Cyber Threats 2024: Sådan arbejder de IT-kriminelle – og sådan beskytter du dig

20. marts - Charlottehaven, København Ø

08:30 - 09:00	**Registrering og morgenmad**
09:00 - 09:05	**Velkomst** Qëndrim Fazliu, samfundsredaktør, Computerworld
09:05 - 09:35	**Trusselsbilledet i Danmark og hvor cyber crime bevæger sig hen** Lars Mortensen, Centerchef/politiinspektør, Nationalt Cyber Crime Center (NC3) der er en del af National enhed for Særlig Kriminalitet (NSK) Henriette Erbs, Afdelingsleder for Teknologi og Projekter i Nationalt Cyber Crime Center (NC3), National enhed for Særlig Kriminalitet (NSK)
09:35 - 10:00	**Sådan kommer du dig over et cyberangreb - hurtigt og billigt!** Martin Plesner-Jacobsen, Senior System Engineer, Veeam Software
10:05 - 10:30	**Zero-Day Sårbarheder 2024: Trusselslandskabet og Strategier til Beskyttelse"** Christian Rutrecht, Director, System Engineering, Fortinet Thomas Raabo, Director of Network Services, NetNordic
10:30 - 10:50	**Pause**
10:50 - 11:15	**Forsvar dig mod AI genererede phishing-e-mails** Ariel Merzer, Email Security Engineers EMEA & APAC, Check Point Software Technologies Ltd
11:20 - 11:45	**Det er tid til at overveje menneskelig threat hunting - at finde nålen i høstakken** Jonas Gyllenhammar, Senior Systems Engineer, Sophos
11:45 - 12:00	**Pause**
12:00 - 12:25	**Cyberhygiejne – Hvad virker bedst i det fundamentale Cyberforsvar?** Christian Schmidt, Direktør, Dediko A/S
12:25 - 13:10	**Frokost**
13:10 - 13:40	**Hvorfor supply chain vil være årets største emne inden for cybersikkerhed** Jan Lemnitzer, Assistant Professor at the Department of Digitalization, Copenhagen Business School
13:40 - 14:05	**Ustruktureret data er en "liablity" hvis man ikke får ryddet op** Dan Thomsen, Partner, Data & More
14:05 - 14:25	**Pause**
14:25 - 14:55	**Gen Z'erne indtager arbejdsmarkedet, og det kan udfordre cybersikkerheden** Claus Holm, landechef, Samsung, Danmark
14:55 - 14:55	**Opsummering og tak for idag** Qëndrim Fazliu, samfundsredaktør, Computerworld

08:30 - 09:00: Registrering og morgenmad

09:00 - 09:05: Velkomst

Qëndrim Fazliu
samfundsredaktør
Computerworld

09:05 - 09:35: Trusselsbilledet i Danmark og hvor cyber crime bevæger sig hen

Lars Mortensen
Centerchef/politiinspektør
Nationalt Cyber Crime Center (NC3) der er en del af National enhed for Særlig Kriminalitet (NSK) / Keynote

Henriette Erbs
Afdelingsleder for Teknologi og Projekter i Nationalt Cyber Crime Center (NC3)
National enhed for Særlig Kriminalitet (NSK) / Keynote

09:35 - 10:00: Sådan kommer du dig over et cyberangreb - hurtigt og billigt!

Martin Plesner-Jacobsen
Senior System Engineer
Veeam Software / Partner

Når du tager backup med Veeam, kan hackerne bare komme an!

På 30 minutter fortæller Martin Plesner-Jacobsen, hvorfor Veeam Backup & Recovery giver dig nattero - og it-kriminelle mareridt.

Lyt med og bliv blandt andet blive klogere på, hvordan du kan sikre, at du kan genskabe data efter et angreb med ransomware – hurtigt og billigt.

10:05 - 10:30: Zero-Day Sårbarheder 2024: Trusselslandskabet og Strategier til Beskyttelse"

Christian Rutrecht
Director, System Engineering
Fortinet / Partner

Thomas Raabo
Director of Network Services
NetNordic / Partner

I 2023 så vi en stigning i antallet af sårbarheder og Zero Days og tendensen er fortsat i 2024. Især internet eksponerede services som VPN, fjernadgang og VDI platforme er et yndet mål for de cyberkriminelle. I denne talk vil vi derfor give et overblik over aktuelle Zero Days og hvordan trusselsaktørerne anvender dem i praksis.

Herefter følger vi op med nogle konkrete løsningsforslag og use cases til hvordan vi kan arbejde uden om risikoen ved Zero days sårbarheder ved hjælp af Zero Trust.

***Hvad er en zero-day sårbarhed?** Forestil dig et hul i din softwaresikkerhed. Et hul, som softwareudvikleren ikke kender til. Hackere kan udnytte disse huller til at snige sig ind i dine systemer og stjæle dine data, før der er en patch tilgængelig.*

***Hvorfor er "Patch in time" vigtigt?** At installere sikkerhedsopdateringer ("patches") hurtigst muligt er som at smække døren i for næsen af ubudne gæster. Jo hurtigere du reagerer, jo mindre sandsynligt er det, at de får adgang til dine data.*

***Risikoen ved eksponerede services og applikationer:** Når dine services og applikationer er tilgængelige på internettet, er de som et åbent hus for hackere. De kan udnytte sårbarheder til at stjæle data, forstyrre driften eller bare forårsage generelt kaos.*

