KPMG

DI Digital

Visioner og løsninger i bekæmpelsen af cyberkriminalitet i Danmark

Oktober 2025

Indhold

01

Introduktion

Introduktion

Baggrund

Cyberkriminalitet udgør en stigende trussel mod det danske erhvervsliv, og det er afgørende, at vi arbejder sammen for at beskytte vores virksomheder og samfund bedre imod denne udfordring. Vi skal med andre ord arbejde for, at det bliver sværere at begå cyberkriminalitet end i dag.

På den baggrund har Dansk Industri og KPMG igangsat et initiativ, der har til formål at styrke Danmarks evne til effektivt at imødegå truslen fra cyberkriminelle.
Det kræver en mangfoldighed af indsatser og et tillidsfuldt samarbejde på tværs af virksomheder, myndigheder og civilsamfundet, hvis vi skal nå i mål.

Ambition og scope

Ambitionen med projektet er at styrke samarbejdet mellem offentlige og private aktører for at undersøge og udvikle nye dimensioner og initiativer, der kan bidrage til at imødegå cyberkriminalitet mod dansk erhvervsliv.

Vi har set på hele processen fra flere perspektiver, herunder hvordan vi kan forebygge angreb, minimere deres konsekvenser og styrke modstandsdygtigheden hos virksomheder på tværs af brancher. Vores resultater og anbefalinger er samlet i dette white paper, hvor vi fokuserer på konstruktive og fremadskuende initiativer, der kan styrke samarbejdet i kampen mod cyberkriminalitet.

Metode

I projektet, som er forløbet fra maj til oktober 2025, har vi undersøgt forhold og erfaringer relateret til cyberkriminalitet fra en kvantitativ og en kvalitativ tilgang:

- Vi har gennemført en **spørgeskemaundersøgelse** som del af Dansk Industris Virksomhedspanel fra juni 2025 med svar fra 475 virksomheder, der udgør et repræsentativt udsnit af DI's medlemskreds. Undersøgelsen omfatter 49.000 ansatte i Danmark og dækker forskellige områder relateret til cybersikkerhed, selvom panelet ikke specifikt var målrettet dette emne.

- Vi har foretaget et **fokusgruppeinterview** med en række virksomheder, som har besvaret Virksomhedspanelet for at nuancere vores forståelse og stille uddybende spørgsmål til virksomhedernes erfaringer.

- Vi har afholdt en **ekspertworkshop** med væsentlige aktører fra den private og offentlige sektor samt civilsamfundet, hvor vi med udgangspunkt i data fra spørgeskemaundersøgelsen og fokusgruppeinterviewet drøftede og udviklede konkrete løsningsforslag til en styrket beskyttelse mod cyberkriminalitet i fremtiden.

Indsigterne fra disse tre aktiviteter er samlet i dette white paper med resultater og løsningsforslag, som kan inspirere til drøftelse af, hvordan vi bedst kan sikre danske virksomheder og samfundet mod cyberkriminalitet.

Deltagere

Dansk Industri og KPMG har ikke kunnet udføre dette projekt uden stor interesse, aktiv deltagelse og åbenhed fra en række virksomheder, myndigheder og organisationer.

Der skal rettes tak til følgende virksomheder, organisationer og myndigheder, som bidrog med konstruktive idéer, rådgivning og ambitioner på vores ekspertworkshop, og som i det følgende vil omtales som ekspertgruppen:

- Microsoft Danmark
- EG
- TDC Erhverv
- CSIS
- Dubex
- DLA Piper
- National Enhed for Særlig Kriminalitet v. NC3
- Styrelsen for Samfundssikkerhed
- Tryg
- Finans Danmark
- Det Kriminalpræventive Råd
- Rådet for Digital Sikkerhed
- Teleindustrien
- Sune Gabelgård

02

Anbefalinger

Anbefalinger til det politiske niveau

Den undersøgelse, som KPMG og DI har gennemført, identificerer en række centrale anbefalinger, som vurderes at have særlig betydning for Danmarks fremtidige robusthed over for cybertrusler. Fokus i disse anbefalinger er på, hvad man fra politisk side kan gøre for at styrke det samlede værn mod cyberkriminalitet. Det er dog vigtigt at understrege, at erhvervslivet og civilsamfundet også har et stort ansvar i at understøtte initiativerne, og næste slide opridser også virksomhedsrettede anbefalinger på baggrund af undersøgelsen.

