

Cyber Security Rapport // Digital oprustning i en ny virkelighed



// BIDRAGSYDERE

Denne cybersikkerhedsrapport er blevet til med bidrag fra følgende personer:

Esben Kaufmann
Erik M. L. Bandholm
Johnni Meldgård Rude
Christian Ingerslev
Christoffer Bech
Antonio Vu Nguyen
Jesper Vester Sandberg
Emilie Zofie Kaae Riis
Jacob Krahn
Danni Louis Nielsen Bred Randeris
Mathias Holdt
Martin Kofoed Høding

Redaktion

Julie Blond Andersen
Louise Nissen
Helle Wittendorff Bohn
Casper Theilgaard

En stor tak til

Dansk Erhverv
Københavns Lufthavn

// FORORD

Det er tid til at gå fra bevidsthed til handling

Cybersikkerhed står nu og i de kommende år højt på agendaen hos mange danske virksomheder og offentlige organisationer. Det er et godt udgangspunkt. Men at være bevidst om truslerne er ikke det samme som at være rustet til at modstå dem.

De seneste år har vist, hvordan cyberkriminalitet, geopolitik og teknologi er smeltet sammen i et komplekst trusselsbillede, hvor virksomheder og offentlige institutioner i Danmark er blevet en del af en voksende, digital frontlinje.

Der er ingen tvivl om, at cybersikkerhed har momentum. Det er ikke længere et spørgsmål, om det sker – men hvornår og hvordan. Og det momentum forpligter og stiller krav til både ledere, beslutningstagere og samarbejdspartnere. Og netop dét er noget, jeg som forhenværende CEO i en virksomhed, der har oplevet konsekvenserne af et massivt cyberangreb, kan skrive under på.

I årets cyberrapport tager vi hos itm8 temperaturen på den digitale oprustning i danske virksomheder. Gennem en omfattende undersøgelse har vi spurgt 192 beslutningstagere i danske virksomheder, hvordan de arbejder med cybersikkerhed. Resultatet viser et tydeligt mønster: Virksomhederne er opmærksomme på truslen – men de mangler fortsat en øget modenhed, prioritering og handlekraft for at følge med udviklingen.

I rapporten giver vi vores perspektiv på det aktuelle trusselslandskab, og kommer med konkrete anbefalinger til, hvordan du kan styrke sikkerheden i din organisation. Du kan blandt andet læse om:

- Hvordan effektiv IT-sikkerhed ikke kun handler om systemer og teknologi – men om mennesker, kultur og processer.
- Hvordan løbende tests kan måle, hvor stærk din organisation i virkeligheden er.
- Hvordan fremtiden ser ud, når det kommer til cybersikkerhed.

Cybersikkerhed er ikke alene en opgave for IT-afdelingen – det er et fælles ansvar for alle i forretningen. Lad os i fællesskab sikre, at 2026 bliver året, hvor cybersikkerhed bevæger sig fra bevidsthed til handling.

Rigtig god læselyst!

Christian Ingerslev
CEO, itm8



itm8 Cyber Security Survey 2025

I løbet af rapporten vil du blive præsenteret for data fra vores egen spørgeundersøgelse, hvor vi har spurgt 192 beslutningstagere i danske virksomheder om, hvordan det står til med cybersikkerheden hos dem. Den data er med til at understøtte fokus og pointer undervejs i rapporten. Du kan læse mere om vores survey og dataindsamling på side 68.



Undersøgelse: Hvordan står det til med cybersikkerheden i danske virksomheder?

// INDHOLD

07 #1 Trusselsbilledet anno 2026

08 Cybersikkerhed har momentum – og det forpligter

13 Udtalelse fra Dansk Erhverv

14 Fire spørgsmål til Københavns Lufthavns CISO

16 Hvilke cybertrusler og konsekvenser frygter danske virksomheder mest?

21 #2 Test og overvåg din sikkerhed

22 Giver det stadig mening at lave sikkerhedstests i 2026?

24 Det stærkeste beredskab er det, der bliver afprøvet i praksis

29 Overvågning er ikke en luksus – det er sikkerhed

32 Quiz: Hvor god er din viden om IT-sikkerhed?

37 #3 AI på godt og ondt

38 AI i hænderne på hackere – truslerne vi glemmer i AI-hypen

42 AI er et forsvarsværktøj – men ikke nok til at stoppe cyberangreb

45 #4 Mennesker og træning som forsvarslinje

46 Sikkerhed bliver først skabt, når teknologi, mennesker og processer arbejder sammen

50 Fremtidens awareness handler om gode ritualer og verificering

55 #5 Cybersikkerhed i fremtiden

56 Cyber Threat Intelligence handler om at være forberedt

61 Næste fase i cybersikkerhedsrejsen kræver handling – ikke flere løsninger

65 7 spørgsmål enhver leder bør stille sig selv

66 4 gode råd til oprustning af danske virksomheders cybersikkerhed

68 Om survey-undersøgelsen

Trusselsbilledet anno



2026

I dette kapitel kan du læse om, hvordan trusselsbilledet ser ud for danske virksomheder lige nu.

Cybersikkerhed har momentum – og det forpligter.

Cybertruslerne vokser hurtigt, og cybersikkerhed er gået fra specialistedisciplin til strategisk nødvendighed. Udviklingen følger en tydelig hockeystick-kurve, hvor både kriminalitet og teknologi accelererer, og hvor Danmark i stigende grad befinder sig i frontlinjen af den digitale konflikt.

Læs artiklen af Esben Kaufmann på side 8.

Digital sikkerhed er et vilkår for at drive virksomhed i dansk erhvervsliv.

Tiden, hvor cyberangreb kunne betragtes som noget fjernt og abstrakt, er forbi. Cybertruslen fylder mere end nogensinde – og digital sikkerhed er blevet et grundvilkår for at drive virksomhed i Danmark. For at stå stærkere skal virksomheder have klare planer, tydelige roller og et beredskab, der aktiveres, før skærmene bliver sorte.

Læs udtalelsen fra Jakob Ellemann-Jensen fra Dansk Erhverv på side 13.

Fire spørgsmål til Københavns Lufthavns CISO

Hvilke trusler bekymrer Københavns Lufthavns sig mest for? Hvilke konsekvenser frygter de ved et cyberangreb? Og hvad er mest udfordrende i arbejdet med at forbedre cybersikkerheden? *Læs interviewet med Christina Hastrup, CISO, Cyber & Information Security, Københavns Lufthavn på side 14.*

Hvilke cybertrusler og konsekvenser frygter danske virksomheder mest?

Vi har spurgt 192 beslutningstagere i danske virksomheder om, hvilke trusler de betragter som mest kritiske og hvilke konsekvenser, de frygter mest ved et cyberangreb. *Se statistikken fra vores survey på side 16.*

// NUTIDENS OG FREMTIDENS CYBERUDFORDRINGER

Cybersikkerhed har momentum – og det forpligter

Vi står midt i en tid, hvor cybersikkerhed ikke længere er et nicheområde for specialister – men en strategisk forudsætning for vækst, stabilitet og tillid. Det momentum, cybersikkerhed har fået de seneste år, kan bedst beskrives som en ”hockeystick-effekt”, hvor kurverne for både teknologi og kriminalitet accelererer stejlt opad.

af Esben Kaufmann

Executive Partner, Professional Services, itm8



Fra simple virusser til strategiske cyberangreb

Ser vi bare 25 år tilbage, var internettet en nysgerrig legeplads for teknikinteresserede, virksomheder og universiteter. I dag er det selve fundamentet for alt – fra økonomi og kritisk infrastruktur til vores private liv. Samtidig er kriminaliteten fulgt med. Hvor simple virusser tidligere kunne forstyrre en enkelt bruger, ser vi i dag ransomware-angreb, der kan lamme hele sektorer og koste samfund milliarder.

Denne acceleration betyder, at sikkerhed ikke længere kan betragtes som et eftertænkt lag, men som en integreret del af enhver beslutning om teknologi, innovation og drift.

Momentum skaber ansvar

Når cybersikkerhed har momentum, forpligter det. Det forpligter virksomheder, myndigheder og beslutningstagere til at:

- forstå de risici, der følger med digitalisering.
- prioritere investeringer i beskyttelse og modstandsdygtighed.
- sikre at ledelser og bestyrelser har den nødvendige indsigt til at træffe informerede beslutninger.

Cyberspace er blevet en del af slagmarken

Den sikkerhedspolitiske virkelighed har ændret sig fundamentalt siden Ruslands invasion af Ukraine i 2022. Cyberangreb er ikke længere blot økonomisk motiverede forbrydelser, men anvendes systematisk som **strategiske våben i den hybridkrig**. Rusland fører mod Vesten.

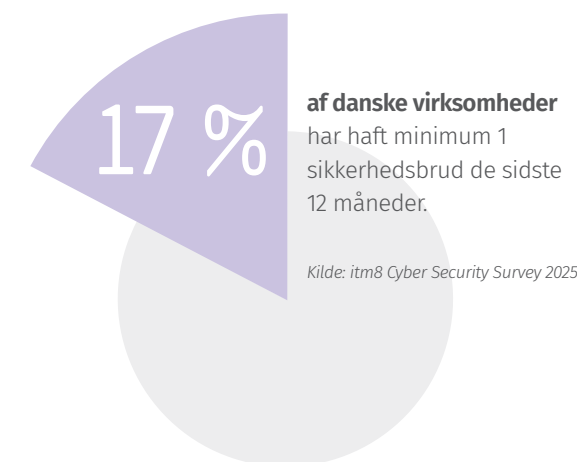
Formålet er at destabilisere, skabe tvivl og svække tilliden til statslige institutioner, medier og forsyningskritiske funktioner.

I løbet af 2024 og 2025 har Danmark oplevet en række koordinerede DDoS-angreb mod ministerier, myndigheder og private virksomheder – ofte udført af pro-russiske hacktivistgrupper som *Killnet* og *NoName057(16)*. Disse angreb har haft til hensigt at forstyrre driften og teste myndighedernes reaktionsevne, snarere end at påføre varig skade.

Danmark i frontlinjen af den digitale konflikt

Angreb mod kritisk infrastruktur, herunder danske vandværker og energiselskaber, har vist, hvordan forsyningssektoren er blevet en del af den digitale frontlinje. Flere hændelser har involveret forsøg på at kompromittere kontrolsystemer (OT) eller udnytte sårbarheder i tredjepartsleverandører – ofte som led i bredere påvirkningsoperationer rettet mod Vesteuropæiske allierede.

Danmark står her som en tydelig allieret i den ukrainske frihedskamp – og dermed også som et oplagt mål for statssponsorerede cyberaktiviteter. Vi befinder os reelt i frontlinjen af en digital konflikt, hvor cyberspace er blevet en del af slagmarken.



Fra compliance til konkurrencekraft

Cybersikkerhed har længe været drevet af krav – lovgivninger som NIS2, CER og DORA – kundernes forventninger og forsikringsselskabers betingelser.

Men med momentum ændres billedet. Sikkerhed er i dag en konkurrenceparameter. Den virksomhed, der kan dokumentere robusthed og ansvarlighed, står stærkere på markedet.

FREMTIDENS UDFORDRINGER BANKER PÅ DØREN

Vi skal ikke alene håndtere de trusler, vi kender i dag.
Nye teknologier rejser nye sikkerhedsspørgsmål, som vi er
nødt til at forholde os til.

Mit bud på fire fokusområder i de kommende år

#1. AI-sikkerhed

Kunstig intelligens bliver en konkurrencefaktor – men også en risiko, når den kan bruges til avanceret phishing, deepfakes og automatiserede angreb.

#2. PQC (Post-Quantum Cryptography)

Den dag kvantecomputere bliver operationelle, risikerer vi, at nutidens kryptering kan brydes. Derfor skal forberedelserne starte nu.

#3. Forsyningskæder

Angreb sker sjældent frontalt. De finder vej gennem svagheder i leverandørled og partnerskaber.

#4. Modstandsdygtighed

Krisestyring, beredskabsplaner og evnen til hurtigt at komme tilbage i drift er lige så vigtige som tekniske kontroller.

Vores perspektiv

Hos itm8 ser vi det som vores ansvar at omsætte teknisk indsigt til strategisk handling. Cybersikkerhed er ikke kun et spørgsmål om værktøjer men om ledelse, samarbejde og forankring i forretningen.

Med denne rapport ønsker vi at give et realistisk, men handlekraftigt billede af, hvordan organisationer kan bruge sikkerhed som drivkraft for digital tillid og vækst.

Momentum og hockystick

Cybersikkerhedens hockystick-effekt viser os én ting: Vi har ikke luksussen at vente. Jo mere digital vores verden bliver, desto større er vores forpligtelse til at tage sikkerhed alvorligt – ikke kun af hensyn til compliance, men fordi det er afgørende for forretning, samfund og tillid.

Momentum er her. 2026 er året, hvor cybersikkerhed skal bevæge sig fra bevidsthed til adfærd. Fra planer til handling!

Vi skal bruge den momentum til at skabe et mere sikkert digitalt Danmark – sammen.

Cyber Security Rapport 2026

Denne rapport giver et samlet billede af det danske cybertrusselsbillede anno 2026. Den bygger på vores erfaringer fra arbejdet med hundredvis af sikkerhedshændelser, sikkerhedsanalyser og rådgivningsforløb på tværs af virksomheder, brancher og kritiske sektorer – samt vores egen survey.

