Cybertrusler: Få styr på it-sikkerheden – aktuelle trusler, strategi og business continuity

22. august - Centralværkstedet, Aarhus C

08:30 - 08:55	**Morgenmad & Registrering**
08:55 - 09:00	**Velkomst** Jakob Schjoldager, redaktør, Computerworld
09:00 - 09:40	**Det aktuelle trusselsbillede** Jan Kaastrup, CTO & Partner, CSIS
09:45 - 10:10	**Fortinet gør op med de tre vise aber "ikke høre, ikke se, ikke tale" i it-sikkerhed** Tommy Pedersen, security engineer, Fortinet
10:15 - 10:45	**Pause**
10:45 - 11:10	**Gør dine end-points til din første forsvarslinje mod cyberkriminalitet** Howard Roberts, Distinguished Technologist, HP
11:15 - 11:40	**Luk af for hackerne i tide** Mikkel Bjørklund, GDPR and Data Quality consultant, Tabellae A/S
11:45 - 12:45	**Frokost**
12:45 - 13:10	**Sådan bliver du mere modstandsdygtig i skyen** Niels Frederiksen, Senior Sales Engineer, Mimecast
13:15 - 13:40	**Cyber incidents? Not on my watch** Philippe Motet Jessen, it-sikkerhedsrådgiver med speciale i awareness, behavior og compliance
13:45 - 14:10	**Multiple clouds - kontrol og compliance** Balder Caspersen Borup, Channel Security Engineer and Cloud SME, Check Point Software
14:15 - 14:35	**Pause**
14:35 - 15:00	**Holder dine beredskabsplaner? Og hvad skal der være i en krisekuffert?** Ken Bonefeld Nielsen, Senior Cyber Security & Resilience Advisor, Norlys
15:05 - 15:45	**"Krigshistorier" fra en travl hverdag** Peter Winkel Madsen, Manager IT Operations & Security Group IT, Bunker Holding A/S
15:45 - 15:45	**Tak for i dag**

08:30 - 08:55: Morgenmad & Registrering

08:55 - 09:00: Velkomst

Jakob Schjoldager
redaktør
Computerworld

09:00 - 09:40: Det aktuelle trusselsbillede

Jan Kaastrup
CTO & Partner
CSIS / Keynote

Hør om de største og mest aktuelle cybertrusler i en tid, hvor trusselsbilledet hele tiden ændrer sig i takt med, at hackerne finder nye veje og metoder.

09:45 - 10:10: Fortinet gør op med de tre vise aber "ikke høre, ikke se, ikke tale" i it-sikkerhed

Tommy Pedersen
security engineer
Fortinet / Partner

Aberne er løs! Velkommen til vores kvartalsmæssige løb gennem det vilde og skøre cyber-trusselslandskab. Q2 viste mange temaer og tendenser, som vi har set før, og vores research-team stødte også på masser af nye og bemærkelsesværdige udviklinger.

FortiGuard har netop offentliggjort "Q2 2019 Quarterly Threat Landscape Report". Vi ser på de trends, som vi har set det seneste kvartal, og på de muligheder, somFortinet fabric giver for at beskytte din virksomhed og organisation overfor disse trusler.

Slut med at lukke øjne, ører og mund – Nu skal der tages fat.

10:15 - 10:45: Pause

10:45 - 11:10: Gør dine end-points til din første forsvarslinje mod cyberkriminalitet

Howard Roberts
Distinguished Technologist
HP / Partner

End-points er i stigende grad mål for it kriminelle, der udnytter sårbarheder til at trænge dybere ind i organisationen.

Med en proaktiv strategi kan du omdanne sårbare enheder til at blive din første forsvarslinje.

Indlægget afholdes på engelsk.

11:15 - 11:40: Luk af for hackerne i tide

Mikkel Bjørklund
GDPR and Data Quality consultant
Tabellae A/S / Partner

Gennem mange år har selskabers it-sikkerhed bestået af løsninger, som blokerer eller filtrerer trusler. Desværre er det ikke nok.

De trusler, der nu rammer alle virksomheder, er så avancerede, at de går igennem selv de bedste firewalls. Det er vigtigt at være forberedt, når hackerne kommer igennem. Med Kill-Switch™ i din infrastruktur kan du hurtigt og sikkert lukke ned for de enkelte systemer eller spærre vejen for hackerne, så de ikke får adgang til hele virksomheden. Hør mere om, hvordan Kill-Switch™ isolerer truslen på få minutter og sikrer, at den ikke spreder sig til hele virksomheden. Og få en bedre forståelse af, hvad Kill-Switch™ kan gøre for dig.

