Cyber Briefing: AI kan udnytte dine VPN svagheder og lække dine data

8. april - Online,

10:00 - 10:05	**Velkomst ved dagens moderator** David Guldager, Tech ekspert og moderator
10:05 - 10:20	**AI-agenter arbejder ikke som mennesker – de opererer kontinuerligt, i maskinhastighed og på tværs af systemer** Niels Billekop, Enterprise Accounts, Arrow ECS
10:20 - 10:45	**Fra VPN til ZTNA: Sikkerhed i en AI domineret tid** Christoffer Callender, Regional Technology Officer, Broadcom
10:45 - 10:55	**Q&A til talere**
10:55 - 11:00	**Opsummering og tak for i dag**

10:00 - 10:05: Velkomst ved dagens moderator

David Guldager
Tech ekspert og moderator

10:05 - 10:20: AI-agenter arbejder ikke som mennesker – de opererer kontinuerligt, i maskinhastighed og på tværs af systemer

Niels Billekop
Enterprise Accounts
Arrow ECS / Partner

Det udfordrer traditionelle VPN-baserede adgangsmodeller, hvor netværksadgang ofte giver bred og implicit tillid. I stedet for at fokusere på netværket bør vi fokusere på data.

I dette indlæg sætter vi fokus på, hvorfor Datakontrol som et styrende kontrolpunkt i kombination med en ZTNA sikkerhedsmodel er kritisk:

· Fjerner implicit tillid og håndhæver kontekstbaseret adgang
· Beskytter følsomme data mod eksfiltrering – også via AI-services
· Skaber granular kontrol på tværs af endpoints, cloud og private apps
· Understøtter compliance-krav som GDPR, NIS2 og DORA.
Vi ser på, hvordan DLP, informationsklassifikation og adgangskontrol i en ZTNA sikkerhedsmodel er afgørende for at sikre AI-drevet produktivitet uden at øge risikoen.

10:20 - 10:45: Fra VPN til ZTNA: Sikkerhed i en AI domineret tid

Christoffer Callender
Regional Technology Officer
Broadcom / Partner

Organisationer, der vil følge med udviklingen i en AI domineret virkelighed, skal kunne reagere i maskinhastighed. Derfor er en Zero Trust arkitektur ikke længere en valgmulighed, men en nødvendighed. I dette oplæg får du konkrete værktøjer til at:

· Verificere identitet, enheder og AI agenter hurtigt og kontinuerligt
· Sikre hver AI forespørgsel med principper om mindst privilegium
· Kombinere ZTNA, DLP og CASB for fuld datakontrol
Kort sagt: Du får opskriften på Zero Trust arkitektur, der sikrer, at selv godkendte AI agenter kun får adgang, når de skal, og kun til det, de må.

Oplægget er på engelsk

10:45 - 10:55: Q&A til talere

Afholdes på engelsk

10:55 - 11:00: Opsummering og tak for i dag