Formålet er ikke kun at kortlægge risici men at omsætte erfaringer til handling – så organisationer kan styrke deres digitale modstandsdygtighed og ledelser kan træffe beslutninger på et oplyst grundlag.

Teknologisk indflydelse

HOCKEYSTICK-EFFEKTEN
Den teknologiske udvikling har ramt en "hockey stick effekt" fordi særligt de sidste 5 års udvikling har været massiv.

2020 2021 2022 2023 2024 2025 2026

73 %

af danske virksomheder har et ønske om at forbedre IT-sikkerheden

Kilde: itm8 Cyber Security Survey 2025

// UDTALELSE FRA DANSK ERHVERV

Digital sikkerhed er et vilkår for at drive virksomhed i dansk erhvervsliv

Gennem historien har balancen mellem evnen til at angribe og evnen til at forsvare sig været afgørende for samfundets tryghed. Når vi har haft stærke defensive kapabiliteter, har konflikter og angreb været færre. Ganske enkelt fordi, det har været for dyrt og for besværligt at slå til. Men i dag løber de offensive teknologier stærkt. Særligt på det digitale område. Det betyder, at vi risikerer at blive løbet over ende, hvis vi ikke styrker vores digitale sikkerhed.

Vi bliver nødt til at stoppe med at se cyberangreb som et abstrakt og isoleret fænomen. Vi må se det som et af hovedværktøjerne i arsenalet af gråzoneoperationer mod Danmark og Europa. Som en naturlig følge af den nuværende verdens(u)orden.

Dansk erhvervsliv skal derfor se digital sikkerhed som et vilkår for at drive virksomhed. Det er ikke længere et spørgsmål om, hvorvidt man skal sikre sig, men rettere et spørgsmål om hvordan.

Blandt Dansk Erhvervs medlemsvirksomheder er cybertruslen den næststørste bekymring. Det taler sit tydelige sprog om, at cybertruslen er flyttet ind i vores bevidsthed. Det er essentielt, at den bevidsthed omsættes til sikkerhedsforanstaltninger og beredskab. Det er vigtigt for virksomheder at have en klar plan for, hvem der gør hvad, når uheldet er ude. Roller og opgaver skal være defineret på forhånd – ikke først, når skærmene bliver sorte.

Heldigvis rummer investeringer i sikkerhed ikke kun et nødvendigt værn mod trusler; de er også en forudsætning for vores konkurrenceevne.

Derfor var jeg rigtig glad for at få lov at skrive et bidrag til itm8s nye rapport og opfordre danske virksomheder til at tage cybersikkerhed alvorligt.

Rigtig god læsning.

Jakob Ellemann-Jensen
Vicedirektør, Dansk Erhverv

DANSK ERHVERV





// INTERVIEW

Fire spørgsmål til Københavns Lufthavns CISO

Vi har stillet fire spørgsmål vedrørende cybersikkerhed til Christina Hastrup der er CISO, Cyber & Information Security i Københavns Lufthavn.

Christina Hastrup

CISO, Cyber & Information Security, Københavns Lufthavn



#1

Hvilke cybertrusler bekymrer dig mest?

Det er svært med sikkerhed at vide, hvad der kommer, hvad der rammer, og hvilke angreb der vil gøre mest ondt. Men det er klart de store destruktive cyberangreb, vi er mest bekymrede for. For uanset hvor meget vi forbereder os, vil et stort og veltilrettelagt angreb betyde nedsat kraft, kriseberedskab og dårligere betingelser for vores kunder og passagerer.

Jeg tror ikke, at vi har set det værste endnu, for det er svært at forestille sig, hvad de store aktører kan. Og jeg tror, at det, vi ikke kan forestille os, er det, der kommer til at have størst konsekvenser for os.

#3

Hvad holder jer tilbage i forhold til at forbedre cybersikkerheden i Københavns Lufthavn?

Vi har arbejdet med cybersikkerhed i Københavns Lufthavn længe og er i fuld gang med at optimere yderligere – det er et konstant arbejde på et område i hurtig udvikling. Men det er en kompleks opgave. Cybersikkerhed er ikke et quick-fix – det er en disciplin, der kræver tid og tålmodighed.

Cybersikkerhed skal og kan ikke kun etableres af sikkerhedsafdelingen. Det er en opgave, som alle i organisationen skal være med til at løfte. Og her er jeg bevidst om, at når vi øger sikkerheden, så pålægger vi vores kollegaer i organisationen en tidskrævende opgave. Det er ikke nok bare at købe et system, der skal også bruges mennesker til at implementere og anvende det. Og det er en balancegang at få nok tid til det set i forhold til alle de andre opgaver, der også er behov for at løse i en virksomhed.

#2

Hvilke konsekvenser frygter du mest ved et cyberangreb?

Jeg frygter selvfølgelig, at vores operation bliver ramt af et angreb. Det vil betyde, at vi mister kapacitet, og at folk ikke kan komme derhen, hvor de skal. Selvom vi har lavet manuelle driftsprocedurer og kriseplaner til sådan en situation, vil det betyde nedsat kraft, og det koster jo – både økonomisk og i forhold til passageres tillid og vores samarbejde med forskellige luftfartsselskaber.

#4

Hvad ville du anbefale andre danske virksomheder for at forbedre cybersikkerheden?

Jeg vil helt klart starte med basics. Der er stadigvæk rigtig mange der kæmper med at få styr på passwords, patching og sårbarheder.

Og det er altafgørende, at der er styr på det underliggende fundament. Det er ikke simpelt – men det er vigtigt.

Det er helt forståeligt, at cybersikkerhed ikke står øverst på listen hos de små virksomheder. Men det er bare så vigtigt at prioritere at "låse døren på sit hus" så godt, at aktørerne ikke gider at bøvle med at komme ind.

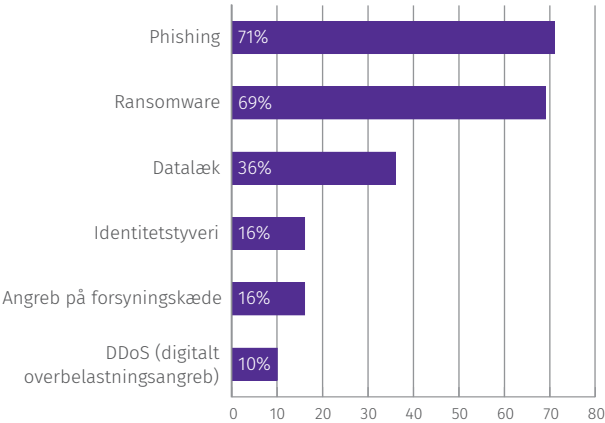
// CYBERTRUSLER

Hvilke cybertrusler og konsekvenser frygter danske virksomheder mest?

I vores survey har vi spurgt de 192 beslutningstagere i danske virksomheder om, hvilke trusler de betragter som mest kritiske og hvilke konsekvenser de frygter mest ved et cyberangreb.

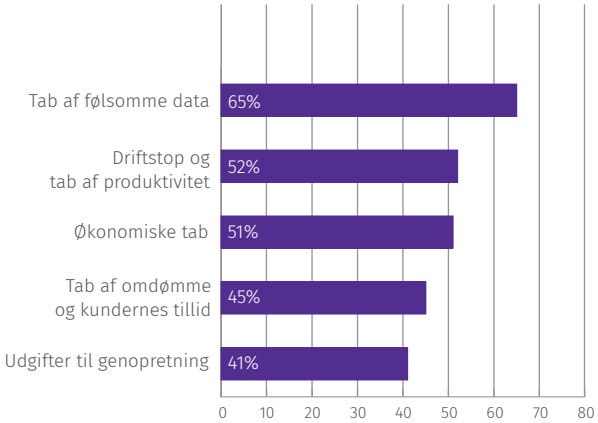
Hvilke typer trusler vurderer du som mest kritiske?

Respondenterne kunne vælge flere svar.



Hvilke konsekvenser frygter du mest ved et cyberangreb?

Respondenterne kunne vælge flere svar.



Kilde: itm8 Cyber Security Survey 2025

10 typiske årsager til, at virksomheder bliver ramt af cyberangreb

- 1. Ufuldstændig viden om forretningskritiske systemer og udstyr
- 2. Svage adgangskodepolitikker
- 3. Ingen implementering af multifaktorgodkendelse (MFA)
- 4. Ingen kontinuerlig patch management
- 5. Utilstrækkelig vedligeholdelse af adgangskontrol og tilladelser
- 6. Manglende alarmer og logning konfigureret til vigtigt udstyr
- 7. Ufuldstændige eller ubekræftede sikkerhedskopier af kritiske data
- 8. Fravær af Active Directory (AD) niveauinddeling (AD Tiering)
- 9. Ingen begrænsning på adgang til Remote Desktop
- 10. Begrænset fokus på reduktion af lokale konti og domæneadministratorer

Listen er baseret på vores Incident Response-sager fra 2022 til 2025



41 % af danske virksomheder anvender kun multifaktor-login på **nogle af** deres systemer.

Kilde: itm8 Cyber Security Survey 2025

Test og overvåg



din sikkerhed

I dette kapitel dykker vi ned i, hvordan virksomheder kan teste, træne og styrke deres sikkerhed i praksis.

Giver det stadig mening at lave sikkerhedstests i 2026? Mange virksomheder føler sig trygge, fordi de har investeret i sikkerhed – men uden tests er det kun en følelse. Mange virksomheder ved reelt ikke, om deres forsvar holder. Sikkerhedstests giver et faktabaseret billede af svaghederne, både digitalt og fysisk, og afslører de blinde vinkler, som angribere udnytter først. Med andre ord er test det mest ærlige spejl på virksomhedens modstandsdygtighed. *Læs artiklen af Christoffer Bech på side 22.*

Det stærkeste beredskab er det, der bliver afprøvet i praksis. Alt for mange virksomheder har enten ingen beredskabsplan – eller en plan, der aldrig er afprøvet. Når presset stiger, er det træning og klare roller, der afgør, om driften kan holdes i gang. Et stærkt beredskab kræver øvelser, forankring og et simpelt, brugbart styringsværktøj, der fungerer i praksis – ikke blot på papir. Når tiden er afgørende, og beslutninger skal træffes hurtigt, viser test i virkeligheden, om organisationen faktisk er klar til krisen. *Læs artiklen af Antonio Vu Nguyen på side 24.*

Overvågning er ikke en luksus – det er sikkerhed. Uden overvågning ved virksomheder reelt ikke, hvad der foregår i deres eget miljø. Med overvågning er det muligt at opdage mønstre, reagere hurtigt og begrænse skaden, før et mindre brud bliver til en hændelse med store konsekvenser. Selv små virksomheder kan være attraktive mål – derfor handler overvågning om synlighed, reaktionsevne og evnen til at beskytte driften i et landskab, hvor angreb ofte foregår stille og ubemærket. *Læs artiklen af Jesper Vester Sandberg på side 29.*

Quiz: Hvor god er din viden om IT-sikkerhed? Test din viden med 10 spørgsmål, der enten er sande eller falske. Se hvor mange du kan få rigtige. *Prøv quizen på side 32.*

// SIKKERHEDSTESTS

Giver det stadig mening at lave sikkerhedstests i 2026?

Det er ikke unormalt at høre en leder sige, at de føler sig godt stillet, fordi de har købt en cybersikkerhedsservice. Men virkeligheden er, at hvis selvsamme ikke tester deres cyberforsvar – inklusive de fysiske – så kan det faktisk være ligegyldigt. Det er tid til at kigge indad. Og at basere sin sikkerhed på fakta frem for følelser.

Af Christoffer Bech

Director of Technical Security and Incident Response, itm8

**Fakta frem for følelser**

Danmark står lige nu i en verden, hvor den geopolitiske temperatur bliver ved med at stige. Cyberoperationer er nu en del af den daglige internationale politik, og både statsstøttede og kriminelle aktører er særdeles aktive.

Politikeren har lært et nyt ord: hybridkrig. Men gå ikke i panik. Det er aldrig for sent at begynde at arbejde struktureret og målrettet med cybertrusler.

For danske virksomheder – uanset størrelse – betyder det, at cybersikkerhed ikke handler om håb eller tro. Det handler om fakta! At "føle" sig sikker er ikke det samme som at være sikker.

I 58 % af danske virksomheder er der ikke lavet tekniske sikkerhedstests eller organisatoriske øvelser de sidste 12 måneder.

*Kilde: itm8 Cyber Security Survey 2025***Derfor er sikkerhedstest stadig vigtige**

En penetrationstest er en kontrolleret måde at opdage, hvordan en angriber ville bryde ind i dit IT-miljø. Testen viser dig, om virksomhedens sikkerhedsforanstaltninger fungerer, eller ej. Gerne på tværs af alle lag af din digitale og fysiske sikkerhed.

En penetrationstest er ikke bare et afkrydningsfelt eller en compliance-opgave. Det er den eneste måde du kan se den faktiske, aktuelle tilstand i øjnene og handle på det.

Sikkerhedsværktøjer, awareness-programmer og politikker har alle en værdi. Men uden at teste dem, antager du kun, at de virker. Den virkelige verden er ligeglad med antagelser.

