Datasikkerhed

30. august - Comwell Hotel Aarhus, Aarhus

08:30 - 09:05	**Morgenmad & registrering** Dan Jensen, redaktionschef, Computerworld
09:05 - 09:35	**Siscon: Ingen panik endnu - men praktisk og struktureret tilgang** Jesper B. Hansen, CTO, Siscon
09:40 - 10:10	**Datasikkerhed - nødvendigt onde eller konkurrenceparameter?** David Hald, chief strategy officer, CensorNet
10:15 - 10:40	**Kaffepause og networking**
10:40 - 11:05	**Keepit: Sikkerhed i en Skyet fremtid - Fokus på Microsoft Office 365** Magnus Cohn, Chief Commercial Officer, Uniqkey
11:10 - 11:35	**Conscia: Visibilitet og kontrol i infrastrukturen: real-time og end-to-end!** Torben Nissen Ernst, security expert, Conscia
11:40 - 12:05	**Live hacking session** Kim Elgaard, Security Specialist/Etisk Hacker, Arrow ECS Denmark A/S
12:10 - 13:00	**Frokost**
13:00 - 13:25	**RSA: Cyber risk - The perfect storm** Jesper Sachmann, Nordic GRC Lead, RSA
13:30 - 14:05	**Den kommende EU-dataforordning - hvad kan danske virksomheder forvente?** Martin Von Haller Grønbæk, partner, Bird & Bird
14:10 - 14:35	**Check Point: En af tidens største trusler mod IT-sikkerhed: Ransomware** Kim Thostrup, team lead SE, Check Point Software Technologies
14:40 - 15:00	**Kaffe og kage**
15:00 - 15:25	**Hvordan modnes fokus på informationssikkerhed i en global virksomhed?** Peter Winkel Madsen, Manager IT Operations & Security Group IT, Bunker Holding A/S
15:30 - 15:55	**Det aktuelle trusselsbillede: Cyberangreb mod danske virksomheder og myndigheder** Thomas Kristmar, Afdelingschef, Policyafdelingen, Forsvarets Efterretningstjeneste, Center for Cybersikkerhed
16:00 - 16:00	**Tak for i dag**

08:30 - 09:05: Morgenmad & registrering



Dan Jensen
redaktionschef
Computerworld

09:05 - 09:35: Siscon: Ingen panik endnu - men praktisk og struktureret tilgang



Jesper B. Hansen
CTO
Siscon / Partner

Kravene i den kommende forordning kan med fordel implementeres som en overbygning på det informationssikkerheds-fundament, der forventeligt allerede findes i din virksomhed.

Formår du at anvende dit nuværende it- og informationssikkerhedsarbejde som fundament, bliver det nemlig langt enklere at efterleve og opfylde EU-forordningens krav på en struktureret og overskuelig måde. Implementeringen af EU-persondataforordningen er en fælles øvelse mellem forretningen, compliance og informationssikkerhed i din virksomhed.

Med en praktisk vinkel gennemgår Jesper B. Hansen de opgaver, som du bør have på din agenda:

- Opbygning og overblik over hvordan forretningsprocesserne er understøttet.
- Dataflowanalyse til at skabe overblik over virksomhedens kritiske data, og hvordan de flyder.
- DPIA (Data Protection Impact Assesment') som udvidelse til den eksisterende risikostyring.

09:40 - 10:10: Datasikkerhed - nødvendigt onde eller konkurrenceparameter?



David Hald
chief strategy officer
CensorNet / Partner

Vi har aldrig har været mere afhængige af data, og samtidig har vores systemer aldrig været mere udsatte, end de er i dag. Det er med andre ord vanskeligt at balancere forholdet mellem sikkerhed og forretningsbehov, men ikke desto mindre afgørende for virksomhedens fortsatte konkurrenceevne.

Truslerne er mange, og hvad enten faren kommer ude fra eller sker som følge af medarbejderes uagtsomhed, er det nødvendigt at kunne identificere problemet hurtigt og gribe til handling.

Med CensorNet's Unified Security Service kan du få syn for sagen.

Du kan blandt andet se, hvilke applikationer der bliver brugt på jeres netværk, vurdere risikoen og om nødvendigt gribe til handling. Alt sammen fra ét brugervenligt dashboard.

Produktet giver ikke alene mulighed for at kontrollere adgangen til cloud-applikationer, men også hvilke features brugerne kan anvende i de enkelte applikationer. Dertil kommer effektiv web filtrering og avanceret e-mail scanning samt beskyttelse af fjernadgang med SMS PASSCODE.

