Indhold i sessionen:

- Hvad er DLP
  – og hvad er DLP ikke
- Overvejelser man skal gøre sig inden man påbegynder et DLP projekt
- Hvad er IT's rolle – og hvad skal andre afdelinger levere
- DLP og BYOD
- Faser i implementeringen af et DLP projekt
- Et par Symantec erfaringer fra DLP projekter

OVERVÅGNING

11.30 **Overvågning er dit bedste sikkerhedsværktøj**

v/Jacob Herbst, CTO, Dubex A/S

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.

12.00 **Opdag angreb tidligt**

v/Henrik Kramshøj, internet samurai, Solido Networks

Hvordan finder man nålen i høstakken, når brugere og applikationer genererer store mængder netværksdata og metadata.

Når vi idag skal efterforske hændelser, er det vitalt, at man ved, hvad der sker på netværket. Vi vil med udgangspunkt i vores erfaring med angreb på internet pege på de vigtigste områder, man bør overvåge i netværket. Vi vil henvise til de underliggende teknologier, som alle kan bruge med eksempler på, hvordan angreb opdages og bekæmpes effektivt ud fra en leverandøruafhængig tilgang.

Indlægget er således vores bud på praktiske tiltag til at forbedre sikkerheden ved brug af Network Security Monitoring.

HACKING

11.30 **Beskyt dine identiteter**

v/Morten Skovsgaard, SMS PASSCODE

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 forsat stigende krav fra brugerne om fleksibel adgang til it-systemer.

12.00 **Krig i cyberworld**

v/Jens Monrad, Fireeye

Cyber attacks have already proven themselves as a low-cost, high-payoff way to defend national sovereignity and to project national power.

Cyber weapons are being used as an advantage in real-world conflict; the biggest challenge is to deterring, defend against, or retaliating for cyber attacks is the problem of correctly identifying the perpetrator. Ballistic missiles come with return addresses, but computer viruses, worms, and denial of service attacks often emanate from behind a veil of anonymity. The best chance to pierce this veil comes with the skillful blending of forensic “back hacking” techniques.

Understand ”Nation-State Motives Behind Today’s Advanced Cyber Attacks”, that describes the unique international and local characteristics of cyber attack campaigns.

INTERNE DATALÆKAGER

11.30 **Human Behaviour: The Final Frontier?**

v/Rene Rydhof Hansen, lektor, Aalborg Universitet

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 interne datalækager, og hvordan forskerne forestiller sig, at man kan tackle problemet.

12.00 **Datalækager - en af vor tids største digitale udfordringer**

v/Kim Aarenstrup, formand, Information Security Forum

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.

I samarbejde med:

Check Point Software Technologies Ltd. · sms passcode · ADDPRO · TREND MICRO · ezenta · Symantec · Dubex: MANAGING RISK. ENABLING GROWTH.® · FireEye

Arrangeret af:

COMPUTERWORLD