De svage punkter

I vores løbende arbejde på tværs af danske organisationer, ser vi fortsat de samme svage punkter:

- **Applikationer:** Websystemer, API'er, mobil apps og AI-integrationer har ofte skjulte sårbarheder, fordi det stadig er i deres tidlige dage.
- **Adgangskontrol:** Svage adgangskoder, manglende multifaktorgodkendelse (MFA) og delte konti er stadig almindelige indgangspunkter.
- **Segmentering og niveauinddeling:** Utilstrækkelig segmentering gør det muligt for angribere at bevæge sig frit, når de først er inde.
- **Incident Response:** Mange organisationer mangler klare procedurer, når tingene går galt. Når et angreb først er opdaget, tæller hvert sekund, og kaos er ikke en strategi.

Fysisk og digitalt er ikke længere adskilte verdener

Moderne modstandere tænker ikke i siloer – og det bør vi heller ikke. Et fysisk indbrud kan nemt blive til et cyberangreb, og en digital kompromittering kan muliggøre fysisk adgang.

Forestil dig en angriber, der får adgang til dit kontor, tilslutter en ondsindet enhed eller manipulerer netværksenheder. Disse hybride angreb er ikke længere teori; de sker.

Derfor fusionerer modne organisationer nu fysiske og cybersikkerhedsmæssige indsatser – og tester begge dele som én.

At se virkeligheden i øjnene

I 2026 giver sikkerhedstests stadig mening, ja nok mere end nogensinde. Fordi sikkerhedstest giver dig fakta, ikke følelser. Det fortæller dig, om dit forsvar rent faktisk holder, ikke blot at du bare håber, at det vil.

Cybersikkerhed handler ikke om at undgå frygt, det handler om at håndtere frykten med viden og fakta. Du kan kun forsvare det, du virkelig forstår – og du kan kun forstå dine svagheder ved at teste dem.

I en tid, hvor modstandere bliver hurtigere, smartere og mere koordinerede, er sikkerhedstest stadig det mest ærlige spejl, du kan holde op mod din organisation.

Omgå mennesker med de rette kompetencer

At være virksomhedsleder i den aktuelle verdenssituation er kompliceret. Engang handlede det kun om at se på tallene. Nu kan cybertrusler i værste fald lukke virksomheder ned.

Det handler i stigende grad om fremsynethed, robusthed og at være omgivet af de rigtige mennesker med de rigtige kompetencer og færdigheder.

Måske er du ikke en teknisk leder? Men du kan altid stille opklarende spørgsmål og ansætte andre end dem, du cykler eller spiller padel med.

Det er ikke flovt som leder at ikke vide alt. Men det kan være farligt ikke at anerkende det!

Det er aldrig for sent

Den positive nyhed er, at du har hjemmebanefordel. Du kender dit system bedre end modstanderne. Hold fast i det! Og husk, at det er aldrig for sent at begynde at arbejde målrettet på de cybersikkerhedsudfordringer, du måtte have.

↓ 3 ting, jeg vil anbefale i 2026

1. Få testet for lavthængende frugter angående fysisk sikkerhed. Kan en ondsindet aktør forholdsvis nemt komme til IT-udstyr?

2. Test jeres overvågning – hvad opdager I? Overvåges det rigtige? Bliver alarmer hurtig henkastet som falsk alarm?

3. Invester i eller udarbejd et sikkerheds-årshjul blandet med penetrationstest, hærkning og strategisk rådgivning.

Hvis du formår at gennemføre disse tiltag, opnår du et faktabaseret grundlag, der styrker din virksomheds beredskab og evne til at imødegå de aktuelle og kommende trusler.

// BEREDSKABSPLANER

Det stærkeste beredskab er det, der bliver afprøvet i praksis

Mange virksomheder har slet ikke har nogen beredskabsplan. Og dem der har en – der ligger den ofte i en skuffe og er sjældent afprøvet i praksis – det viser tal fra vores egen undersøgelse. For det er først, når virksomheden står i en situation, hvor planen skal bruges, at det viser sig, om den rent faktisk beskytter det vigtigste i virksomheden: driften, kunderne og omdømmet.

Af Antonio Vu Nguyen
Strategic Cyber Risk Advisor, itm8



“Train as you fight”

Formålet med en beredskabsplan er i sin kerne enkel: den skal sikre, at virksomheden kan opretholde sine vigtigste funktioner, når noget uventet rammer. Samtidig skal planen give ledelsen et klart mandat til at træffe hurtige og forretningskritiske beslutninger.

Her kommer princippet “Train as you fight” ind. Det stammer fra de militære styrker, som jeg også selv har personlig erfaring med. Gennem oplevelser i blandt andet Afghanistan og Irak har man erfaret, at ingen kan improvisere sig ud af en krise. Når presset stiger, falder den menneskelige beslutningsevne.

Med andre ord handler vi ikke, som vi ønsker, men ud fra det, som vi er trænet til. Det princip kan direkte overføres til enhver virksomhed.

Øvelser, forankring og accept af ledelsen er afgørende

Det er ikke først når virksomheden står midt i en krisesituation, at man skal afklare, hvem der bestemmer, eller i hvilken rækkefølge beslutninger træffes.

Det skal være øvet, forankret og accepteret af ledelsen på forhånd. Ellers risikerer man forsinkelser og tab af overblik, der forringer beskyttelsen af virksomhedens kerneinteresser og værdier.

En beredskabsplan er først et reelt og brugbart værktøj, når den er testet i praksis, og kriseorganisationen kan navigere efter den med sikkerhed om at roller, beføjelser og retningen er tydeligt fastlagt.



Alvoren går ofte op for sent

Tager virksomheder ikke arbejdet med beredskabsplaner, krisestyring og forankring af disse alvorligt? Jo, det gør de måske. Men virkeligheden er nok desværre sådan, at alvoren først går op for dem, når de står i situationen.

Jeg har flere gange opleve virksomheder blive komplet handlingslammede, fordi de mister overblikket. Og det kan have store konsekvenser til følge.

Når en virksomhed bliver ramt af et cyberangreb eller driftsforstyrrelse er tid altafgørende. Jo længere uret tikker, des større økonomisk tab vil virksomheden opleve.

Omkostningsfuldt at være på bagkant

I itm8 har vi flere gange arbejdet med virksomheder, der ikke havde en beredskabsplan. Og vi har gentagende gange set, at de har måtte starte forfra på flere niveauer efter at være blevet ramt af et angreb eller nedbrud.

Det viser tydeligt, at det er langt mere omkostningsfuldt for virksomhederne på bagkant – end hvis de havde prioriteret en plan fra begyndelsen.

Virksomhedens interne forsikring

En beredskabsplan er virksomhedens interne forsikring. Ligesom man forsikrer sig mod tyveri af sit indbo – så bør man også forsikre sig mod digitale trusler og driftsnedbrud.

Spørgsmålet er blot, om forsikringen er god nok.

Uden den rette krisestyring og beredskabsplan er virksomheden ekstra sårbar overfor cybertrusler – for selv små hændelser kan få store konsekvenser, når klare procedurer mangler.

Fra dokument til styringsværktøj

En beredskabsplan må ikke være for kompleks. Når det går galt, skal man ikke først læse 50 sider. Tværtimod skal den fungere som en enkel tjekliste, der skaber overblik og sikrer, at intet bliver glemt.

Planen skal være praktisk, let at handle ud fra og kunne bruges, selv når dokumentet ikke ligger foran en. Den skal skabe struktur i usikkerhed og understøtte hurtige beslutninger med ét formål: at beskytte forretningen.

Når planen bygger på klare, gennemprøvede elementer, bliver den ikke bare et dokument – men et aktivt styringsværktøj, der hjælper ledelsen med at beskytte drift, økonomi, lovkrav og omdømme.

Beredskabet er først stærkt, når man afprøver det

Mange virksomheder føler sig trygge, når de har en beredskabsplan på plads. Men arbejdet stopper ikke dér. Det afgørende er at teste planen i virkeligheden.

Først gennem træning og realistiske øvelser viser det sig, om beredskabet kan holde til pres og beskytte de værdier, som er afgørende for virksomhedens fortsatte drift.

En plan kan se solid ud på papiret – men det er først, når den bruges i praksis, man finder ud af, om den faktisk virker.

Hvordan kommer du i gang med en plan?

Rom blev ikke bygget på én dag. Det gør en beredskabsplan heller ikke. Det vigtigste er at starte simpelt. Start med at definere virksomhedens kerneværdier – hvad er jeres kronjuveler, som I skal beskytte?

↓ 7 vigtige elementer i en robust beredskabsplan

- 1

Klare kriterier for hvornår beredskabet aktiveres, og hvem der har mandat til det.
- 2

Præcisering af roller og ansvar i forhold til, hvem der leder indsatsen, hvem der koordinerer, og hvem der træffer beslutninger.
- 3

Et fast beslutningsgrundlag, som gør det muligt at prioritere korrekt, også når der mangler information.
- 4

En struktureret kommunikationslinje, så interne og eksterne parter får rettidig og troværdig information.
- 5

Identifikation af kritiske funktioner og systemer, så fokus og ressourcer er på at beskytte forretningen bedst.
- 6

Handlingskort for centrale scenarier (både worst case og most likely), så indsatsen kan igangsættes med det samme uden forsinkelse.
- 7

En indarbejdet proces for læring og forbedring, så planen hele tiden afspejler virkeligheden og organisationens aktuelle behov.

“Vi er for små til
at være interessante.”
Det udtryk hører
vi ofte.



// OVERVÅGNING OG ALARMER

Overvågning er ikke en luksus – det er sikkerhed

Man kan ikke beskytte det, man ikke kan se. Låse og politikker er godt. Men uden sikkerhedsovervågning er det svært at handle i tide og dokumentere, hvad der egentlig skete. Og så får hackerne altså frit spil.

Af Jesper Vester Sandberg

Manager of Managed Response & CTI, itm8



En bankboks er ikke sikker uden alarm og overvågning

Forestil dig en bankboks. Den er massiv, låst og designet til at modstå alt fra tyveknegte til sprængstof. Men hvad hvis boksen står i et mørkt rum uden alarmer, uden overvågningskameraer og uden nogen, der holder øje med den?

En indbrudstyv ville ikke bare have tid – han ville have hele natten. Ingen alarm ville gå i gang. Ingen vagt ville reagere. Boksen kunne være brudt op og tømt, uden nogen opdagede det før langt senere. Og når man endelig opdager det? Ja, så er det for sent.

Det samme gælder virksomheders IT-infrastruktur. De fleste virksomheder har “bankbokslåsen” på plads: firewall, antivirus og adgangskontrol. Men låsen siger ikke noget, hvis den brydes. Den ringer ikke efter hjælp, den dokumenterer ikke, hvad der skete, og den peger ikke på, hvor næste svaghed er.

Et angreb kan se harmløst ud

Moderne angreb er sjældent et stort brag. De forløber stille, i flere trin og ligner legitim drift: en kompromitteret konto, en ny mail-regel, et usædvanligt login midt om natten, et massivt download fra et cloud-drev.

Hver hændelse kan se harmløse ud alene. Værdien opstår, når du ser mønsteret og reagerer, før skaden udvikler sig til noget uoverskueligt. Her kommer overvågning ind i billedet. I praksis er det forskellen mellem “vi tror, det gik godt”, og “vi ved, hvad der skete, og vi fik også handlet i tide.”

Svagheder kommer i alle (firma)størrelser

“Vi er for små til at være interessante.” Det udtryk hører vi ofte. I dag er de fleste angreb automatiserede og leder efter svagheder – ikke firmastørrelse.

En offentlig eksponeret administrationsportal, en genbrugt adgangskode, en server, der ikke er opdateret eller udstyr uden ejerskab, der både er gemt og glemt. Det er længe nok.

For angriberen er en mindre virksomhed ofte et nemt mål: der er færre øjne på loggene, færre processer og hurtigere afkast.

Overvågning handler derfor ikke om at være “store nok”, men om at have syn, sans og gennemsigtighed i sit eget miljø.



Kan man undvære monitorering?

Selvfølgelig. Også forretningsmæssigt? Ja, men kun hvis man accepterer blinde vinkler og længere nedetid som vilkår. Uden overvågning er det svært at opdage angreb tidligt, dokumentere hændelsesforløbet overfor kunder og myndigheder eller lære af nærvæd-hændelser.

Når ingen holder øje, får hackerne frit spil

Men hvad er forskellen egentlig på at overvåge og ikke overvåge sit miljø?

Lad os tage et eksempel på et typisk forløb uden overvågning:

En medarbejder falder for en troværdig phishing-mail. Angriberen opretter en mail-regel, der skjuler bestemte svar og udvider langsomt adgangen, mens data tappes i små bidder. Intet går i rødt, for ingen eller intet kigger efter sammenhængen. Først da en kunde klager over en falsk faktura, starter jagten baglæns – på mavefornemmelse og fragmenter af data, der er spredt rundt i forskellige portaler.

Kontrasten til et overvåget miljø er klar: Unormale logins og nye mail-regler udløser alarm, adgang spærres og hændelsen håndteres og kunden kontaktes.

Begræns omfanget og skaden

Med overvågning kan du forkorte tiden fra kompromittering til opdagelse og samtidig begrænse omfanget, når noget går galt. Det kan have stor betydning for, hvor omfattende en hændelse bliver – både i forhold til ressourcer og økonomi.