Denne komplette produktportefølje giver en 360 graders-sikkerhedsløsning, som gør it i stand til at håndtere de nye udfordringer og sikre, at virksomhedens systemer, data og medarbejdere er godt beskyttede og kan udføre deres arbejde med god samvittighed.

Se CensorNet's indlæg og bliv klogere på:

- *Hvordan du kan kaste lys over skygge-it i virksomheden-*
- *Hvor nemt du kan kontrollere cloud-applikationer på bruger/feature niveau.*
- *Hvordan SMS PASSCODE kan styrke produktiviteten.*
- *Hvordan maskinlæring hjælper med at korrelere data på tværs af trusler.*

10:15 - 10:40: Kaffepause og networking

10:40 - 11:05: Keepit: Sikkerhed i en Skyet fremtid - Fokus på Microsoft Office 365



Magnus Cohn
Chief Commercial Officer
Uniqkey / Partner

Sikkerhedsbilledet ændrer sig konstant, og det er svært at følge med og understøttelse nye teknologier og cloud-tjenester.

En samlet løsning som Office 365 er et fantastisk værktøj til enhver organisation, men samtidig udgør det en risiko at gemme al virksomhedens data ét sted.

Mange tror fejlagtigt at cloud-tjenester er ensbetydende med backup - men i virkeligheden har de brug for støtte.

*Kom og hør om **Sikkerhed i en skyet fremtid** og hør mere om de primære kilder til datatab i skyen samt hvilke elementer, det er vigtigt at overveje, når man flytter/har flyttet jeres data i en cloud-tjeneste som Office 365.*

Hvad er Office 365 backup fra Keepit?

Ved at tilføje et ekstra sikkerhedslag fra en uafhængig backup-løsning løftes sikkerhedsniveauet, og I opnår en uvurderlig beskyttelse af jeres vitale data og sikrer, at I kan komme hurtig i gang efter eksempelvis et ransomware-angreb.

Keepit er Danmarks største leverandør af online backup- og restore-løsninger. Keepit Office 365 Connector med Continuous Data Protection giver jer et værdifuldt overblik over al jeres data i Office 365 og nem adgang til hurtigt at genskabe tabt data efter for eksempel et ransomware-angreb.

11:10 - 11:35: Conscia: Visibilitet og kontrol i infrastrukturen: real-time og end-to-end!



Torben Nissen Ernst
security expert
Conscia / Partner

Conscias Security Lead, Torben Nissen Ernst, giver en opdatering af trusselsbilledet, baseret på de nyeste rapporter fra Cisco og Center for Cybersikkerhed under Forsvarets Efterretningstjeneste. Han vil især fokusere på de organisatoriske og tekniske tiltag, som virksomhederne skal igangsætte for at have det nødvendige beredskab på plads, når angrebet finder sted.

Traditionel perimeterbeskyttelse kommer i stigende grad til kort overfor mere avancerede angreb. Derfor er det blevet afgørende for sikkerhedsindsatsen, at man har en robust og skalérbar infrastruktur, som ikke alene kan adressere sårbarheder men også give visibilitet, kontrol og løbende overblik over netværket end-to-end, fra det kablede og trådløse access-lag, gennem distributions- og core-infrastruktur til det moderne datacenter med virtuelle driftsmiljøer.

11:40 - 12:05: Live hacking session



Kim Elgaard
Security Specialist/Etisk Hacker
Arrow ECS Denmark A/S / Partner

Et hackerangreb består typisk af fem faser:
· Reconnaissance.
· Scanning.
· Gaining access.
· Maintaining access.
· Clearing tracks.
Men hvordan ser det reelt ud, når en hacker tiltvinger sig adgang til et system?

Kim Elgaard fortæller om hackerangrebets fem faser og demonstrerer løbende ved hjælp af forskellige værktøjer, hvordan en rigtig hacker arbejder sig vej ind i et system.

Få et sjældent kig bag hackerens skærm og hør, hvordan du bedst beskytter din virksomhed mod angreb.

12:10 - 13:00: Frokost

13:00 - 13:25: RSA: Cyber risk - The perfect storm



Jesper Sachmann
Nordic GRC Lead
RSA / Partner

'Cyber risk' er et stadigt vigtigere emne i den danske og udenlandske presse, på konferencer og som diskussionsemne i virksomhederne. 'Cyber risk' virker som en vedvarende storm som undervejs skaber usikkerhed med potentielt alvorlige konsekvenser til følge.

