SUMMARY CYBERSECURITY

Det aktuelle trusselsbillede for danske virksomheder i 2026

Indledning

Jacob giver et samlet overblik over det aktuelle og fremadrettede cybertrusselsbillede for danske virksomheder og placerer cybersikkerhed i en bred samfundsmæssig, geopolitisk og forretningsmæssig kontekst.

Kompleksitet og digital afhængighed

Kombinationen af stigende kompleksitet og total digital afhængighed er, ifølge Jacob, det, gør nutidens trusler svære at håndtere og konsekvenserne særligt alvorlige. Udgangspunktet er en erkendelse af, at digitalisering har gjort virksomheder mere effektive og mere forbundne, men også mere sårbare. Cybertrusler er ikke længere isolerede IT-hændelser, men hændelser med direkte konsekvenser for drift, tillid og samfundsstabilitet.

Kompleksiteten betyder, at cyberrisici ikke kan håndteres i siloer, men være en integreret del af hele virksomheden – fra ledelse til yderste endpoint.

Trusselsbilledet i 2026: aktører, katalysatorer og dynamikker

Jacob tegner et samlet billede af et trusselspil, der er blevet både bredere og mere komplekst. Cybertrusler drives i dag af flere samtidige katalysatorer og aktører, som forstærker hinanden.

Centralt i trusselsbilledet står:

- Professionalisering af cyberkriminalitet, med klare roller, arbejdsdeling og forretningsmodeller.
- Statslige aktører og cyberspionage, hvor særligt Rusland, Kina, Iran og Nordkorea spiller forskellige, men markante roller.
- Hybridtrusler, hvor cyberangreb kombineres med fysisk sabotage, påvirkning, misinformation og pres mod kritisk infrastruktur.
- Forsyningskædeangreb, hvor leverandører bruges som indgang til mange virksomheder på én gang.
- Geopolitik, som i stigende grad styrer målvalg, timing og intensitet i angreb.
- Kunstig intelligens, der accelererer både angreb, sårbarheder, social engineering og skalering af trusler.

Ifølge myndighedernes risikovurderinger placerer cyberhændelser sig blandt de mest alvorlige risici overhovedet – både målt på sværhedsgrad og konsekvensniveau. Truslerne er globale, men konsekvenserne rammer lokalt og direkte.

Konsekvenser for virksomheder

Jacob understreger, at dette trusselsbillede har klare og håndgribelige konsekvenser for danske virksomheder – uanset branche og størrelse. Og de konsekvenser viser sig på flere niveauer:

- **Akut:**
  Driftsstop, tabt omsætning, høje omkostninger til incident response og manglende serviceleverancer.
- **Mellemlang sigt:**
  Tab af kundetillid, juridiske og regulatoriske konsekvenser samt øget ledelses- og bestyrelsesansvar.
- **Lang sigt:**
  Svækket konkurrenceevne, fald i virksomhedsværdi og reduceret tillid til digitalisering som fundament.

Samtidig peger han på, at mange organisationer stadig undervurderer deres egen digitale afhængighed og indbyrdes sammenhæng med leverandører, kunder og kritisk infrastruktur.

Vejen mod øget modstandsdygtighed

For at styrke modstandsdygtigheden peger Jacob på behovet for en mere helhedsorienteret tilgang til cybersikkerhed:

- Cybersikkerhed skal være ledelsesforankret og strategisk prioriteret.
- Risiko skal forstås og styres, så indsatser kan prioriteres korrekt.
- Organisationen skal have de rette kompetencer, processer og standarder på plads.
- Infrastruktur og systemer skal løbende vedligeholdes og opdateres.
- Der skal være et realistisk beredskab for, når hændelser indtræffer.

Budskabet er klart:
Cybersikkerhed handler ikke om at eliminere risiko, men om at opbygge en virksomhed, der kan modstå, håndtere og komme videre efter angreb.

Key take aways

- Cybertrusler i 2026 er drevet af digital afhængighed, kompleksitet og geopolitik, hvilket gør konsekvenserne både alvorlige og uundgåelige.
- Virksomheder er en integreret del af et globalt trusselspil og kan rammes både direkte og via leverandører og partnere.
- Cyberkriminalitet er professionaliseret og ofte koblet til statslige interesser, hvilket øger både kapacitet og intention.
- Kunstig intelligens accelererer både angreb og sårbarhedsfund og stiller nye krav til ledelse, risikostyring og sikkerhed.

Vil du vide mere?

Kontakt vores specialist

Jacob er vores specialist
Kontakt ham til en snak om dine virksomhedsbehov.

Jacob Herbst
Director of Strategic Cybersecurity and Policy, Conscia
jher@conscia.com

Conscia
Conscia A/S
Østbanegade 135,
2100 København Ø
Denmark

Kontakt
+45 70 20 77 80
conscia.com

Conscia
Secure progress