Overvågning kan også være med til at skabe et indblik i konfigurationsfejl. En servicekonto, der er udløbet, en adminkonti, der ved en fejl er sat op til at håndtere en service, eller sågar en printerkonfiguration, der er gået amok på netværket. Det er alt sammen set før.

Sådan kommer virksomheder nemt i gang med overvågning

Når man skal i gang med overvågning, er det vigtigt at starte med de mest værdifulde kilder. Det kan f.eks. være Microsoft 365, identiteter, endpoint-beskyttelse, firewall/VPN og forretningskritiske systemer.



3 steps til at komme i gang

1. **Definér få, skarpe alarmer:** Det kan f.eks. være logins fra nye geografier uden for arbejdstid, oprettelse af lokale admin-konti, masse-download fra cloud, nye mail-regler, trafik mod kendte ondsindede domæner eller kendte og farlige applikationer.
2. **Aftal roller på forhånd:** Hvem afviser adgang, hvem kontakter brugeren, hvem dokumenterer, hvornår eskaleres der og til hvem? Hvilken del håndteres internt og eventuelt eksternt?
3. **Byg videre:** Fortsæt udviklingen, få flere logkilder ind og få oprettet nogle standarder for de hyppigste hændelser.

Overvågning omsætter signaler til handling

Værdien af at overvåge sin virksomheds systemer er ikke kun teknisk. Overvågning giver både governance og ro i maven. Man dokumenterer hændelser, viser rettidig omhu over for kunder, leverandører og ledelse – og målretter sine investeringer, der hvor risikoen faktisk ligger. Det styrker tilliden både internt og eksternt, og gør sikkerhed til en disciplin, der måles og styres i stedet for en bekymring, der skubbes foran sig.

I en tid hvor angreb ikke længere er et spørgsmål om hvis, men hvornår, er overvågning en nødvendighed. IT-sikkerhed skal ikke bare være en låst dør. Den skal være en overvåget, alarmbeskyttet, reaktionsparat bankboks – med kameraer der virker, og folk der reagerer.

Konklusionen er enkel: Man kan ikke beskytte det, man ikke kan se. Låse og politikker er nødvendige, men uden øjne og reaktion forbliver de tavse. Sikkerhedsovervågning i øjenhøjde har en tydelig værdi, fordi den omsætter signaler til handling i tide. For en virksomhed er det ikke luksus. Det er driftssikkerhed, dokumentation og handlekraft i samme pakke.

19 % af danske virksomheder overvåger kun deres IT-miljø inden for normal åbningstid.

15 % overvåger slet ikke.

Kilde: itm8 Cyber Security Survey 2025

// QUIZ

Hvor god er din viden om IT-sikkerhed?

Test din viden i 10 spørgsmål om sandt eller falsk.
Du kan se de rigtige svar på side 34.

#1

Phishing-angreb kan kun ske via e-mail.

- ☐ Sandt
☐ Falsk

#2

To-faktor-godkendelse eller multifaktor-godkendelse gør det sværere for hackere at få adgang til dine konti?

- ☐ Sandt
☐ Falsk

#3

Et stærkt kodeord bør indeholde mindst 14 tegn – både store og små bogstaver, tal og symboler.

- ☐ Sandt
☐ Falsk

#4

Antivirus-software er kun nødvendigt på computere og ikke på mobile enheder.

- ☐ Sandt
☐ Falsk

#5

Hvis du kun besøger 'sikre' og kendte hjemmesider, behøver du ikke bekymre dig om malware.

- ☐ Sandt
☐ Falsk

#6

Offentlige WiFi-netværk er sikre at bruge til alle slags aktiviteter, så længe du ikke deler kodeord.

- ☐ Sandt
☐ Falsk

#7

Ransomware-angreb låser filerne på en computer og kan kræve løsepenge for at frigive dem.

- ☐ Sandt
☐ Falsk

#8

En firewall kan forhindre uautoriseret adgang til et netværk.

- ☐ Sandt
☐ Falsk

#9

Software-opdateringer er ikke vigtige – medmindre der tilføjes nye funktioner.

- ☐ Sandt
☐ Falsk

#10

Et databrud betyder altid, at en virksomheds data er blevet slettet

- ☐ Sandt
☐ Falsk



Korrekte svar

#1. Phishing-angreb kan kun ske via e-mail.
Falsk

Phishing bliver ofte brugt om angreb via e-mail – men det er faktisk et overordnet begreb for forskellige typer angreb. SMS-angreb kaldes smishing og angreb via opkald kaldes for vishing.

#2. To-faktor-godkendelse eller multifaktorgodkendelse gør det sværere for hackere at få adgang til dine konti? **Sandt**

Tofaktorgodkendelse tilføjer et ekstra lag af forsvar mod den stigende mængde af IT-angreb ved at styrke loginsikkerhed.

#3. Et stærkt kodeord bør indeholde mindst 14 tegn – både store og små bogstaver, tal og symboler. **Sandt**

Det stærkeste kodeord er dog, hvor brugeren ikke selv skal indtaste en traditionel adgangskode, men gør brug af en autentifikationsmetode for ekstra sikkerhed.

#4. Antivirus-software er kun nødvendigt på computere og ikke på mobile enheder. **Falsk**

Mobile enheder kan også være udsat for malware og phishing. Derfor kan antivirus-software også være nødvendigt på mobile enheder.

#5. Hvis du kun besøger 'sikre' og kendte hjemmesider, behøver du ikke bekymre dig om malware. **Falsk**

Malware kan også ske via annoncer og inficerede filer.

#6. Offentlige WiFi-netværk er sikre at bruge til alle slags aktiviteter, så længe du ikke deler kodeord. **Falsk**

Offentlige Wi-Fi-netværk kan være usikre og åbne for aflytning.

#7. Ransomware-angreb låser filerne på en computer og kan kræve løsepenge for at frigive dem. **Sandt**

Det er dog ikke alle angreb, hvor hackerne er interesseret i penge. De kan også være interesserede i blot at kryptere og offentliggøre ens filer.

#8. En firewall kan forhindre uautoriseret adgang til et netværk. **Sandt**

En firewall er et sikkerhedssystem til dit netværk. Det hjælper med at blokere uønsket eller skadelig trafik fra at komme ind eller forlade dit system.

#9. Software-opdateringer er ikke vigtige – medmindre der tilføjes nye funktioner. **Falsk**

Opdateringer kan også rette sikkerhedssårbarheder.

#10. Et databrud betyder altid, at en virksomheds data er blevet slettet. **Falsk**

Et databrud betyder typisk, at data er blevet kompromitteret, altså tilgået uautoriseret, men det er ikke nødvendigvis blevet slettet.

Hvor mange rigtige fik du?

10 rigtige

Tillykke. Du har helt styr på IT-sikkerhed. Men husker du også at efterleve det?

7-9 rigtige

Du har godt styr på IT-sikkerhed. Men der er plads til forbedring.

4-6 rigtige

Du er på rette vej, men der er meget at lære om IT-sikkerhed endnu.

0-3 rigtige

Av. Det er kritisk. Du har noget at læse op på. Både for din og din virksomheds skyld.



3

AI



på godt og ondt

I dette kapitel ser vi på AI som både en risiko og en ressource i cybersikkerheden. Du får indblik i, hvordan teknologien kan misbruges af angribere – og hvordan den samtidig kan styrke virksomheders forsvar (dog uden at være en løsning i sig selv).

AI i hænderne på hackere – truslerne vi glemmer i AI-hypen

AI giver virksomheder nye muligheder, men den samme teknologi øger samtidig hastigheden og præcisionen i moderne cyberangreb. Når algoritmer kan skrive kode, skabe troværdige phishing-forsøg og manipulere data, bliver AI en katalysator for trusler, der udvikler sig hurtigere end mange organisationer kan følge med. AI forstærker det, der allerede virker – både for angribere og forsvarere – og derfor kræver den nye virkelighed et skarpt blik på risici, ansvar og forberedelse.

Læs artiklen af Johnni Meldgård Rude på side 38.

AI er et forsvarsværktøj – men ikke nok til at stoppe cyberangreb

Når flere små og mellemstore virksomheder fristes af "one-click-løsninger", overser de, at AI både kan fejlvurdere trusler og falde bagud, når angribere skifter taktik. AI kan styrke virksomheders forsvar, men teknologien kan ikke erstatte den menneskelige dømmekraft, der er nødvendig i pressede og forretningskritiske situationer. AI er et stærkt værktøj – men kun som supplement til mennesker, der forstår konteksten, kan prioritere rigtigt og handle hurtigt, når det gælder.

Læs artiklen af Erik Martin Lilienthal Bandholm på side 42.

// AI-ANGREB

AI i hænderne på hackere – truslerne vi glemmer i AI-hypen

AI-teknologien effektiviserer processer, genererer tekst og analyserer data hurtigere end nogensinde før. Men udviklingen har også en bagside. For de samme værktøjer, der kan løfte effektiviteten i en virksomhed, kan misbruges af hackere til at øge tempoet, præcisionen og omfanget af deres angreb. Spørgsmålet er derfor ikke længere, om AI bliver en del af trusselsbilledet – men hvordan du forbereder din virksomhed på det?

Af Johnni Meldgård Rude
Security Director, itm8



Den teknologiske hockey stick-effekt

De seneste fem år har den teknologiske udvikling taget fart som aldrig før. Vi befinder os midt i en hockey stick-effekt, hvor teknologien udvikler sig eksponentielt. Og allerede nu oplever vi, at cyberkriminelle aktivt anvender AI til at understøtte deres kriminelle handlinger.

Og selvom mange virksomheder stadig kun bruger AI til at skrive mails eller skabe overblik i data, er det kun begyndelsen. Om få år vil AI ikke bare assistere os passivt – AI vil agere, forudsige og tilpasse sig. Og den samme udvikling gælder også for dem, der udnytter teknologien til onde formål.

Fra “narrow AI” til “tomorrows AI”

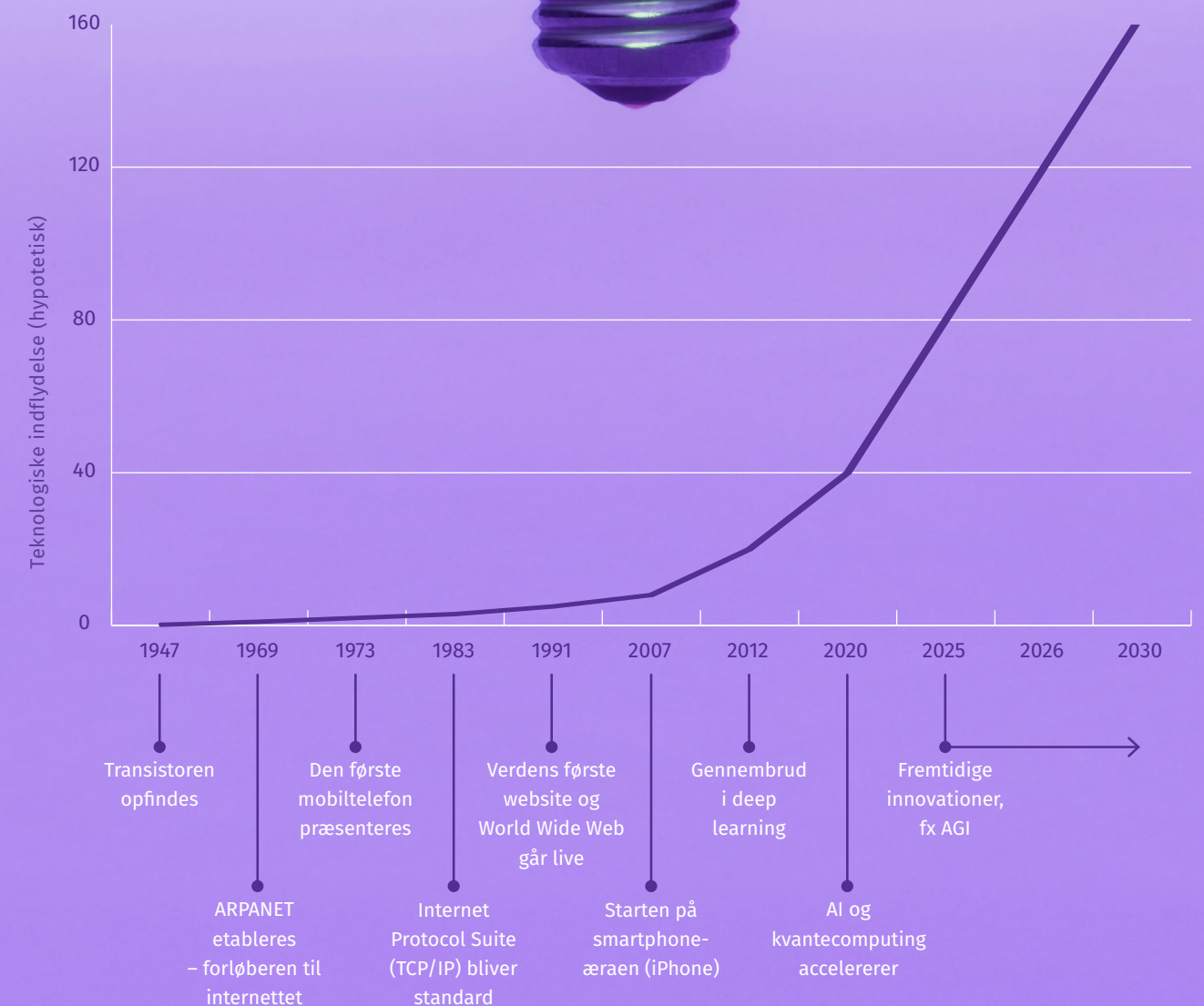
De fleste virksomheder arbejder i dag med “narrow AI”, der anvendes til afgrænsede opgaver som sprogforståelse og billedgenkendelse.