Antallet af emner vi skal tage stilling til er stigende og behovet for investeringer i teknologiske værktøjer er øget.

Konkrete hændelser og tiltage som ransomware og GDPR-compliance udfordrer mange virksomheder. Analyser viser, at vi er i gang med at tabe kapløbet mod de kriminelle, hackerne og aktivisterne. Tilmed skal vi opfylde diverse standarder og efterleve nye lovkrav.

Kom og hør RSA's bud på, hvordan virksomheder kan navigere i en verden, hvor cyberangreb og skærpet lovgivning er hverdagskost. Hør mere om, hvordan man bør fokusere sin cyber- og risiko-indsats ud fra det, som er væsentligt for virksomheden. Det er en tilgang, der tager udgangspunkt i vurdering af relevante risici.

Få svar på spørgsmål som:
· Hvor skal vi begynde?
· Hvilken rolle spiller topledelsen?
· Hvordan håndterer vi risiko effektivt?
· Hvordan nedbryder vi siloer når vi taler risiko?

13:30 - 14:05: Den kommende EU-dataforordning - hvad kan danske virksomheder forvente?



Martin Von Haller Grønbæk
partner
Bird & Bird / Partner

Indlægget giver et overblik til virksomhedens CTO, CIO, BizDevs og andre forretningsfolk over forordningsforslaget væsentligste dele som de ser ud nu og her.

Hvorledes påvirkes forretningen af nyheder som privacy by design, data portability og data protection officers? Hvorledes indgår "the right to be forgotten" i forordningen? Hvad sker det med samtykkekrav og cookies efter forordningen? Hvad med it-sikkerhedskrav? Og hvad er status på Safe Harbor-reglen, efter den blev skudt ned af EU-domstolen?

14:10 - 14:35: Check Point: En af tidens største trusler mod IT-sikkerhed: Ransomware



Kim Thostrup
team lead SE
Check Point Software Technologies / Partner

Ransomware angreb fortsætter med at modne både i hyppighed og intensitet, og deres indvirkning på erhvervslivet vokser eksponentielt.

Hackere har krypterede hundredtusindvis af filer, herunder fælles netværk drev, backup løsninger og ofte tager hele netværk gidsel.

De kræver løsepenge til gengæld for dekrypteringsnøgler, så du kan få adgang til dine filer.
For at kunne forhindre ransomware angreb mod din organisation, er du nødt til at forstå deres natur, hvordan de virker, og hvordan du kan opdage og stoppe dem, inden de kommer ind i jeres organisation.

14:40 - 15:00: Kaffe og kage

15:00 - 15:25: Hvordan modnes fokus på informationssikkerhed i en global virksomhed?



Peter Winkel Madsen
Manager IT Operations & Security Group IT
Bunker Holding A/S / Partner

Indlægget giver indblik i arbejdet med IT sikkerhed i en global virksomhed, og på hvordan IT sikkerhed bliver sat på dagsordenen fra den øverste ledelse og i resten af virksomheden, herunder bl.a. placering af ansvaret.

15:30 - 15:55: Det aktuelle trusselsbillede: Cyberangreb mod danske virksomheder og myndigheder



Thomas Kristmar
Afdelingschef, Policyafdelingen
Forsvarets Efterretningstjeneste, Center for Cybersikkerhed / Partner

Trusselsbilledet for Danmark og danske virksomheder har ændret sig grundlæggende i takt med, at flere konflikter udkæmpes på internettet.

Det viser de ødelæggende angreb på både virksomheder som Sony, medier som TV5 Monde og energiforsyningen som i Ukraine.

Afdelingschef Thomas Kristmar fra Center for Cybersikkerhed hos Forsvarets Efterretningstjeneste kommer derfor ind på:

· Hvad truslerne fra cyberspionage, cyberkriminelle, cyberaktivister og cyberterror bør betyde for danske virksomheders risikovurdering.
· Udbredelsen af statssponseret cyberspionage mod danske virksomheder.
· Hvordan angreb på samarbejdspartnere anvendes som del af målrettede angreb på specifikke virksomheder.
· Hvor de bløde punkter i virksomhedernes teknologi er i en tid, hvor selv firewalls kan anvendes som angrebspunkter ind i virksomheden.
· Hvorfor der er behov for et opgør med tanken om, at sikkerhed er en udfordring som kan løses med mere teknologi.

16:00 - 16:00: Tak for i dag