Hybridkrig og cyberangreb - kommer det mig ved?

Michael Brødsted
SEGES Innovation

23. februar 2026

AI-GENERERET ILLUSTRATION

Agenda

- Trusselbilledet i dag
- Eksempler på angreb der kan påvirke
- IT-sikkerhed er et ledelsesansvar
- De største trusler mod virksomheder i dag
- De vigtigste 5 ting som du bør gøre
- Opsummering

AI-GENERERET ILLUSTRATION

SEGES INNOVATION

Trusselbillede i dag

- **Truslen fra cyberspionage er MEGET HØJ**.
  Typisk fra stater. Særligt Rusland og Kina retter løbende cyberangreb mod danske organisationer i forsøg på at få adgang til viden.

- **Truslen fra cyberkriminalitet er MEGET HØJ**.
  Cyberkriminelle rammer hele tiden ofre i Danmark med forskellige cyberangreb.

- **Truslen fra cyberaktivisme er HØJ**.
  Særligt pro-russiske hackere rammer løbende danske mål.

- **Truslen fra destruktive cyberangreb er MIDDEL**.
  Det er særligt Ruslands brug af wiper-angreb og angreb mod operationel teknologi.

- **Truslen fra aktivister**. Der er en trussel fra aktivister, som er imod landbruget.

SEGES INNOVATION

Eksempel på hacks der kan påvirke jeres bedrift

Til kunder i Azero

Azero har desværre i løbet af natten til fredag den 18-8-2023 klokken 04 været udsat for et ransomware angreb, hvor kriminelle hackere har lagt alle systemer ned. Hjemmesider, e-mail-systemer, kundesystemer, vores kunders hjemmesider mm. Alt. Et indbrud der har lammet Azero fuldstændigt, og som også rammer vores kunder hårdt.

Idet vi ikke kan og ej heller ønsker at imødekomme de kriminelle hackeres økonomiske krav om løsesum, har Azero's IT hold og eksterne eksperter arbejdet på højtryk på at få overblik over skaderne, og over hvad det var muligt at genskabe.

Det har desværre vist sig umuligt at genskabe mere data, og størstedelen af vores kunder har dermed mistet alt data hos os. Det gælder alle vi på nuværende tidspunkt ikke har kontaktet.

Hackingangrebet er meldt til politiet.

NotPetya-cyberangreb koster Mærsk milliardbeløb

Ransomware 16. august 2017 kl. 11:18 4 kommentarer

Skaden fra det globale cyberangreb blev begrænset, fordi koncernen med det samme lukkede de berørte systemer ned, oplyser Mærsk.

Artiklen er ældre end 30 dage

Manglende links i teksten kan sandsynligvis findes i bunden af artiklen.

Sommerens globale cyberangreb - NotPetya - har kostet Mærsk-koncernen mellem 1,3 og 1,9 milliarder kroner i tabt omsætning.

Jaguar-fabrikkerne står bomstille: Hackere kom ind via samme SAP-sårbarhed som ramte Arla

Hjemsendte medarbejdere, kompromitteret SAP-infrastruktur og en teenagehackergruppe med nye våben: Jaguar Land Rover er i så store problemer, at det kan ramme Storbritanniens økonomi.

9. september 2025 kl. 13.55

SEGES INNOVATION

Eksempel på kampange fra PET (er lige startet)

Sikker innovation

Beskyt din teknologi, forretning og Danmarks sikkerhed.

Danmark investerer hvert år milliarder i innovation og kommercialisering af ny viden gennem startups, spinouts og etablerede innovationsmiljøer. Disse investeringer er afgørende for vækst, arbejdspladser og udviklingen af teknologiske løsninger på globale udfordringer som klimaforandringer, energiomstilling og kommunikation.

SEGES INNOVATION

IT-sikkerhed er et ledelsesansvar

Påvirkning af driften

- Produktionsstop
- Ødelagt infrastruktur
- Ændre data (eks. DMS)
- Få jeres systemer offline

Ekstern påvirkning

- Krav fra kunder
- Mistede kunder
- GDPR bøder

AI-GENERERET ILLUSTRATION

SEGES INNOVATION

De største trusler mod virksomheder i dag - Phishing

Truslen kort

- Sender mails fra jeres konti
- Stjæle information og sælge den
- Ødelægge infrastruktur (ransomware)
- Ændre data
- Få jeres systemer offline

Beskyttelse

- Awareness træning
- Opdater software
- Brug stærke passwords og to-faktor login
- Planlæg hvad du gør, når du bliver hacket

AI-GENERERET ILLUSTRATION

SEGES INNOVATION

90% af alle hackerangreb skyldes menneskelige fejl

AI-GENEREret ILLUSTRATION

SEGES INNOVATION

De største trusler mod virksomheder i dag - Ransomware

Truslen kort

- Stjæle information og sælge den
- Ødelægge infrastruktur (ransomware)
- Ændre data
- Få jeres systemer offline