1-2 år

Gentænk cyberindsatsen fra bunden

Politiet og Ministeriet for Samfundssikkerhed bør sammen med private aktører stille sig i spidsen for et initiativ, der systematisk gennemgår de mest skadelige cybertrusler rettet mod dansk erhvervsliv og sikrer, at ressourcer, lovgivning, ansvar og arbejdsdeling matcher truslernes alvor. I den forbindelse bør det også afdækkes, hvordan myndighedernes kommunikation til erhvervslivet kan optimeres i forbindelse med konkrete sagstyper.

Styrk delingen af trusselsinformation

Styrelsen for Samfundssikkerhed anbefales at etablere en national platform for fortrolig deling af trusselsinformation mellem myndigheder, virksomheder og leverandører med afsæt i hændelsesindberetninger i regi af NIS2.
Som et første skridt skal det i tæt samarbejde med cybersikkerhedsleverandører afklares, hvilken type af information, der kan deles på platformen. Fokus skal i første omgang være på beskyttelsen af kritisk infrastruktur.

3-5 år

Investér målrettet i teknologisk innovation

Regeringen vil med sine strategiske prioriteter for forskning og innovation 2026-29 styrke Danmarks sikkerhed med 6,9 mia. kr. i 2026-29 inden for bl.a. kvanteteknologi, AI og forsvar. Det foreslås, at der fra 2027 og frem prioriteres en betydelig andel til forskning og innovation i styrket cybersikkerhed vha. nye teknologier, herunder AI, så Danmark effektivt kan håndtere cybertrusler. Parallelt bør Danmark presse på for etablering af et europæisk DARPA, der accelererer udvikling af bl.a. dual use-teknologi til cybersikkerhed og forsvar via højrisikoinvesteringer.

Accelerér skiftet til post-kvantekryptering

Kvantecomputere truer med at gøre klassisk kryptering forældet og kompromittere alt fra finansielle transaktioner til national sikkerhed. Danmark skal handle nu for at fremtidssikre vores kritiske infrastruktur. Derfor bør der etableres pulje på 100 mio. kr. årligt i tre år under Innovationsfonden til implementering og integration af post-kvantekryptografi i sektorer som finans, energi mv.

5+ år

Flere specialister og styrket beredskab

Regeringen bør sammen med uddannelses-institutionerne sikre, at cybersikkerhed indtænkes på alle relevante it-uddannelser, hvor det ikke er pensum. Dertil bør alle kvalificerede ansøgere optages på IT- og cyberuddannelserne, og samtidig opfordres Ministeriet for Samfundssikkerhed til allerede nu til at etablere en beredskabsordning, hvor eksperter kan aktiveres via standby-kontrakter, så samfundets samlede cyberkompetencer udnyttes effektivt, når større cyberhændelser rammer.

Styrk beskyttelsen med netværksfiltrering

Ministeriet for Samfundssikkerhed anbefales at etablere en national digital infrastruktur med integreret DNS-beskyttelse og netværkssegmentering, der effektivt kan filtrere skadelig trafik og mindske angrebsfladen for både virksomheder og borgere. Løsningen skal være frivillig, balancere behovet for sikkerhed, ytringsfrihed og privatliv og evt. suppleres af en national enhed, der overvåger og håndterer cybertrusler på tværs af sektorer som overbygning på de sektorvise enheder (CERT'er).

