IAM - din genvej til højere sikkerhed uden uautoriseret adgang og datatab

18. april - HUONE Copenhagen, Kastrup

08:30 - 09:00	**Registrering og morgenmad**
09:00 - 09:05	**Velkomst** Qëndrim Fazliu, Samfundsredaktør og moderator, Computerworld
09:05 - 09:35	**Hvordan sikrer man, at de rette medarbejdere har adgang til de rette ressourcer på det rette tidspunkt samtidig med at man overholder alle lovmæssige krav og sikkerhedsstandarder?** Maja C.P. Andersen, Director for Global Identity & Access Management, DSV
09:35 - 10:00	**Skiftet til identitetscentreret sikkerhed - et kig indefra på trusler, der ændrer sig** Mandeep Sandhu, Solutions Engineering Manager and Investigator, EMEA, SpyCloud Ian Greenwood, Regional Sales Director, SpyCloud
10:00 - 10:20	**Pause**
10:20 - 10:45	**Highlights fra Gartner IAM Summit i London** Tommy Petersen, Director IAM, Columbus
10:50 - 11:15	**'MODERN IDENTITY' gør op med digital sårbarhed, så ingen bliver efterladt på den digitale perron.** Vinay Dabas, Senior Solutions Architect, Ping Identity
11:15 - 11:30	**Pause**
11:30 - 11:55	**Netwrix, ITDR & IGA som virker for dig** Hazem Taouai, PreSales Engineer for Netwrix Usercube, Netwrix
12:00 - 12:25	**Løsning af de sikkerhedsmæssige blinde pletter ved MFA-dækning og beskyttelse af servicekonti** Lars Gotlieb, Regional Sales Manager – Nordics, Silverfort Kev Smith, Principal Sales Engineer EMEA, Silverfort
12:25 - 13:20	**Frokost**
13:20 - 13:45	**Innovation i IGA, der sikrer større værdi og afkast for din fortsatte IGA-investering** Anna Nordström, Senior Product Manager, Omada Identity
13:50 - 14:15	**Privileged Access Management (PAM) vs. Identity Access Management (IAM), og hvorfor du har brug for begge dele** João Fiuza de Alencastro, Sales Engineer, senhasegura
14:15 - 14:30	**Pause**
14:30 - 14:55	**Gevinstrealisering i IAM-projekter – når driften overtrumfer mulighederne** Jens Nielsen, Principal Consultant, Columbus
15:00 - 15:30	**Sådan sikrer Postnord sig internt med IAM** Monika Harmiz, IAM Specialist, PostNord Group

15:30 - 15:35 **Opsummering**
Qëndrim Fazliu, Samfundsredaktør og moderator, Computerworld

15:35 - 15:35 **Tak for i dag**

08:30 - 09:00: Registrering og morgenmad

09:00 - 09:05: Velkomst



Qëndrim Fazliu
Samfundsredaktør og moderator
Computerworld

09:05 - 09:35: Hvordan sikrer man, at de rette medarbejdere har adgang til de rette ressourcer på det rette tidspunkt samtidig med at man overholder alle lovmæssige krav og sikkerhedsstandarder?



Maja C.P. Andersen
Director for Global Identity & Access Management
DSV / Keynote

I vores moderne digitale miljø er spredningen af enheder, brugere og data på tværs af forskellige platforme en betydelig udfordring for IT-sikkerheden. "Identity Governance and Administration" (IGA) refererer til praksis og teknologier, der effektivt styrer brugeridentiteter og deres adgang til systemer og data. Implementering af IGA sikrer ikke blot øget sikkerhed, men også en mere effektiv og standardiseret drift. Det reducerer tiden og ressourcerne brugt på at integrere og afskedige medarbejdere, det øger gennemsigtigheden og sikkerheden i sporbarhed og det beskytter mod cybertrusler og databrud. Og det er noget, som Maja Andersen ved en masse om.

09:35 - 10:00: Skiftet til identitetscentreret sikkerhed - et kig indefra på trusler, der ændrer sig



Mandeep Sandhu
Solutions Engineering Manager and Investigator, EMEA
SpyCloud / Partner



Ian Greenwood
Regional Sales Director
SpyCloud / Partner

Den kriminelle undergrund boomer, og cyberkriminalitet vokser med en eksponentiel hastighed. Denne ekstreme vækst i cyberkriminalitet kræver, at organisationer tager en ny, identitetscentreret tilgang til at beskytte deres medarbejderes og kunders identitet.

