Digital konference: It-sikkerhed 2020 - Trusler, tendenser og strategi

28. august - Online, Online

08:30 - 09:00	**De digitale døre åbner - login og tjek lyd og billede**
09:00 - 09:05	**Velkomst** Jakob Schjoldager, redaktør, Computerworld
09:05 - 09:30	**Keynote** Jan Kaastrup, CTO & Partner, CSIS
09:30 - 09:50	**Det bedste forsvar begynder med en struktureret analyse** Christian Schmidt, Direktør, Dediko A/S
09:50 - 10:10	***Ændring af cyberlandskaber: Slaget om algoritmer*** Marley Hasselbach, Senior Commercial Manager, Darktrace
10:10 - 10:25	**Keynote interview - Erfaringer om at komme succesfuldt gennem et hackerangreb** Carsten Bryder, COO, GlobalConnect
10:25 - 10:45	**Gone phishing** Teemu Myllykangas, Director, B2B Product Management, F-Secure
10:45 - 11:05	**A Quick Guide to Ensuring a Productive Remote Workforce** Joseph Carson, Chief Information Security Scientist & Advisory CISO, Thycotic
11:05 - 11:15	**Pause**
11:15 - 11:35	**Keynote Interview - de vigtigste sikkerhedsværktøjer** Morten Steiner, CIO, PFA Pension
11:35 - 11:55	**Sådan beskytter AI dit netværk mod fremtidens cyber-angreb** Andreas Wehowsky, CEO, Wehowsky.com
11:55 - 12:15	**Sikkerhed – fra omkostning til forretningsværdi** Nikolaj Andersen Wølck, Sikkerhedsarkitekt og Tech Chat redaktør, Conscia Kristian Balle, Key Account Manager, Conscia
12:15 - 12:15	**Tak for i dag**

08:30 - 09:00: De digitale døre åbner - login og tjek lyd og billede

09:00 - 09:05: Velkomst

Jakob Schjoldager
redaktør
Computerworld

09:05 - 09:30: Keynote

Jan Kaastrup
CTO & Partner
CSIS / Keynote

09:30 - 09:50: Det bedste forsvar begynder med en struktureret analyse

Christian Schmidt
Direktør
Dediko A/S / Partner

Antallet af cyberangreb i Danmark er stigende, og flere undersøgelse peger på, at mere end halvdelen af alle danske virksomheder bliver ramt af et cyberangreb i en eller anden form. Det et således ikke et spørgsmål OM, men HVORNÅR din virksomhed bliver ramt af et angreb.

Kan du nedsætte denne risiko til et acceptabelt niveau, og hvordan måler du, om organisationen har nået dette niveau? Kan du på forhånd mindske konsekvenserne af et angreb uden at gå på kompromis med produktivitet og virksomhedskultur. Hvordan sikrer du en effektiv kommunikation mellem ledelsen, it-afdelingen, HR og resten af organisationen?

Ved at bruge vores modenhedsmodeller og analysemetode, der bygger på CIS20, ved du altid, hvor skoen trykker, og hvad du skal gøre for at nå det accepterede niveau af risiko. Metoden gør det nemmere at kommunikere it-sikkerhed til både ledelse, it og organisation, så ejerskabet af den accepterede risiko forankres korrekt. Analysen gennemføres på under en uge, og du får en pragmatisk og let forståelig handlingsplan at agere på.

09:50 - 10:10: Ændring af cyberlandskaber: Slaget om algoritmer

Marley Hasselbach
Senior Commercial Manager
Darktrace / Partner

Blandt hurtigt udviklende teknologiske fremskridt gør fremkomsten af AI-forbedret malware cyberangreb eksponentielt mere farlige og sværere at identificere. I den nærmeste fremtid vil vi begynde at se superladede, AI-drevne cyberangreb blive udnyttet i større skala. For at beskytte sig mod de offensive AI-angreb vender organisationer sig i stigende grad mod defensiv cyber AI, der kan identificere og neutralisere de nye og ondsindede aktiviteter, uanset hvornår eller hvor de slår til.