Anbefalinger til erhvervslivet

På baggrund af undersøgelsen har DI og KPMG udvalgt en række anbefalinger, som står frem som særligt relevante for fremadrettet at sikre danske virksomheder over for cyberkriminelle. Fokus i disse anbefalinger er på, hvad man fra erhvervslivets side kan gøre for at styrke værnet mod cyberkriminalitet, men det er vigtigt at understrege, at de myndighedsrettede indsatser skal supplere disse tiltag for at sikre et højt fælles niveau af cybersikkerhed og stærk koordinering på tværs af sektorer.

Sæt i gang nu i jeres egen forretning

Arbejd ud fra en risikobaseret tilgang

Skab overblik over jeres væsentligste risici med en risikovurdering, fx med afsæt i IT-risikovurderings-værktøjet på sikkerdigital.dk. Sørg uanset hvad for, at jeres basale cybersikkerhed er på plads via løbende backup, adgangsstyring, software-opdateringer, træning mv. og for, at ledelsen løbende tager stilling til jeres risici og indsatser.

Udarbejd en beredskabsplan og test den

Alle virksomheder bør have en beredskabsplan. Tag afsæt i DI's gratis skabelon og vejledning til beredskabsplaner og husk at opdatere planen løbende. Planlæg også løbende øvelser for at teste, om planen virker. Deltag i Hele Danmark Øver-kampagnen, som kører hvert år i oktober.

Prioritér en aktiv leverandørstyring

Aktiv leverandørstyring handler om at have styr på, hvem der leverer jeres IT- og digitale løsninger, og hvordan de håndterer sikkerhed. Kom godt i gang med afsæt i konkrete vejledninger og tjeklister til aktiv leverandørstyring på sikkerdigital.dk.

Bidrag til den fælles cybersikkerhed

Bliv D-mærket

D-mærket er Danmarks mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse. Ved at blive D-mærket styrker I ikke kun jeres egen sikkerhed, men bidrager til den fælles cybersikkerhed ved at gøre det lettere for kunder at vælge sikre løsninger og gøre sikkerhed til et konkurrenceparameter.

Anmeld cyberangreb og sikr jeres beviser

Hvis I bliver ramt, bør I straks anmelde angrebet til politiet og øvrige relevante myndigheder. Det er afgørende for at forhindre angreb i at sprede sig og skabe et retvisende overblik over truslerne, så myndighederne kan tilrettelægge deres indsats ud fra det. Husk at sikre digitale beviser, fx med afsæt i datasikringsskabelonen på sikkerdigital.dk.

Bidrag til en større åbenhedskultur

Del erfaringer om cybertrusler og hændelser i relevante netværk. Anerkend, at alle kan blive ramt, og at åbenhed om hændelser hjælper hele erhvervs-livet med at lære og styrke det fælles forsvar.

Specifikt til leverandører

Skræddersy flere løsninger til SMV'er

Udvikl brugervenlige og omkostningseffektive løsninger, der matcher SMV'ers forskellige behov og modenhedsniveau, og gør det nemt for SMV'er at komme i gang med basale sikkerhedstiltag.

Indtænk sikkerhed fra starten i løsninger

Sørg for, at sikkerhed ikke er et tilvalg, men en integreret del af jeres produkt fra start, så det bliver nemt at vælge sikkert. Implementér de kommende råd fra Cybersikkerhedspagten i jeres produkter, så jeres kunder automatisk lever op til minimums-anbefalinger for cybersikkerhed.

Styrk videndelingen på tværs

Bidrag til styrket deling af trusselsinformation, så både kunder, andre leverandører og myndigheder får adgang til opdateret viden om aktuelle cybertrusler og angrebsmetoder. Deltag aktivt i at sikre, at viden om angreb rejser på tværs af sektorer og bidrager til et stærkt værn mod cyberkriminalitet.

03

Analyse

Analyse af den danske indsats mod cyberkriminalitet

Vores analyse er baseret på data fra Dansk Industris Virksomhedspanel, et fokusgruppeinterview med danske virksomheder afholdt i forlængelse af Virksomhedspanelet, samt indsigt og input fra en ekspertworkshop afholdt i september 2025. Vi har samlet vores indsigter i syv centrale tematikker, som vi i det følgende vil gennemgå og uddybe.