Forskningen bevæger sig dog mod “Artificial General Intelligence” (AGI), som kan lære og handle på tværs af domæner – med både større innovationspotentiale men samtidig med en højere risiko for misbrug.

Hvor “narrow AI” kun kan misbruges inden for sit formål, kan AGI anvendes bredt og reagere selvstændigt. Fremtidens angreb kan derfor orkestreres af algoritmer, der selv optimerer taktik og timing.

Risikoen flytter sig fra menneskelig intention til systemisk adfærd, hvor et kompromitteret AGI-system kan lære af fejl og forbedre sin evne til at undgå detektion.

Når AI integreres i beslutningsprocesser, bliver sikkerhed et spørgsmål om at beskytte selve beslutningskraften.



AI giver hackerne mere fart på

Cybertruslen har udviklet sig fra simple angreb mod enkeltpersoner til professionelle og automatiserede metoder, der går efter selve forretningens grundstøjtje og hvor profit – til de kriminelle – er et meget centralt element.

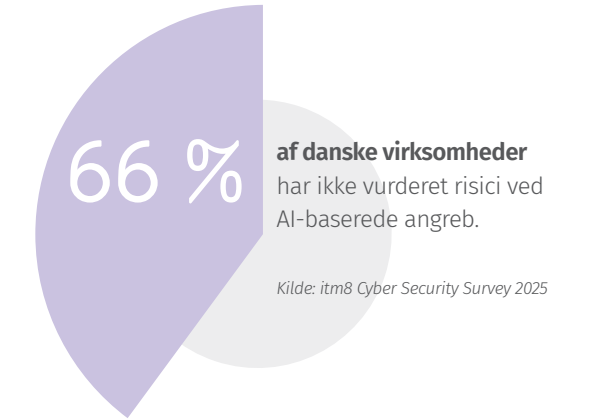
Vi lever i en tid, hvor omkostninger relateret til cyberkriminalitet og angreb svarer til verdens 3. største økonomi. 10.500 milliarder dollars¹. Så mange penge er involveret på den globale spilleplade i 2025. Cyberangrebet ”notPetya”, der i 2017 blandet flere ramte virksomheden Mærsk, viste, hvordan en global virksomhed kan blive lagt ned på få minutter – og hvordan konsekvenserne rækker langt ud over teknikken.

Med AI i værktøjskassen får hackerne nu endnu mere fart på. AI ændrer ikke alt – men den forstærker alt, hvad der allerede virker. Hackere anvender allerede generativ AI til at optimere tekst, kode og måludvælgelse. Phishing-angreb via e-mail bliver mere troværdige, misinformation spredes hurtigere, og selv simple svindelforsøg bliver sværere at opdage.

AI som våben – sådan udnytter hackerne teknologien

Hackere bruger i stigende grad metoder som ”dataforgiftning”, ”støjinjektion” og ”undvigelsesangreb” til at manipulere og snyde AI-agenter og chatbots. Ved at manipulere data som modellerne bliver trænet på eller ved at holde sig lige under alarmgrænserne, forsøger hackerne at få AI til at overse reelle trusler.

Denne form for angreb viser, at AI ikke blot er et nyt og innovativt værktøj for os med gode intentioner – men også et nyt sårbart led i sikkerhedskæden.



1) Kilde: Cybercrime Magazine artikel ”Cybercrime To Cost The World \$10.5 Trillion Annually By 2025”

Andre typer af AI-relaterede angreb

AI ændrer ikke blot måden, vi arbejder på – den ændrer også, hvordan angreb planlægges, udføres og skjules. Hvor cyberkriminalitet tidligere krævede teknisk kunnen og tid, kan AI nu automatisere og skalere angreb med hidtil uset hastighed og præcision.

Her er fem eksempler på, hvordan teknologien allerede bruges som katalysator for nye og mere avancerede trusselsformer:

- 1. **Automatiserede angreb:** Generativ AI gør det muligt for hackere at skabe troværdige mails, tekster og kode på få sekunder.
- 2. **Måltrettede social engineering-angreb:** AI kan analysere offentligt tilgængelige data og skabe ekstremt personlige svindelforsøg. Resultatet? BEC-angreb (Business Email Compromise) bliver mere sofistikerede, og phishing bliver næsten umulig at skelne fra virkelighed.
- 3. **AI uden filtre**
Dark web-fora bugner i dag af generative AI-modeller i form af GPT’er (Generative Pre-trained Transformers), der bevidst er trænet uden etiske begrænsninger. De bruges til alt fra phishing-kampagner til kodegenerering af malware.
- 4. **Deepfakes og misinformation**
AI bruges til at producere falske lyd- og videooptagelser, som kan misbruges til afpresning eller scam-opkald. Når virkeligheden kan manipuleres på lyd og billede, bliver tillid en af de største sikkerhedsudfordringer i den kommende AI-æra.
- 5. **Statslige aktører og påvirkningskampagner**
AI bliver også brugt i geopolitisk kontekst – til at sprede misinformation, påvirke valg og destabilisere økonomier. Her er målet ikke penge men magt.

Når chatbotten bliver virksomhedens ansvar

Anvendelsen af AI vil medføre nye trusler og risici, vi som virksomhedsledere og medarbejdere skal forholde os kritiske til – også uden for cybersikkerhedens kerneområder.

Et eksempel er Air Canada-sagen, hvor en chatbot udviklet til at yde kundesupport, gav en kunde forkert information om refusion ved køb af en flybillet. Flyselskabet afslog i første omgang at betale refusion, hvilket kunden klagede over, og til slut anmeldte til de canadiske myndigheder.

Da sagen blev behandlet i retten, fastslog domstolen, at chatbotten var en lovlig og ansvarlig repræsentant for virksomheden – og Air Canada måtte betale erstatning.

Pointen er klar: Når AI handler på dine vegne, har du stadig ansvaret.

42 % af danske virksomheder har ikke retningslinjer for, hvordan AI må bruges i virksomheden.

Kilde: itm8 Cyber Security Survey 2025

AI forstærker både det gode og det onde

AI ændrer spillereglerne – ikke fordi teknologien er ond, men fordi den forstærker både det gode og det onde. Hackere får stærkere værktøjer, men virksomheder får også nye muligheder for forsvar. Forskellen ligger i, hvem der forstår at bruge teknologien klogest – og hvem der reagerer for sent.

AI bliver i fremtiden ikke blot et værktøj – det bliver en medspiller i både forsvar og angreb. Spørgsmålet er, om din organisation er klar til at styre den, før nogen andre gør det for dig?

↓ Sådan forbereder du dig på en mere intelligent virkelighed

- #1. **AI skal ikke frygtes – men styres.** Og det kræver, at virksomheder tager teknologien alvorligt som en del af deres sikkerhedsstrategi.
- #2. **Brug AI med omtanke** – forstå teknologien og de risici, der følger med.
- #3. **Træn medarbejderne** – gør AI-relaterede trusler til en del af jeres awareness-program.
- #4. **Hold styr på fundamentet** – AI er ikke et quickfix; sikkerhed starter stadig med det basale.
- #5. **Overvåg jeres AI-løsninger** – behandl dem som enhver anden systemkomponent med ansvar, logging og kontrol.
- #6. **Integrér cybersikkerhed i innovationen** – nye muligheder kræver nye sikkerhedsvaner.

// AI SOM CYBERFORSVAR

AI er et forsvarsværktøj –men ikke nok til at stoppe cyberangreb

Kunstig intelligens er blevet et vigtigt redskab i kampen mod cybertrusler. Men teknologien kan ikke stå alene. Den kan analysere mønstre og sandsynligheder – men ikke erstatte menneskelig erfaring og dømmekraft, som er afgørende egenskaber, når kritiske beslutninger skal træffes hurtigt.

Af Erik Martin Lilienthal Bandholm
Partner, Cyber Defence Center, itm8



De cyberkriminelle udpeger "lette" mål

Flere danske virksomheder bliver ramt af cyberangreb. Mange af de cyberangreb er målrettet dem, der er lettest at ramme: små og mellemstore virksomheder med begrænsede ressourcer.

Samtidig bliver de cyberkriminelle dygtigere og mere kreative. Det stiller store krav til ens cyberforsvar.

Derfor ser flere virksomheder lige nu i retning af AI som svaret på den udfordring og de trusler, de er stillet overfor. Men kan AI stå alene? Og er det er uden risiko at overlade sin virksomheds cybersikkerhed til kunstig intelligens?



Tre grunde til ikke at overlade sit cyberforsvar til AI:

1. **Manglende kontekst og dømmekraft:** AI kan ikke forstå den forretningsmæssige betydning af en alarm og kan derfor fejlprioritere kritiske hændelser.
2. **Sårbarhed over for nye metoder:** Når de cyberkriminelle ændrer taktik, risikerer AI at overse trusler, der ikke matcher nye mønstre.
3. **Fejlvurdering:** Enten drukner virksomheden i unødvendige alarmer, eller også overses de reelle angreb. Begge dele er alvorlige risici.

En bekymrende tendens

Vi ser lige nu en bekymrende tendens, hvor flere og flere virksomheder – særligt de små og mellemstore – bliver lovet "AI-løsninger", som med ét klik gør dem sikre. Men det er desværre langt fra virkeligheden.

For nyligt fik mine kollegaer og jeg et lidt specielt udbud i indbakken. Her fremgik det, at i den pågældende virksomhed skulle kunstig intelligens ved 80 % af alarmtilfælde vurdere, om der skulle reageres på alarmen eller ej. Det var virkelig alarmerende (ja, ordspillet var med vilje). Og det er risikabelt af flere årsager.

AI er ikke magi

AI alene er ikke nok til at stoppe eller bekæmpe cyberangreb. Det lyder måske skørt at sige som en, der arbejder både med teknologi og cybersikkerhed. Men det er sandt.

AI er ikke magi. Det er et fantastisk værktøj. Men det erstatter ikke menneskelig dømmekraft, erfaring og forretningsforståelse.

Cybersikkerhed kræver ansvar, dømmekraft – og mennesker

Selvom AI er et effektivt værktøj, kræver cybersikkerhed mere end algoritmer. Det kræver intuition, tillid og menneskelig dømmekraft – især når forretningskritiske beslutninger skal træffes hurtigt - og rigtigt.

Derfor skal vi bruge den kunstige intelligens dér, hvor det giver mening. Feks. ved at lade AI analysere mønstre og sandsynligheder, men overlade forståelsen og ansvaret til rigtige mennesker.

Det er også en af grundene til, at vi i itm8 altid har mennesker tilgængelige døgnet rundt. Ikke bare for at overvåge – men for at forstå og handle.

Mennesker og træning



som forsvarslinje



I dette kapitel ser vi på sikkerhedskultur som en central del af virksomheders sikkerhedsniveau. Hvordan gode vaner, tydelige ritualer og en kultur af verificering kan styrke organisationens modstandskraft. For når teknologi, mennesker og processer arbejder sammen, bliver awareness en reel del af forsvaret og ikke bare træning på papir.

Sikkerhed bliver først skabt, når teknologi, mennesker og processer arbejder sammen

Virksomhederne har hjemmebanefordel, fordi de ved præcis, hvilke systemer og data der er kritiske – men kun hvis fundamentet er i orden, og processerne er på plads. Når struktur, overblik og risikovurdering mangler, forsvinder fordelene, og teknologien står alene uden den kultur og de arbejdsgange, der får sikkerheden til at fungere i praksis.

Læs artiklen af Johnni Meldgård Rude på side 46.

Fremtidens awareness handler om gode ritualer og verificering

Fremtidens awareness handler mindre om at kunne spotte en phishing-mail og langt mere om de små ritualer, der skaber sikker adfærd i hverdagen. Når truslerne bliver mere sofistikerede, er verificering, sund tvivl og klare vaner ofte det stærkeste værn. Awareness gør først en forskel, når den bliver en del af kulturen – ikke et årligt kryds i en compliance-boks.

Læs artiklen af Emilie Kaae Riis på side 50.

// EFFEKTIV IT-SIKKERHED

Sikkerhed bliver først skabt, når teknologi, mennesker og processer arbejder sammen

Mange virksomheder tror fejlagtigt, at et enkelt værktøj eller en ekstern service kan lukke sikkerhedshullerne. Men effektiv IT-sikkerhed kræver en tilgang, hvor teknologi, mennesker og processer trækker i samme retning.

Af Johnni Meldgård Rude
Security Director, itm8



Virksomheden har hjemmebanefordelen

De cyberkriminelle vil altid lede efter den letteste vej ind. Derfor målretter de deres indsats mod det svageste led – et uopdateret system, en udvalgt bruger eller en uigennemsigtig proces.

Men midt i svagheden ligger også virksomhedens største fordel: Det er deres banehalvdel, de spiller på. De ved bedre end nogen andre, hvilke systemer og data der er kritiske for at holde forretningen i gang. Den indsigt er ikke blot en fordel – den er fundamentet for enhver bæredygtig sikkerhedsstrategi.