***Sikkerhed skal følge klienten:** Uanset hvor dine klienter befinder sig, skal de have adgang til sikker og pålidelig infrastruktur. Det er som at have en livvagt, der følger dem overalt. I forbindelse med en arkitektur hvor brugere sikkert via zero trust tilgår services og applikationer, så er det ofte overset at man samtidig også kan løse zero day & sårbarheds problematikker.*

10:30 - 10:50: Pause

10:50 - 11:15: Forsvar dig mod AI genererede phishing-e-mails

Ariel Merzer
Email Security Engineers EMEA & APAC
Check Point Software Technologies Ltd / Partner

År efter år er vi vidne til et stigende antal cyberangreb, der stammer fra ondsindede eller phishing-e-mails. Generative AI gør det nu også muligt for hackere at udforme phishing-e-mails, der ligner legitim korrespondance med korrekt sprogbrug.

Derfor dykker vi i dette indlæg ned i de seneste phishing-angreb og hvorfor reaktive sikkerhedsløsninger efterlader dig sårbar og hvorfor det er nødvendigt at prioritere forebyggelse og beskytte cloud-baserede e-mails og andre samarbejdsplatforme mod malware, phishing og relaterede trusler.

Vi viser dig derefter en løsning, som ikke kun nem at implementere og bruge, men som også problemfrit integrerer med andre sikkerhedsværktøjer i organisationen. Ved at udnytte Threat Emulation og avanceret maskinlæring kan du nemlig opretholde en uovertruffen detektionskvalitet.

Indlægget afholdes på engelsk

11:20 - 11:45: Det er tid til at overveje menneskelig threat hunting - at finde nålen i høstakken

Jonas Gyllenhammar
Senior Systems Engineer
Sophos / Partner

Cybersikkerhed er blevet for kompleks for de fleste organisationer at håndtere effektivt, og aktive trusler er blevet almindelige.
Teknologi alene er derfor ikke nok, så på dette indlæg kan du få indsigt i, hvordan trusselslandskabet har udviklet sig, og hvad du kan gøre for at beskytte din organisation.

11:45 - 12:00: Pause

12:00 - 12:25: Cyberhygiejne – Hvad virker bedst i det fundamentale Cyberforsvar?

Christian Schmidt
Direktør
Dediko A/S / Partner

Robustheden i dit cyberforsvar er summen af alle dine individuelle tiltag.
Men i en situation, hvor manglen på fuldtids cybermedarbejdere, ægte ledelsesforankring kombineret med en udvikling i cybertruslen via AI er det ekstremt vigtigt at prioritere er spørgsmålet:

Hvad skal der til i praksis for at opbygge et effektivt Cyberforsvar?

I dette indlæg får du derfor et bud på cyberforsvarets grundkomponenter, samt en "Cybersnack", som du kan bruge til at måle modenheden af dit cyberforsvar:

1. Hvordan opnår du ægte ledelsesforankring og tilstrækkelige ressourcer / budget?
2. Hvad er grundpillerne i cyberhygiejne?
3. Hvordan måler du effektiviteten i din cybersikkerhed?
4. Hvor kommunikerer du cybersikkerheden til ledelsen og omverdenen?
5. Hvad er de største trusler mod en effektiv cybersikkerhed?

12:25 - 13:10: Frokost

13:10 - 13:40: Hvorfor supply chain vil være årets største emne inden for cybersikkerhed

Jan Lemnitzer
Assistant Professor at the Department of Digitalization
Copenhagen Business School / Keynote

Cyberkriminelle angriber i stigende grad supply chains for at finde den svageste forbindelse ind i en virksomheds netværk, mens avancerede statslige hackere har manipuleret udbredt software for at inficere alle klientvirksomheder på én gang.

EU har nu reageret ved at inkludere nye krav om overvågning og håndtering af cybersikkerhedsrisici i forsyningskæden for virksomheder omfattet af den nye NIS2-regulering, der beskytter kritisk infrastruktur.

Dette betyder, at NIS2 ikke kun vil påvirke virksomheder direkte omfattet af direktivet, men også indebærer øget kontrol med cybersikkerhedsstandarderne for virksomheder, der er underleverandører til disse virksomheder.

I dette indlæg vil Jan derfor give indsigt i, hvorfor cybersikkerhed i supply chainen er så vanskelig at skalerer, hvilke nye krav danske virksomheder sandsynligvis vil stå over for fra deres større kunder, og hvordan de kan forberede sig.

Indlægget afholdes på engelsk

13:40 - 14:05: Ustruktureret data er en "liablity" hvis man ikke får ryddet op

Dan Thomsen
Partner
Data & More / Partner

Vi dykker ned i, hvorfor ustruktureret data er et problem for alle virksomheder og organisationer.
I dette indlæg viser vi derfor, hvordan du finder ud af hvor slemt det står til, og hvordan du hurtigt og enkelt kan få ryddet op dine i ustrukuterede data.

14:05 - 14:25: Pause

14:25 - 14:55: Gen Z'erne indtager arbejdsmarkedet, og det kan udfordre cybersikkerheden

Claus Holm
landechef
Samsung, Danmark / Partner

Det kan blive en farlig cybercocktail, når gen z'erne begiver sig ud på danske arbejdspladser uden at tage sikkerhedstruslen alvorligt. Derfor skal kommende arbejdsgivere have fokus på uddannelse i øjenhøjde.

14:55 - 14:55: Opsummering og tak for idag

Qëndrim Fazliu
samfundsredaktør
Computerworld