Identity-first-sikkerhed fokuserer på at beskytte brugernes identitet og de data, der er knyttet til dem, uanset placering og enhed. Men uden løbende validering af, at privilegerede brugeres identiteter ikke afsløres, lader du dine organisationer stå åbne over for sårbarheder og dræner dit sikkerhedsteams ressourcer. Under denne session vil SpyCloud demonstrere, hvordan cyberkriminelle tilpasser taktik for at omgå forskellige sikkerhedsforanstaltninger, såsom MFA, og hvordan du kan integrere de mest nøjagtige og seneste cyberkriminalitetsdata i eksisterende arbejdsgange og automatisere afhjælpning for at frigøre teamressourcer.

10:00 - 10:20: Pause

10:20 - 10:45: Highlights fra Gartner IAM Summit i London



Tommy Petersen
Director IAM
Columbus / Partner

Hvad rører sig på IAM-scenen lige nu, og hvordan ser fremtiden ud for Identity Security? Tommy Petersen har samlet sine highlights fra det seneste Gartner IAM Summit, som foregik i London i starten af marts. Få dugfriske tips til, hvad I bør have fokus på i jeres IAM-strategi på den korte og lange bane.

10:50 - 11:15: 'MODERN IDENTITY' gør op med digital sårbarhed, så ingen bliver efterladt på den digitale perron.



Vinay Dabas
Senior Solutions Architect
Ping Identity / Partner

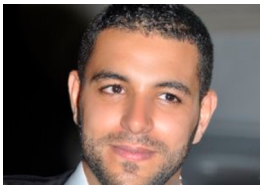
Vores digitale verden er et spejl af vores fysiske virkelighed. Men mens vi i mange år har gjort en indsats for at tilpasse samfundets faciliteter til fysisk handicappede, ser det ud til, at vi har glemt dem, der føler sig sårbare og udfordret i den digitale transformation.

Størrelsen på skrifttypen er ikke længere tilstrækkelig, og vi indfører rask væk nye tekniske sikkerhedskontroller uden at tage hensyn til dem, der ikke bevæger sig så hurtigt digitalt. Vi går ud fra, at alle har en smartphone og kan navigere gennem den skov af spørgsmål, de bliver mødt med, når de venter på at komme igennem til en kundeservicemedarbejder. Digital sårbarhed kan ramme os alle sammen og kommer til udtryk i mange former. Vi synes at have glemt, at – ligesom i den virkelige verden – så har vi mennesker brug for hinandens hjælp.

I denne præsentation undersøger vi, hvordan vi kan integrere inklusion og medfølelse i vores cyber-drevne identitetsprogrammer, hvor sikkerhed og tilgængelighed er afstemt til dem, der er digitalt udfordrede. Fremtidens inkluderende sikkerhed foregår på alle kanaler, er forbundet og kan tilpasse sig den enkelte bruger.

11:15 - 11:30: Pause

11:30 - 11:55: Netwrix, ITDR & IGA som virker for dig



Hazem Taouai
PreSales Engineer for Netwrix Usercube
Netwrix / Partner

84% af alle organisationer har været udsat for identitetsbrud i det seneste år. I disse angreb antager trusselsaktører identiteten af en legitim bruger for at kompromittere systemer, bevæge sig lateralt i netværk og opnå højere adgangsniveauer. Men disse trusler er svære at opdage, fordi traditionelle værktøjer mangler evnen til at skelne mellem en legitim bruger og en ondsindet aktør. Derfor, for at beskytte deres følsomme data og missionskritiske systemer, har organisationer brug for en omfattende Identity Threat Detection and Response (ITDR) tilgang, som med IGA er den bedste måde at opdage og reagere på identitetstrusler.