Men hvis de ikke har risikovurderet og beskyttet de mest kritiske områder, går fordelene tabt.

Få orden i penalthuset

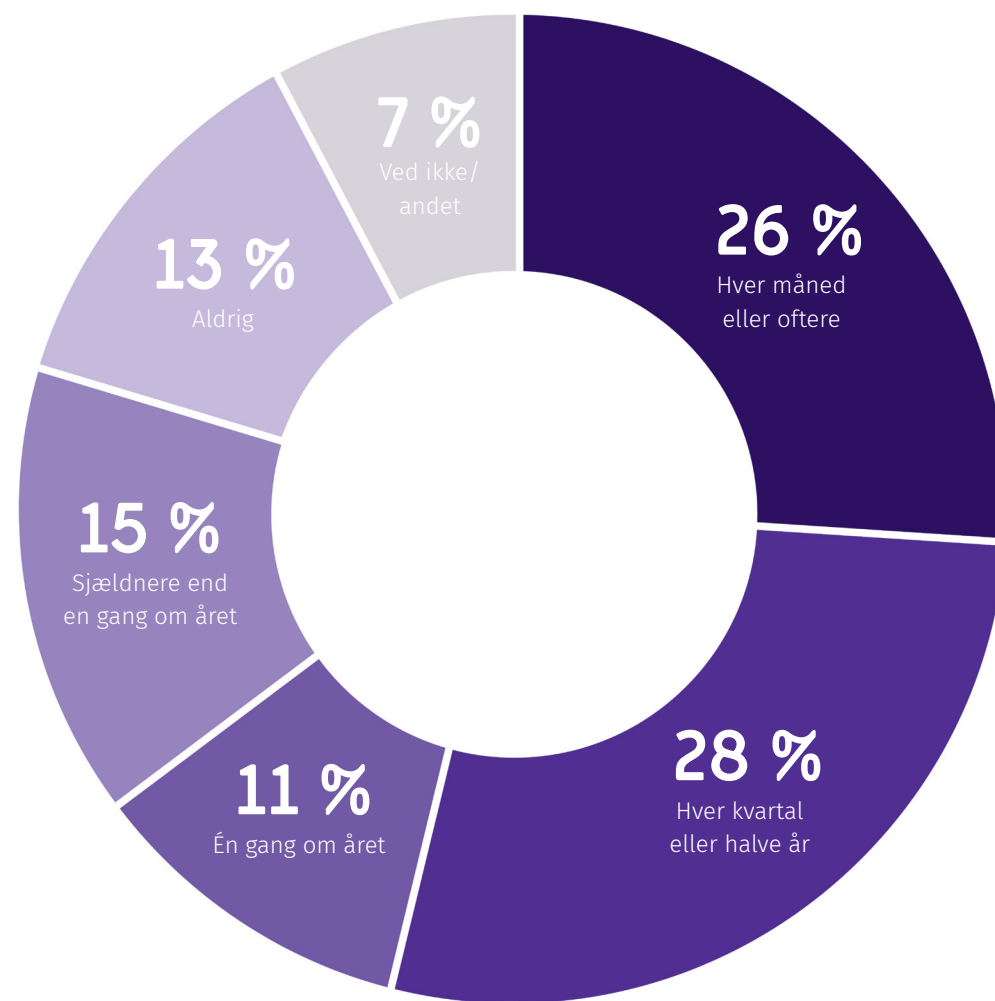
Selv den mest avancerede teknologi kan ikke kompensere for manglende struktur. Hvis drift og opdateringer ikke er sat i system og understøttet af klare processer, opstår der huller, som hackere kan udnytte.

Derfor er første skridt at skabe overblik og risikovurdere systemerne i forhold til forretningen. Når de mest kritiske områder er identificeret, kan man vælge de tiltag, der giver reel værdi.

Men arbejdet stopper (desværre) ikke her. IT-sikkerhed er et kontinuerligt arbejde, der skal genbesøges og forankres i organisationens drift.



Hvor ofte træner danske virksomheder deres medarbejdere i IT-sikkerhed?



Kilde: itm8 Cyber Security Survey 2025

Hvorfor kan man ikke købe sig til IT-sikkerhed?

Mange virksomheder fristes måske til at tro, at IT-sikkerhed kan købes som en færdig pakke eller outsources helt. Men sikkerhed er ikke et produkt på hylden – det er en disciplin, der skal forankres i organisationen. Eksterne løsninger kan sagtens understøtte arbejdet, men det kan aldrig stå alene.

Det afgørende ansvar ligger hos ledelsen. Bestyrelsen og direktionen må have fingeren på pulsen i forhold til forretningens systemer og risici.

For langt de fleste virksomheder er pengene bedre givet ud på at styrke de basale lag – drift, processer og overblik – end på dyre enkelttiltag. Først når fundamentet er på plads, kan investeringer i teknologi skabe reel værdi.

Samspeilet mellem mennesker, teknologi og processer

En stærk sikkerhedsindsats bygger på en balance mellem tre elementer: teknologi, mennesker og processer. Faktisk kræver de mest effektive tiltag ikke særlig store investeringer, men primært tid og engagement fra organisationen selv.

Men det kræver, at man har den rette indsigt i virksomheden, og ved, hvor sårbarhederne er. Derfor kan ansvaret ikke overlades til eksterne partnere alene – ledelsen og medarbejderne skal aktivt involveres.

Teknologi spiller selvfølgelig en vigtig rolle. Men uden klare processer og en sikkerhedskultur blandt medarbejderne, skaber den kun en falsk tryghed.

Man kan købe sig til meget. Men det er først når alle tre elementer arbejder sammen, at virksomheden får et forsvar, der både er robust og tilpasset forretningens virkelighed.

Tre gode råd til at arbejde med IT-sikkerhed

1. **Skab et overblik:** Du kan ikke beskytte det, du ikke kender. Start med at kortlægge systemlandskabet: Hvilke systemer er forretningskritiske, og hvordan er de eksponeret? Det giver et klart billede af, hvor indsatsen skal prioriteres.
2. **Etabler en solid baseline:** Byg et fundament af grundlæggende sikkerhedsforanstaltninger som adgangsstyring, opdateringer og overvågning. Først derefter giver det mening at tilføje mere avancerede løsninger, som passer til jeres branche, nøgleaktiver og risikoprofil.
3. **Gør mennesker til en aktiv ressource:** Medarbejdere kan være den største risiko – men de er også en vigtig del af forsvaret. Prioritér træning og awareness, så alle forstår truslerne og ved, hvordan de skal reagere i praksis.

// SIKKERHEDSTRÆNING

Fremtidens awareness handler om gode ritualer og verificering

Hvordan gør man awareness til mere end et kryds i en compliance-boks? Svaret ligger ikke i flere kurser og at lære at genkende trusler – men at skabe en kultur, hvor det er naturligt at stoppe op, verificere og tage ansvar.

Af Emilie Kaae Riis

Strategic Cyber Risk Advisor, itm8



Awareness er et vigtigt våben mod cyberangreb

Ifølge Verizon starter 60 % af alle IT-sikkerhedsbrud i virksomheder hos en medarbejder². Det er den hårde sandhed. Derfor er det altafgørende, at medarbejderne er trænet til at genkende og håndtere potentielle trusler.

Lige nu ser vi angreb som social engineering, phishing, deepfakes og fysiske brud tordne frem. Men det handler i virkeligheden mindre om teknologi – og mere om udnyttelse af menneskelige mekanismer som tillid, travlhed og autoritetstro.

Måltrettet awareness kan beviseligt reducere risikoen markant, fordi den skaber et fælles sprog, et ansvar og små mentale pauser, hvor vi stopper op og tænker os om, før vi klikker, deler eller giver adgang. Uden den adfærdsmæssige dimension kan selv den bedste tekniske sikkerhedsløsning blive sårbar.

Det handler ikke om at tjekke en compliance-box af

Effektiv awareness bør ikke blot være et e-learning-modul én gang om året – men en målrettet adfældsindsats, der understøtter virksomhedens og medarbejderes evne til at reagere hensigtsmæssigt før, under og efter et cyberangreb.

Det kræver, at træning, kommunikation og beredskab er tilpasset den konkrete virksomhed.

Jeg oplever, at mange virksomheder vælger generiske standard awareness-løsninger for – sat på spidsen – at kunne tjekke en compliance-boks af. Det er på sin vis fuldt forståeligt, for det kan være uoverskueligt, hvor man skal starte, og hvad medarbejderne egentlig har brug for at blive trænet i. Men det er en kortsigtet løsning.



2) Kilde: Verizon Data Breach Investigations Report 2025

28 % af danske virksomheder træner sjældnere end én gang om året eller aldrig.

Kilde: itm8 Cyber Security Survey 2025

Mangler opfølgning, måling og reel forankring

Udfordringen er, at mange – i forsøget på at leve op til lovgivning og standarder – risikerer ikke at få stillet de rette spørgsmål, og dermed mangler en klar strategi for opfølgning (gennemføres træningen overhovedet?), måling (bliver træningen omsat til adfærd?) og reel forankring (kommunikeres forventninger og konsekvenser af adfærd tydeligt?) af sikker adfærd blandt medarbejderne.

Hvis awareness alene implementeres for at opfylde formelle krav, risikerer man derfor en form for awareness-washing, hvor man godt nok kan dokumentere awareness-træning, men potentielt uden reel effekt på adfærd og sikkerhedskultur. Og det er en farlig fælde, fordi medarbejderne ikke bliver tilstrækkeligt klædt på til virkelige situationer, og så står virksomheden stadig med et væsentligt risikogab.

En holistisk og lavpraktisk tilgang til awareness skaber større værdi

Når mange virksomheder vælger at bruge betydelige ressourcer på awareness, bør første skridt være at forsøge at skabe en kultur og forståelse for, at awareness ikke handler om ligegyldige, intetsigende kurser, der bare skal overstås, men om at beskytte virksomheden og medarbejderne. Hvis formålet er tydeligt, bliver det markant lettere at få organisationen med.

Samtidig bør virksomheden afklare sine konkrete behov: Hvilke trusler er mest relevante for os? Hvem er mest udsat? Og hvilken adfærd vil vi gerne ændre? Svarene bør omsættes til få, lavpraktiske greb – f.eks. en enkel step-by-step proces for, hvordan man rapporterer en phishing-mail i virksomhedens systemer, hvad man gør, hvis man er i tvivl, og hvordan man bør handle i dagligdagen.

Ved at vende perspektivet 180 grader kan virksomheden opnå en mere holistisk tilgang til awareness, der skaber reel værdi og giver "valuta for pengene". På den måde lever virksomheden ikke kun op til compliance, den øger også sandsynligheden for, at medarbejderne faktisk kan bruge træningen til noget.

Fysisk sikkerhed er (ofte) en overset del af trusselsbilledet

Når vi taler om awareness, fylder den digitale adfærd ofte mest. Men i mange virksomheder er den fysiske sikkerhed et mindst lige så reelt (og ofte overset) risikoområde.

Grænsen mellem fysisk og digital sikkerhed er blevet mere flydende: Uautoriseret fysisk adgang til bygninger, mødelokaler eller serverrum, mistede laptops, telefoner og dokumenter samt tailgating (at følge andre ind i områder, der kræver adgangs-autentifikation) kan være det fysiske udgangspunkt for et alvorligt sikkerhedsbrud.

Netop derfor giver det mening at betragte fysisk sikkerhed som en integreret del af awareness og ikke som et særskilt spor. Erfaringer fra fysiske social engineering-tests og tailgating-audits viser, at træning har en særlig effekt, når den foregår dér, hvor truslen opstår: ved døren og i receptionen, i åbne kontorområder.

Her kan medarbejderne møde realistiske scenarier, få konkret feedback og modtage vejledning i helt simple handlemønstre for, hvordan de siger fra, rapporterer observationer og håndterer adgangskontrol i praksis.

For virksomheder, der allerede investerer i awareness, er budskabet simpelt: *skærmen er ikke nok*.

I 34 % af danske virksomheder indgår fysisk sikkerhed ikke som en del af cybersikkerhedsstrategien.

Kilde: itm8 Cyber Security Survey 2025

Når awareness bliver til gode ritualer

Fremtidens, og faktisk også nutidens, trusselsbillede betyder, at awareness ikke længere kan reduceres til "kan du spotte en phishing-mail?". Angreb bliver mere troværdige, sprogligt korrekte og målrettede, ikke mindst fordi AI gør det nemmere for angriberne at efterligne sprog, afsendere og interne processer.

Derfor bliver gode ritualer vigtigere end mavefornemmelsen. Og at vi som udgangspunkt verificerer, før vi handler. Et telefonopkald til kollegaen, en kontrol via en anden kanal, et ekstra tjek af kontonummer eller afsender, før vi godkender, betaler eller deler.