11:45 - 12:45: Frokost

12:45 - 13:10: Sådan bliver du mere modstandsdygtig i skyen

Niels Frederiksen
Senior Sales Engineer
Mimecast / Partner

Petya, WannaCry og andre former for farlig malware har i de senere år været et wake-up call i mange organisationer, der tidligere mente, at deres it-sikkerhed var god og rigelig.

Det viste angrebene ikke var tilfældet. Efter dem stod det klart, at mange organisationers avancerede it-sikkerheds setup og deres procedurer for business continuity og backup ikke fungerede ordentligt.

Det store spørgsmål efter angrebene er, hvordan organisationer kan forsvare sig selv, når e-mail er hovedangrebs-målet for hackerne.

I dette indlæg kigger vi på fællesnævnerne i rækken af succesfulde angreb og på, hvorfor organisationer bliver nødt til at ændre deres fokus fra 'cybersikkerhed' til 'cyber-modstandsdygtighed' for at være i stand til at beskytte sig selv effektivt.

13:15 - 13:40: Cyber incidents? Not on my watch

Philippe Motet Jessen
it-sikkerhedsrådgiver med speciale i awareness, behavior og compliance / Keynote

Styrk sikkerhedskulturen i virksomheden og reducer risikoen for interne databrud og cyberangreb.

Medarbejderne betragtes ofte som virksomhedens svage led, når det handler om informationssikkerhed.

Så hvordan skaber du en kultur, hvor informationssikkerhed bliver lige så naturlig som at spænde sikkerhedsselen i bilen?

I dette oplæg får du et indblik i de ting, som du med fordel kan gøre for at styrke sikkerhedskulturen.

Vi kombinerer de bedste pointer fra adfærdskommunikation og forandringsteori og krydrer det med konkrete eksempler på tiltag, der får medarbejderne til at droppe dårlige vaner til fordel for gode - og sikre - vaner.

13:45 - 14:10: Multiple clouds - kontrol og compliance

Balder Caspersen Borup
Channel Security Engineer and Cloud SME
Check Point Software / Partner

Det er nemt at tage hul på overgangen mod public cloud, og de fleste har i første omgang ofte en oplevelse af, at deres it-håndtering bliver nemmere og mere overskuelig, når de rykker over i public cloud.
Det er imidlertid meget nemt at miste både kontrollen og overblikket i takt med, at der bliver flyttet flere og flere applikationer over i skyen.

Her er det bydende nødvendigt at sikre sig fuld indsigt på tværs af de ofte flere public cloud-miljøer, som man kommer til at anvende.

For kun med fuld indsigt og med fuld kontrol over alle it-sikkerhedsmæssige konfigurationer på tværs af alle konti, alle virtuelle netværk og regioner i både AWS, Azure og Google Cloud kan man sikre sig, at man er beskyttet mod sårbarheder, identitets-tyveri og datatab i skyen.

Kom og hør, hvordan Check Point kan sikre flere cloud-miljøer og samtidig give dig ny og dybere indsigt i selv komplekse cloud-miljøer.

Du kan også høre om Check Points opkøb af Dome9, der er det nyeste medlem af Check Point Cloud Guard-familien.

14:15 - 14:35: Pause

14:35 - 15:00: Holder dine beredskabsplaner? Og hvad skal der være i en krisekuffert?

Ken Bonefeld Nielsen
Senior Cyber Security & Resilience Advisor
Norlys / Keynote

Ken Bonefeld Nielsen tager aktuelle cybertrusler op og kigger på værdien af de tiltag, der er i gang på forskellige indsatsområder. Prioriterer og investerer vi rigtigt?

Mange virksomheder vil kunne undgå mange af de faldgruber, som man ofte ryger i, når den uventede hændelse indtræffer. Det kræver dog visse kvalificerede forberedelser og en evne til at bevare overblikket, når det virkeligt gælder.

Ken giver et nyt friskt syn på, hvordan du og din organisation kan forbedre jeres eksisterende beredskabsplaner - og tager et kig på, hvad der egentligt skal være i en krisekuffert.

15:05 - 15:45: "Krigshistorier" fra en travl hverdag

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

Bunker Holding, som er en af Danmarks største virksomheder målt på omsætningen, tikker medarbejder antaller derop ad med 10 nyansatte og en ny lokation ude i verden næsten hver måned. En vækst, som de p.t. 36 danske it-folk skal håndtere, både i en operationel og en sikkerheds kontekst. Hvordan de gør dette, fortæller Bunker Holdings IT operations- og sikkerhedsansvarlige, Peter Winkel Madsen.

Indlægget kommer til at sprede sig over traditionel sikkerhed, cloud sikkerhed, red teaming og user awareness krydret med "krigshistorier" fra en travl hverdag.

15:45 - 15:45: Tak for i dag