På dette indlæg kan du lære om:
· Paradigmeskift i cyberlandskabet
· Fremskridt inden for offensive AI-angrebsteknikker
· Immunsystemtilgangen til cybersikkerhed og defensive, autonome responsfunktioner
· Eksempler fra virkelighedens verden på nye trusler, der blev stoppet med cyber AI

Indlægget foregår på engelsk

10:10 - 10:25: Keynote interview - Erfaringer om at komme succesfuldt gennem et hackerangreb

Carsten Bryder
COO
GlobalConnect / Partner

Carsten Bryder fra GlobalConnect giver os et indblik i, hvordan det er at blive angrebet af hackere og hvordan man kommer igennem det.

10:25 - 10:45: Gone phishing

Teemu Myllykangas
Director, B2B Product Management
F-Secure / Partner

E-mail er og bliver angrebsmetode #1 i verden. Den modi operandi, som benyttes af angriberne, ændrer sig dog med cloudification af e-mail-tjenester, hvilket nødvendiggør en ny tilgang på det gamle problem det er, at beskytte e-mail-trafik.

Under præsentationen får deltagerne indsigt i nye e-mail-baserede angrebsmetodologier - specifikt i forbindelse med cloud-baserede e-mail-tjenester samt de handlinger og værktøjer, som de har brug for, hvis de skal beskytte sig mod disse nye trusler.

Indlægget afholdes på engelsk.

10:45 - 11:05: A Quick Guide to Ensuring a Productive Remote Workforce

Joseph Carson
Chief Information Security Scientist & Advisory CISO
Thycotic / Partner

The world is accelerating a shift to the largest remote workforce ever and IT teams have been forced to accelerate cyber security projects to aid this mass digital transformation. A well-executed transition will make working from home possible and maintain security, and it will do so within the limitations of your organization's existing infrastructure.

CISOs and IT security professionals must address important questions to reduce the risks exposed by this transition.

Join Joseph Carson and get the answers to these important questions:
· What data is on my systems and will it still comply with compliance and regulations if employees leave the office and work remotely?
· Does it matter if my users are local administrators
· How can I sustain a business as usual approach and maintain security?
· Will a Zero Trust strategy work?

11:05 - 11:15: Pause

11:15 - 11:35: Keynote Interview - de vigtigste sikkerhedsværktøjer

Morten Steiner
CIO
PFA Pension / Partner

Morten Steiner fra PFA giver os et indblik i sine erfaringer med sikkerhedsværktøjer og foranstaltniner.

11:35 - 11:55: Sådan beskytter AI dit netværk mod fremtidens cyber-angreb

Andreas Wehowsky
CEO
Wehowsky.com / Partner

Hvordan ser fremtidens cyber-angreb ud? Eksperter forventer, at maskiner og kunstig intelligens udgør fremtidens trusler. Det kræver et nyt cyberberedskab, der også anvender maskinlæring og kunstig intelligens.

Traditionelle, regelbaserede værktøjer kan ikke hamle op med fremtidens angreb, og det har vi set flere eksempler på i Danmark. Præsentationen stiller skarpt på de seneste udviklinger inden for kunstig intelligens og cyber-sikkerhed.

Du får et indblik i, hvordan MUNINN anvender kunstig intelligens til at opdage og blokere cybertrusler, der undslipper firewall og endpoint-løsninger, eksempelvis 0 day-angreb, ransomware og interne trusler/spionage.

11:55 - 12:15: Sikkerhed – fra omkostning til forretningsværdi

Nikolaj Andersen Wølck
Sikkerhedsarkitekt og Tech Chat redaktør
Conscia / Partner

Kristian Balle
Key Account Manager
Conscia / Partner

Sikkerhed efterspørges som aldrig før. Virksomheders omdømme kan lide store tab ved sikkerhedsangreb, og den nedetid, der typisk følger med, kan betyde store omkostninger. Selv om virksomheder i mange år har investeret kraftigt i it-sikkerhed er det vigtigt at overveje, om værdien automatisk følger produktet.

Hør mere om, hvordan Conscia kombinerer indsigt i teknologi med solidt forretningskendskab og gode servicemuligheder. Vores erfaring viser, at moderne malware udvikler sig som aldrig før. Kun ved at kombinere de smarte produkter med specialistviden opnås den fulde værdi.

Vi tager en kundevinkel på sikkerhed og dykker ned i, hvordan sikkerhedsprodukter, der overvåges og får den nødvendige opmærksomhed, giver den værdi og det resultat, som virksomhederne efterspørger.

12:15 - 12:15: Tak for i dag