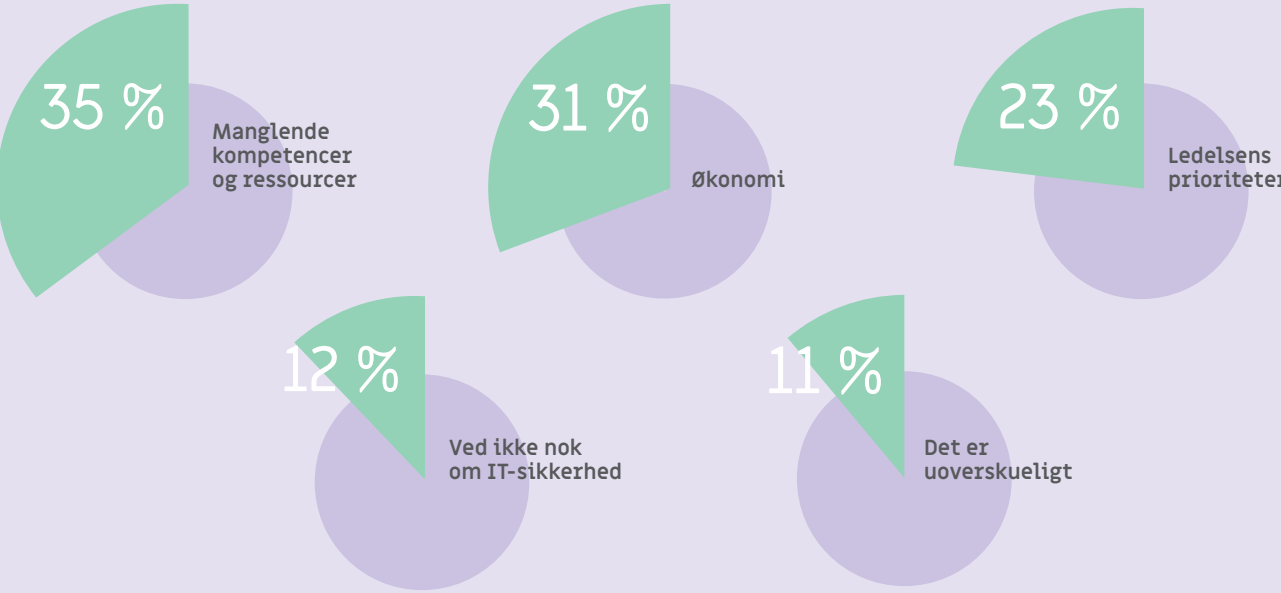
I årevis har vi accepteret ekstra trin for at beskytte vores systemer, såsom krav til stærke passwords og to- og multifaktorgodkendelse. Den samme logik bør gælde for vores adfærd. Verificering, tjek og sund tvivl skal være en form for "*menneskelig multifaktor*", hvor et ekstra trin ikke er irriterende bureaukrati men en indarbejdet sikkerhedsvane.

Det er netop de få, men meningsfulde ekstra trin i adfærd, der i praksis kan være forskellen på et vellykket angreb og en hændelse, der aldrig får lov til at udvikle sig.

3 ting, virksomheder bør prioritere i 2026, når det kommer til awareness

- Gør awareness lavpraktisk og relevant**
Træning skal tage udgangspunkt i medarbejdernes hverdag – ikke i teoretiske scenarier. Det skaber ejerskab og bedre forståelse.
- Byg sikkerhed ind i kulturen**
Skab ritualer, hvor verificering, tvivl og dialog er en naturlig del af arbejdet. Awareness skal leve i hverdagen – ikke kun i e-læringsmoduler.
- Se awareness som et ledelsesansvar**
Awareness er ikke et HR- eller compliance-projekt, men et strategisk ledelsesansvar. Når ledelsen går forrest, prioriterer opfølgning og taler åbent om sikker adfærd, smitter det af på hele organisationen og øger chancen for reel forankring.

Hvad holder danske virksomheder tilbage i forhold til at forbedre IT-sikkerheden?



Cybersikkerhed



i fremtiden

I dette kapitel ser vi frem mod de tendenser, der vil forme cybersikkerheden i de kommende år. Fokus er på, hvordan viden, forberedelse og en stærk sikkerhedskultur bliver afgørende, når truslerne udvikler sig hurtigere end teknologien kan følge med. Det handler ikke om flere værktøjer – men om at forstå, forudsige og reagere, før angrebet rammer.

Cyber Threat Intelligence er forskellen mellem at blive overrasket – og at være forberedt

Når trusselsaktører udvikler sig hurtigere end traditionelle forsvarsmekanismer, bliver viden, analyse og forberedelse en afgørende del af sikkerhedsarbejdet. Cyber Threat Intelligence giver virksomheder mulighed for at reagere før angrebet rammer og gør det tydeligt, hvor virksomheden er mest sårbar, hvilke metoder der er på vej, og hvor indsatsen bør prioriteres. Så man kan gå fra at blive overrasket til at være forberedt.

Læs artiklen af Jacob Krahn og Danni Louis Nielsen Bred Randeris på side 56.

Næste fase i cybersikkerhedsrejsen kræver handling – ikke flere løsninger

Cybersikkerhed handler i fremtiden mindre om at købe nye løsninger og mere om at omsætte viden til konkret handling. Modenhed opstår, når virksomheder kender deres svagheder, tager de første lavpraktiske skridt og bruger sikkerhed som et ledelsesværktøj – ikke kun som en teknisk disciplin.

Tillid, dokumentation og løbende forbedring bliver afgørende konkurrenceparametre, og de virksomheder, der arbejder struktureret og vedholdende, står stærkere i både markedet og hverdagen.

Læs artiklen af Mathias Holdt på side 61.

7 spørgsmål enhver leder bør stille sig selv

Som leder har du ansvaret for at sikre, at IT-sikkerheden er på forkant med både vækst og udfordringer. Derfor er det vigtigt at stille – og svare på – de helt rigtige spørgsmål.

Se spørgsmålene på side 65.

4 gode råd til oprustning af danske virksomheders cybersikkerhed

Der er mange ting at gøre, når det kommer til cybersikkerhed. Her er vores anbefalinger til de fire vigtigste og mest kritiske ting at få styr på.

Se Esbens Kaufmanns fire gode råd på side 66.

// INDSAMLING, ANALYSE OG FORMIDLING AF CYBERDATA

Cyber Threat Intelligence er forskellen mellem at blive overrasket – og at være forberedt

Forestil dig, at vågne mandag morgen til et kaos af utilgængelige systemer, vrede kunder og medarbejdere, der ikke kan udføre deres arbejde. For mange danske virksomheder er det desværre ikke et tænkt scenarie men en realistisk risiko – særligt hvis man ikke arbejder aktivt med Cyber Threat Intelligence. Cyber Threat Intelligence hjælper med at afklare, hvor virksomheden er mest sårbar, og hvor det giver mening at investere – for at kunne opfange truslerne i tide.

Af Jacob Krahn
Security Advisor, itm8

Danni Louis Nielsen Bred Randeris
Head of Security Operations, itm8



Hvad er Cyber Threat Intelligence – og hvorfor betyder det noget?

Cyber Threat Intelligence (CTI) handler i bund og grund om at bruge viden til at tage bedre beslutninger. Det er en proces, hvor man indsamler, bearbejder og analyserer data for at forstå, hvilke trusler der er relevante for netop ens virksomhed – og hvad man kan gøre ved dem.

I stedet for at reagere, når skaden er sket, hjælper CTI virksomheder med at være et skridt foran. Det handler ikke kun om at have firewalls og antivirus på plads, men om at kende modstanderen, forstå deres metoder og kunne genkende faresignalerne, før de bliver til et angreb.

Fra “vi troede, vi var dækket ind” til “vi så det komme”

Lad os tage et fiktivt eksempel med en mellemstor dansk e-commerce virksomhed, der sælger sko. De har investeret i firewalls, endpoint protection og “alt det fancy”. Men deres sikkerhedsteam har ikke fulgt med i udviklingen – de ved ikke, hvad der trender i hackerverdenen, eller hvilke grupper der er aktive netop nu. Og de har ikke noget intelligent system til at informere om nyeste trusler og teknikker.

En kriminel ransomware-gruppe – lad os kalde dem DarkNet Kings – kender alle de nyeste metoder og har endda lavet deres egne. De har ramt en serie af virksomheder, og derfor er deres teknikker blevet kendte.



”Trusselsaktører bliver hele tiden bedre til at udnytte nye teknologier som AI, automatisering og globale angrebsnetværk. Derfor står de virksomheder, der arbejder aktivt med Cyber Threat Intelligence, stærkere – både når angreb rammer, og når de skal forebygges.”

Men direktøren for skovirksomheden er lykkeligt udvidende, da han mandag morgen møder ind til sin virksomhed, der er lammet. Systemerne er nede, kunderne er utilfredse, medarbejderne er frustrerede – og et sikkerhedsteam, der desperat prøver at finde ud af, hvad der ramte dem. Og alle øjne er selvfølgelig på direktøren og IT-chefen.

Et år senere ser situationen anderledes ud. Skovirksomheden har investeret i CTI og fået adgang til analyser, rapporter og netværk, der holder dem opdateret på de seneste trusler. Da DarkNet Kings igen forsøger sig på skovirksomheden, står de klar.

Deres CTI-specialister har allerede opfanget tegn på angreb gennem rapporter fra samarbejdspartnere. Awareness-kampagner har gjort medarbejderne mere opmærksomme. De nye overvågningsregler opfanger truslerne tidligt. Det betød, at angrebet denne gang blev stoppet, før det nåede at gøre skade.

Den skjulte værdi af Cyber Threat Intelligence

Cyber Threat Intelligence er ikke bare et værktøj for teknikere. Det er et beslutningsgrundlag for ledelsen. For når man ved, hvilke trusler der er relevante for ens branche, kan virksomheden prioritere rigtigt – både strategisk og økonomisk. Med andre ord gør CTI det lettere at se, *hvor virksomheden er mest sårbar, og hvor det giver mening at investere.*

Cyberangreb bliver mere komplekse, og grænsen mellem kriminelle og statssponsorerede aktører udviskes. Derfor er reaktive sikkerhedsforanstaltninger ikke længere nok. Cyber Threat Intelligence kan være forskellen mellem at blive overrasket – og at være forberedt.

Derfor er tiden inde nu

De fleste angreb i dag bruger kendte metoder og værktøjer – men tempoet i udviklingen stiger. Nye teknikker og kampagner opstår nærmest dagligt. Med Cyber Threat Intelligence får virksomheder et redskab til at overvåge, analysere og formidle den viden, der betyder noget for netop deres forretning.

Det er ikke bare endnu en sikkerhedsinvestering. Det er en investering i viden, beslutningskraft og ro i maven – ikke kun på et strategisk niveau men også operationelt.



Tre spørgsmål, du som leder bør stille dig selv, før du investerer i Cyber Threat Intelligence:

1. **Ved vi, hvilke trusler** der er mest relevante for vores virksomhed lige nu?
2. **Har vi et system** eller samarbejde, der løbende overvåger og formidler ny viden om trusler og deres metoder?
3. **Har vi testet**, at vi er klar, hvis den nyeste trussel forsøger at bryde ind? Eller er vi reaktive hvis angrebet er ude?

Hvordan implementerer man Cyber Threat Intelligence i praksis?

Processen foregår typisk ved hjælp af **fem steps**:

#1



Retning og målsætning

Definer hvad der er vigtigt at vide for at foretage en beslutning.

#2



Indsamling

Indsaml rå data fra relevante kilder.

#3



Bearbejdning

Processér indsamlet data til brugbare datapunkter og information.

#4



Analyse

Lav datapunkter og informationen til intelligence, hvilket besvarer spørgsmålene.

#5



Formidling

Levér disse insights til interessenter og brug deres feedback til at raffinere cycles senere.

// EN BEVIDST KULTUR

Næste fase af cybersikkerhedsrejsen kræver handling – ikke flere løsninger

Cybersikkerhed har for alvor fået sit gennembrud som et ledelsesanslgende. Mange virksomheder har allerede indført politikker, procedurer og tekniske løsninger, der øger sikkerheden. Det er en vigtig udvikling. Men i 2026 er opgaven en anden: at omsætte det til handling.

Af Mathias Holdt
Director, Strategic Cyber Risk Advisory, itm8



Det handler om at kende sine svagheder og forbedre sig

For mange små og mellemstore virksomheder kan cybersikkerhed virke som et tungt og teknisk emne. Men i virkeligheden handler det om noget meget jordnært: at kende sine svagheder, tage hånd om dem og hele tiden forbedre sig lidt.

Hvert skridt tæller. Det vigtigste er ikke, hvor langt man er, men at man rykker sig.

Hvor de seneste år har handlet om at reagere på nye krav og direktiver, handler den næste fase om at forankre sikkerhed som en del af den måde, man driver virksomhed på.

Modenhed betyder ikke flere systemer eller akademiske analyser. Det betyder, at man arbejder med cybersikkerhed i et tempo og på et niveau, der giver mening i hverdagen.

Tillid og dokumentation er blevet konkurrenceparametre

I år vil det blive endnu tydeligere hvilke virksomheder, der arbejder struktureret med deres sikkerhed, og hvem der ikke gør.

Kunder og samarbejdspartnere forventer i stigende grad, at man har styr på sine data og sin drift. Tillid bliver derfor et konkurrenceparameter. Når en kunde vælger leverandør, vælger de også det ansvar, der følger med. Den virksomhed, der kan dokumentere, at den har styr på sin cybersikkerhed – på et niveau der passer til dens størrelse og rolle – står stærkere i markedet.