01

Tilliden til myndighederne

Tilliden til, at danske myndigheder kan behandle sager om cyberkriminalitet og retsforfølge cyberkriminelle er i bund. Vi gennemgår de årsager og erfaringer, som ligger til grund herfor og drøfter mulige løsninger.

02

De væsentligste trusler

Vi gennemgår de trusler, som virksomheder anno 2025 anser som de væsentligste, og forholder os til det fremtidige trusselsbillede, hvor ny teknologi vil spille en rolle på flere baner.

03

Beredskabet mod cyberkriminalitet

Vi redegør for de beredskabsindsatser, som danske virksomheder har iværksat og identificerer væsentlige blinde vinkler. Vi gennemgår bl.a. udbredelsen af beredskabsplaner og cyberforsikringer.

04

Et fælles ansvar

Cybersikkerhedsindsatsen består af mange aktører, hvorfor ansvaret også må regnes som delt. Der er særligt behov for, at leverandører byder ind med flere løsninger til SMV'erne, hvor sikkerhed er indtænkt fra start.

05

Organisering og samarbejde

Det danske samarbejde om cybersikkerhed er under udvikling i takt med, at det koordinerende ansvar styrkes. Der er dog stadig behov for en gentænkning af myndighedernes håndtering af cyberkriminalitet i tæt samarbejde med erhvervslivet.

06

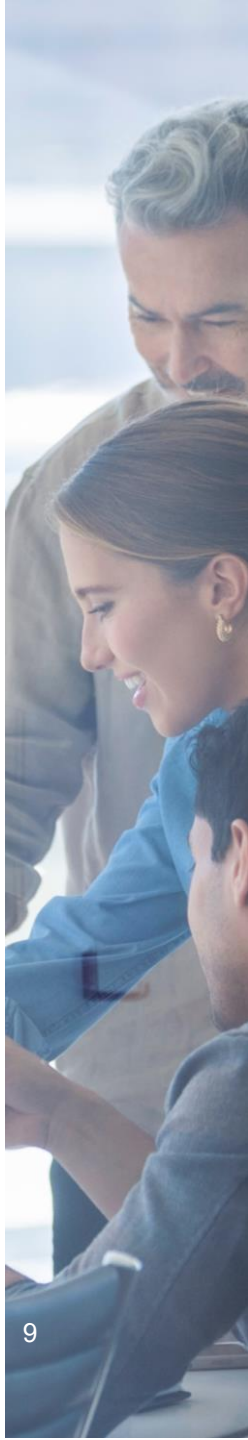
Uddannelse og awareness

Det bedste værn mod cyberkrimalitet er i sidste ende borgerne og virksomhederne selv, hvorfor det er essentielt, at de er klædt tilstrækkeligt på. Der er samtidig massivt behov for flere specialiserede cyberkompetencer i fremtiden.

07

Netværk og overvågning

Vi drøfter, hvordan man fra centralt hold kan beskytte danske borgere og virksomheder gennem løsninger som et nationalt cyberfilter og en national overbygning til de sektorvise enheder (CERT'er), men at disse løsninger skal balanceres med hensynet til privatliv.



01
02
03
04
05
06
07

Tilliden til myndigheder

Et af de mest markante resultater fra vores spørgeskemaundersøgelse var, at **64% af de adspurgte virksomheder angiver, at de har lav eller ingen tillid til, at politi og andre myndigheder effektivt kan efterforske og retsforfølge cyberkriminelle.**

Tallet skal især ses i lyset af cybertruslens grænseoverskridende karakter, der gør det vanskeligt for myndigheder at finde og retsforfølge de ansvarlige og sætte effektivt ind over for fødekæden af kriminelle. Samtidig hænger resultatet sammen med, at flere virksomheder ikke oplever, at deres sager tages op.