Beskyttelse

- Vælg sikkerhedsbeviste leverandører
- Opdater software
- Tag backup
- Brug stærke passwords og to-faktor login
- Lær at spotte mistænkelige mails
- Planlæg hvad du gør, når du bliver hacket

SEGES INNOVATION

Planlæg hvad du gør når du bliver hacket

AI-GENEREret ILLUSTRATION

SEGES INNOVATION

De største trusler mod virksomheder i dag – Menneskelige fejl

Truslen kort

- Klikke på phishing mails
- Fejlkonfiguring af udstyr
- Spring over hvor gæret er lavest

Beskyttelse

- Vælg sikkerhedsbeviste leverandører
- Opdater software
- Tag backup
- Brug stærke passwords og to-faktor login
- Lær at spotte mistænkelige mails
- Planlæg hvad du gør, når du bliver hacket

AI-GENERERET ILLUSTRATION

SEGES INNOVATION

Stil krav til dine leverandører

AI-GENEREret ILLUSTRATION

SEGES INNOVATION

Stigende trussel mod virksomheder i dag – Hacktivister

Truslen kort

- Stjæle information og offentliggøre den
- Tiltvinge sig adgang til produktionen
- Ændre data
- Få jeres systemer offline

Beskyttelse

- Vælg sikkerhedsbeviste leverandører
- Opdater software
- Brug stærke passwords og multi-faktor login
- Lær at spotte mistænkelige mails
- Planlæg hvad du gør, når du bliver hacket
- Fysisk sikkerhed på lokation (døre) Overvågning/alarm

SEGES INNOVATION

Overvej hvilke døre der skal være låst

AI-GENEREret ILLUSTRATION

SEGES INNOVATION

De 5 vigtigste ting I bør gøre

- Backup
- Awareness træning
- Stil krav til jeres leverandører
- Multi-faktor login
- Hav en plan for hvis I bliver hacket

KILDE: https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/4-tag-backup-af-data

SEGES INNOVATION

Backup

- Daglig backup
- Have en offline backup
- Test den minimum en gang om året
- Overvej ekstern partner
  B4Restore, USER IT, Atea m.f.

KILDE: https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/4-tag-backup-af-data

SEGES INNOVATION

Awareness træning

- Månedlige krav til træning
  Også for små virksomheder
- Lav løbende phishing test
  Husk at tale om evt. fejl
- Hav en kultur der understøtter sikkerhed
- Brug en ekstern partner
  Moxso, Cyberpilot m.f.

SEGES INNOVATION

Stil krav til jeres leverandører

- Generel vurdering af leverandøren
- Vælge nogen med branche kendskab
- Certificering (ISO 2700x, ISAE 3xxx ect.)
- Kan de leve op til lovgivningen (NIS2, GDPR ect.)
- Løbende opdatering af software
- Dokumentation af løsning

SEGES INNOVATION

Multi-faktor og gode passwords

- Slå multi-faktor alle de steder du kan
- Brug lange passwords
  Eks. J3gM1gEnGaardB4ggeVi1
- Brug gerne en sikker password manager
  Eksempel proton.me (gratis version), Bitwarden.com (gratis version), Keeper, OnePass m.f.
- Genbrug IKKE passwords, det vil sige unikke passwords (et password til en tjeneste)

SEGES INNOVATION


PRESS ANY KEY!

Når det rammer

- Hav en plan inden I bliver ramt
- Sikkerdigital Cyberhotline (3337 0037) gratis
- Dubex Incident Response (3283 0403)
- Itm8 Incident Response Team (9195 9595)
- RIT Cyberhotline (8736 8899)

AI-GENERERET ILLUSTRATION

SEGES INNOVATION

Hvis du vil læse mere (i prioriteret rækkefølge)

- Syv gode råd om IT-sikkerhed
  https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed
- Cyberhotline (3337 0037)
  https://www.sikkerdigital.dk/cyberhotline
- UDSYN 2025 (IT trusselvurdering)
  https://www.fe-ddis.dk/da/produkter/Risikovurdering/risikovurdering/udsyn-2025/
- Nationalt Risikobillede (Generel risikovurdering)
  https://samsik.dk/wp-content/uploads/2025/04/NATIONALT-RISIKOBILLEDE-2025.pdf

SEGES INNOVATION

Gode gratis tools

- Sikker mail, vpn og password manager m.m.
  https://proton.me/
- Password manager
  https://bitwarden.com/
- Content blocker
  https://ublockorigin.com/
- Obsidian notetool
  https://obsidian.md/
- Cyberhotline (3337 0037)
  https://www.sikkerdigital.dk/cyberhotline

SEGES INNOVATION