Det betyder ikke, at alle skal have samme ambitionsniveau. For nogle handler modenhed om at få styr på de mest oplagte risici: adgangskoder, backup og beredskab. For andre handler det om at teste, hvordan man reagerer, når noget går galt. Fælles for dem alle er, at man gør noget aktivt ved det.



Start med de lavthængende frugter

En moden tilgang til cybersikkerhed begynder med en ærlig vurdering af, hvor man står i dag. Mange tror, de har styr på sikkerheden – men uden jævnlige tests og gennemgange, bygger man ofte på antagelser.

Et godt udgangspunkt er derfor at tage de lavthængende frugter: sikre, at systemer bliver holdt opdaterede, at medarbejdere ved, hvordan de skal reagere på mistænkelige mails, og at virksomheden kan genskabe data, hvis noget går galt. Det kræver hverken store investeringer eller avancerede processer – men det kræver ledelsesmæssig opmærksomhed.

Når det grundlæggende er på plads, kan man bygge videre. En virksomhed, der jævnligt tester sin beredskabsplan eller laver små øvelser, hvor ledelsen skal træffe beslutninger under pres, bliver hurtigt mere robust. Man opdager, hvor kommunikationen halter, og hvad der virker i praksis. Den slags læring kan ikke købes – den skal opnås gennem erfaring.

Fra teknisk detalje til et spørgsmål om tillid

Virksomheder, der tager cybersikkerhed alvorligt viser ansvar og styring. Forventningerne fra markedet vokser. Flere brancher oplever allerede, at kunder beder om dokumentation for, hvordan deres data beskyttes, eller hvordan leverandøren vil reagere ved et angreb.

Det, der tidligere var en teknisk detalje, er i dag et spørgsmål om tillid. Og i takt med at digitalisering bliver en forudsætning for at drive forretning, bliver en moden cybersikkerhed også en konkurrencefordel.

Derfor er 2026 året, hvor cybersikkerhed bevæger sig fra at være et nødvendigt krav til at blive et aktivt argument for professionalisme. De virksomheder, der kan vise, at de tager sikkerhed alvorligt – ikke bare med ord men med handling – vil skille sig ud. De virksomheder demonstrerer det i praksis. Og det skaber tryghed for både kunder, ejere og medarbejdere.

Fremdrift og prioritering viser modenhed

For ledelsen i en virksomhed er det vigtigste budskab, at arbejdet med cybersikkerhed ikke behøver at være perfekt for at være værdifuldt og værdiskabende. Tværtimod. Modenhed handler om fremdrift og prioritering. Man kan tage et skridt ad gangen – og hvert skridt giver både erfaring og effekt.

Det kan begynde med noget så simpelt som at definere, hvem der gør hvad, hvis systemerne går ned, eller at få en ekstern vurdering af, hvor man er mest sårbar.

Sikkerhed er at tage hånd om sin forretning

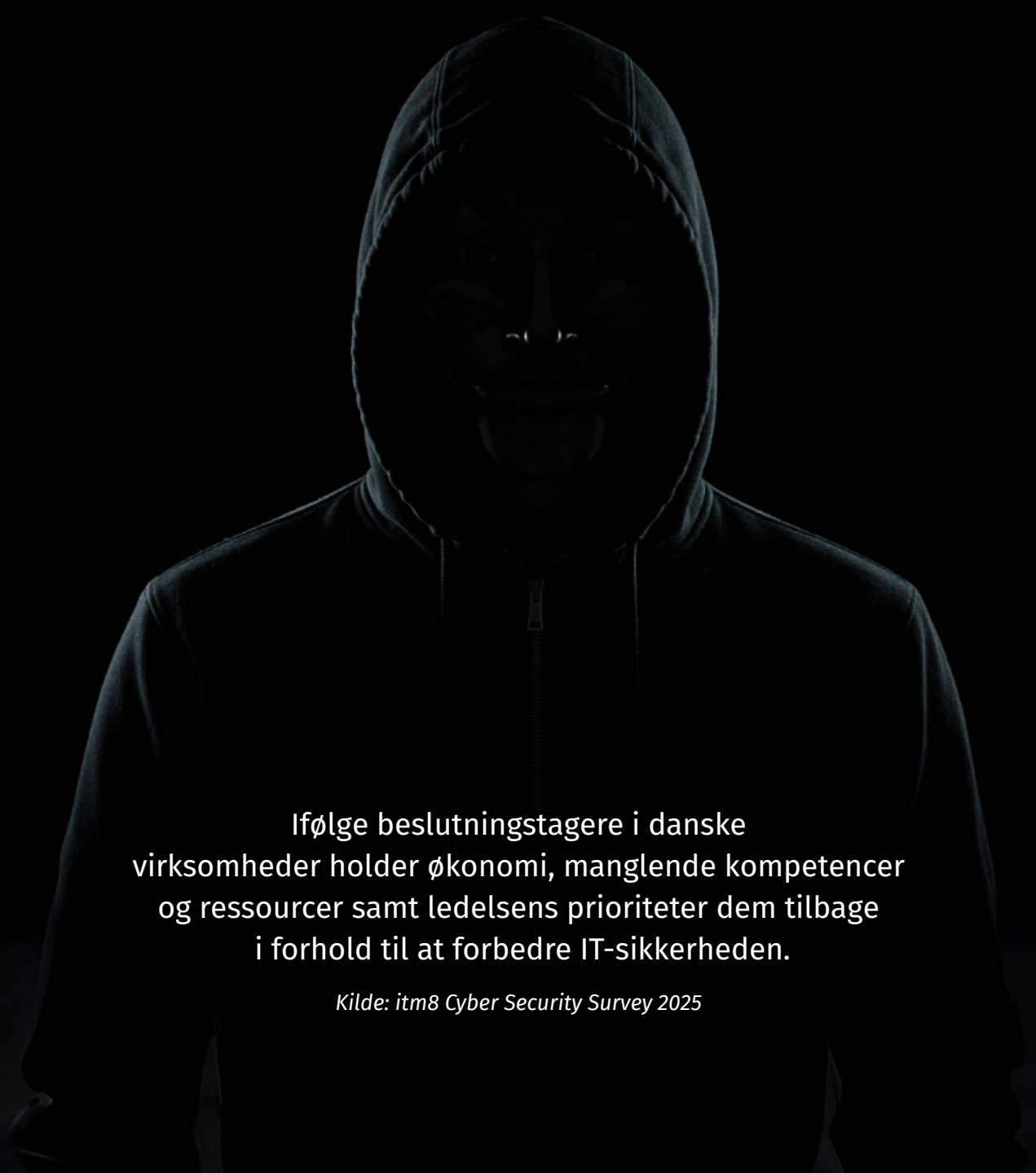
Cybersikkerhed er i sin natur et område, der aldrig bliver færdigt. Truslerne udvikler sig, teknologien ændrer sig, og lovgivningen følger efter. Derfor er det tydeligt, at de virksomheder, der arbejder vedholdende med cybersikkerhed, lærer at håndtere forandringen som en del af hverdagen. De bliver bedre til at reagere, hurtigere til at gendanne og stærkere i deres relation til kunderne.

Den næste fase i cybersikkerhedsrejsen handler derfor ikke om bare at købe flere løsninger men om at skabe en bevidst kultur. En kultur, hvor ledelsen går forrest, hvor medarbejdere ved, hvorfor sikkerhed betyder noget, og hvor man tør lære af sine fejl.

2026 er året, hvor modenhed i cybersikkerhed bliver et synligt tegn på kvalitet. Ikke som en konkurrence i teknologi men som et udtryk for ledelsesstyrke og ansvarlighed.

De virksomheder, der begynder at tænke sådan, tager ikke bare hånd om deres sikkerhed. De tager hånd om deres forretning.

Cybersikkerhed er ikke længere et IT-projekt men et vigtigt ledelsesansvar.



Ifølge beslutningstagere i danske virksomheder holder økonomi, manglende kompetencer og ressourcer samt ledelsens prioriteter dem tilbage i forhold til at forbedre IT-sikkerheden.

Kilde: itm8 Cyber Security Survey 2025

På en modenhedsskala
fra 1-5 vurderer
de adspurgte
virksomheder deres
modenhed til **3,4**

Kilde: itm8 Cyber Security Survey 2025

// GUIDE TIL BEDRE IT-SIKKERHED

7 spørgsmål enhver leder bør stille sig selv

En leder har ansvaret for at sikre, at IT-sikkerheden er på forkant med både virksomhedens vækst og de udfordringer, der følger med. For at gøre dette effektivt, er det vigtigt at stille de rigtige spørgsmål og få de rette svar på plads.

↓ Her er **7 essentielle spørgsmål**, du bør stille dig selv:

- 1 Er IT-sikkerhed forankret på ledelsesniveau i virksomheden?
- 2 Hvornår har vi sidst vurderet hvilke systemer, der er mest kritiske?
- 3 Er IT-sikkerheden fulgt med virksomhedens udvikling?
- 4 Er vores IT-systemer altid opdaterede?
- 5 Hvor ofte tester og verificerer vi vores backup-løsning?
- 6 Hvordan er vi dækket af vores forsikring, hvis vi bliver angrebet?
- 7 Hvad gør vi, hvis vi bliver ramt af et cyberangreb?

// ANBEFALING

4 gode råd til oprustning af danske virksomheders cybersikkerhed

Det var årets cyberrapport 2026. Vi håber, at du har fået nogle nye perspektiver undervejs. Der ér mange ting, man bør overveje og gøre, når det kommer til cybersikkerhed. Men husk på, at lidt også har ret – og at det handler om at starte et sted og være i gang.

Hvis jeg her på falderebet skulle anbefale de fire vigtigste og mest kritiske ting at få styr på, ville det være:

#1

Beskyt dine kritiske aktiver

Identificér dine vigtigste "kronjuveler" – f.eks. systemer der er kernen af din virksomhed.

#2

Test systemernes styrke

Test, hvor godt jeres systemer er beskyttet, ved at udføre regelmæssige sikkerhedstests.

#3

Forbered dig på krisen

Beslut jer for, hvad I gør, og hvem du ringer til i tilfælde af en krisesituation.

#4

Øv beredskabet

Øv jer på jeres beredskabsplan (og hvis I ikke har en – så start med at få lavet en).

God arbejdslyst.

Venlig hilsen

Esben Kaufmann
Executive Partner, itm8

// SPØRGEUNDERSØGELSE

Om survey-undersøgelsen

192 danske ledere, IT-chefer og andre beslutningstagere danner grundlag for itm8 Cyber Security Survey 2025, hvor fokus er på cybersikkerhed i danske virksomheder.

Sikring af datavaliditet

Vores undersøgelse er baseret på et samlet datagrundlag med besvarelser fra i alt 501 respondenter. For at sikre høj relevans og validitet i analysen er data efterfølgende blevet segmenteret til udelukkende beslutningstagere i danske virksomheder – altså personer med direkte ansvar for eller indflydelse på virksomhedens cybersikkerhedsstrategi.

Ved at fokusere udelukkende på beslutningstagere sikrer vi, at de indsamlede svar afspejler strategiske overvejelser og faktiske praksisser frem for generelle holdninger og ønsker blandt medarbejdere.

Segmenteringen giver desuden en afgrænset gruppe af nøglepersoner, hvilket øger den statistiske styrke og relevans af undersøgelsen.

Efter segmenteringen udgør beslutningstagerne 192 personer – som indgår i den endelige dataanalyse.

Kvalificerede og troværdige indsigter

De 192 danske beslutningstagere repræsenterer et bredt udvalg af brancher, virksomhedsstørrelser og geografiske områder, hvilket bidrager til en bred og varieret datamængde. Ud af de 192 er 146 af beslutningstagerne i små og mellemstore virksomheder.

Selvom de 192 virksomheder ikke er repræsentative for alle virksomheder i Danmark, vurderer vi, at mængden alligevel er tilstrækkelig til at give kvalificerede og troværdige indsigter i cybersikkerhed blandt danske virksomheder.

Spørgeundersøgelsen er foretaget i efteråret 2025 blandt itm8s kundedatabase og modtagere af itm8s nyhedsbrev.



192 danske direktører, IT-chefer og beslutningstagere har deltaget i itm8 Cyber Security Survey 2025.

Tak, fordi du læste med.

Har du spørgsmål vedrørende cybersikkerhed, er du altid velkommen til at række ud til os.

+45 6916 0004
information@itm8.com
www.itm8.dk

En forbedret cybersikkerhed i dag holder hackerne ude i morgen.
Læs mere om, hvordan vi kan styrke dit sikkerhedssetup.

<https://itm8.dk/cyber-security> ↩



Et digitalt kompas i en kompleks verden

itm8 er en førende nordisk IT-partner med over 20 års erfaring i at guide organisationer gennem digital udvikling. I et landskab med stigende kompleksitet, sikkerhedskrav og effektivitetspres skaber itm8 overblik og viser vejen.

Med mere end 1.700 ansatte – herunder eksperter i cybersikkerhed, cloud, software og infrastruktur – sikrer itm8 stabil drift og leverer strategisk IT-rådgivning.

Gennem tætte partnerskaber, hvor teknisk indsigt kombineres med forretningsforståelse, hjælper itm8 kunder med at opbygge robuste IT-fundamenter i dag, der styrker deres forretning i morgen.

itm8[®]

+45 6916 0004
information@itm8.com

www.itm8.dk