12:00 - 12:25: Løsning af de sikkerhedsmæssige blinde pletter ved MFA-dækning og beskyttelse af servicekonti



Lars Gotlieb
Regional Sales Manager – Nordics
Silverfort / Partner



Kev Smith
Principal Sales Engineer EMEA
Silverfort / Partner

I dagens verden er identitetstrusler en betydelig udfordring for organisationer. Multifaktorautentificering (MFA) har vist sig at være en vigtig sikkerhedsforanstaltning til at beskytte mod identitetstrusler.

Men der er stadig kritiske blinde vinkler i MFA og beskyttelsen af servicekonti, som kan udnyttes af angribere.

I denne session vil vi udforske disse blinde vinkler og diskutere, hvordan Silverforts Unified Identity Protection-platform adresserer dem. Denne platform udvider MFA til alle ressourcer, herunder ældre apps, kommandolinjeadgang, fildeling og andre kritiske ressourcer, som tidligere var svære at sikre.

Vi vil også vise, hvordan Silverfort automatiserer opdagelse, overvågning og beskyttelse af servicekonti, som ofte overses, men som kan udgøre betydelige sikkerhedsrisici, hvis de ikke sikres.

12:25 - 13:20: Frokost

13:20 - 13:45: Innovation i IGA, der sikrer større værdi og afkast for din fortsatte IGA-investering



Anna Nordström
Senior Product Manager
Omada Identity / Partner

I denne session vil Anna Nordström dele koncepter, der vil hjælpe dig med overgangen til mere moderne IGA-kapaciteter, som er nødvendige for at være på forkant med de stigende krav fra din organisation.

13:50 - 14:15: Privileged Access Management (PAM) vs. Identity Access Management (IAM), og hvorfor du har brug for begge dele



João Fiuza de Alencastro
Sales Engineer
senhasegura / Partner

Identity Access Management (IAM) og Privileged Access Management (PAM) er to kritiske komponenter i cybersikkerhed. Hvad er forskellen mellem PAM og IAM, og hvorfor har du brug for begge løsninger?

IAM bruges i hele organisationen til at sikre en bred vifte af brugere og enheder med fokus på at identificere, verificere og give adgang for at forhindre uautoriseret adgang. Den håndterer generel brugeridentifikation og bred netværkssikkerhedsstyring.

PAM gør det også. PAM administrerer specifikke brugere og systemer, der har brug for øget adgang til følsomme opgaver, med fokus på at sikre meget følsomme systemer og kritiske data. Det overvåger og kontrollerer brugeraktiviteter ved at anvende avancerede sikkerhedsmetoder til at mindske risici og administrere adgang til afgørende ressourcer.

OBS: Indlægget afholdes på engelsk

14:15 - 14:30: Pause

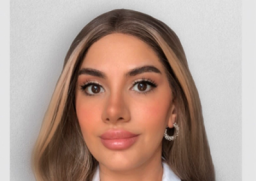
14:30 - 14:55: Gevinstrealisering i IAM-projekter – når driften overtrumfer mulighederne



Jens Nielsen
Principal Consultant
Columbus / Partner

IAM projekter har ofte deres afsæt i en specifik udfordring, som projektet skal hjælpe til at løse. Imidlertid kan IAM ofte levere gevinster på en lang række områder, som hurtigt kan overses ved at betragte IAM som et vanligt IT-projekt. Ved at involvere de rigtige belutningstagere, prioritere de forventede forretningsgevinster og kontinuerligt synliggøre fremdriften får IAM projektet de bedste muligheder for at blive en succes.

15:00 - 15:30: Sådan sikrer Postnord sig internt med IAM



Monika Harmiz
IAM Specialist
PostNord Group / Keynote

PostNord leverer kommunikations- og logistikløsninger, der er dybt afhængige af data og information, hvoraf størstedelen er digitalt lagret. Cyberkriminalitet er i stigende grad rettet mod brugere af teknologien snarere end selve teknologien. Derfor er det mere afgørende end nogensinde at beskytte ressourcer i virksomheden mod uautoriseret adgang og sikre overholdelse af relevante reguleringskrav. I denne sammenhæng spiller IAM en central rolle i Postnord ved at sikre, at rette personer har adgang til de passende ressourcer på det rigtige tidspunkt.

15:30 - 15:35: Opsummering



Qëndrim Fazliu
Samfundsredaktør og moderator
Computerworld

15:35 - 15:35: Tak for i dag