Baseret på erfaringer

Da vi spurgte deltagerne i vores fokusgruppe ind til den manglende tillid til politi og øvrige myndigheders håndtering af cyberkriminalitet henviste flere virksomheder til konkrete erfaringer. Flere virksomheder har tidligere anmeldt cyberkriminelle forhold uden at blive kontaktet efterfølgende eller modtage respons på deres anmeldelse. Derfor beskrev flere virksomheder, at de ikke så nogen grund til at melde det, hvis det ikke gav anledning til handling eller respons. Overordnet gav dialogen indtryk af, at der er et ønske om at få hjælp fra myndighederne og anmelde forhold, men at mange vælger at lade være, fordi de har oplevelsen af, at det ikke fører noget med sig.

I vores spørgeskemaundersøgelse var det ligeledes kun **hver tredje virksomhed som angav, at de ville henvende sig til politiet eller andre myndigheder i forbindelse med et cyberangreb.**

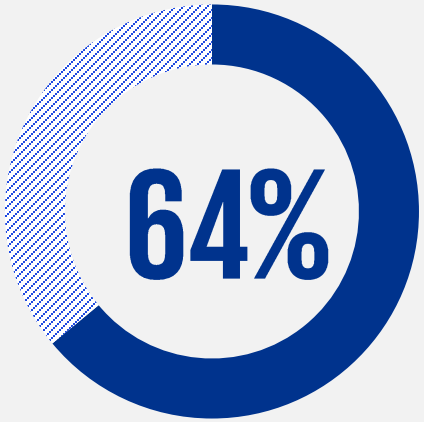
Et skyggetal i anmeldelser

Ovenstående er overraskende, da antallet af anmeldelser generelt stiger. National Center for IT-kriminalitets (NCIK) årsrapport 2024 viser således en generel stigning i antallet af anmeldelser om it-relateret økonomisk kriminalitet på 40% i perioden 2020-2024. Når man dykker ned i tallene, kan man dog se, at det særligt er borgerrettet kriminalitet (såsom salg via DBA, Marketplace, falske webshops, mv.), der driver stigningen, mens **virksomhedsanmeldelser faktisk er faldet fra 896 i 2020 til 554 anmeldelser i 2024.** Disse taler stemmer altså med erfaringerne fra vores undersøgelse, og givet den øgede aktivitet af cyberangreb, kan vi med rette antage, at der er et stort skyggetal, når det kommer til cyberangreb mod virksomheder, som vi ikke kender til.

Flere ressourcer og større åbenhed

Når angrebsfladen stiger, er der behov for, at der følger flere ressourcer med til bekæmpelsen af cyberkriminalitet, ligesom det er afgørende, at politiet fortsat deltager aktivt i det internationale samarbejde om at sætte ind mod de globale fødekæder af cyberkriminelle, der i stigende grad udbyder "cybercrime-as-a-service" i et bredt forgrenet netværk.

Derudover vidner vores undersøgelse om behovet for en mere transparent dialog mellem politi, myndigheder og virksomheder om, hvilke trusler og angrebsformer, der prioriteres, og hvordan myndighederne bruger anmeldelser fra virksomheder i deres arbejde, så incitamenterne til at anmelde cyberangreb øges.



af de adspurgte virksomheder **har lav eller ingen tillid til, at politi og andre myndigheder effektivt kan efterforske og retsforfølge** cyberkriminelle.

01
02
03
04
05
06
07

De væsentligste trusler

Vores data fra Virksomhedspanelet viser, at **udefrakommende trusler som ransomware (48 %) og phishing (60 %) generelt anses som større trusler end interne trusler som datatyveri (9 %) eller insider-trusler (8 %).** Virksomheder er mest bekymrede for truslen udefra, og jo større virksomheden er, jo mere komplekst bliver deres opfattelse af trusselsbilledet både fra interne trusler og eksterne trusler.

I lyset af det nuværende trusselsbilllede er det forståeligt, at phishing og ransomware anses som store trusler, og ofte vil de to være del af den samme angrebskæde. Phishing og underkategorier som CEO-fraud, social engineering, smishing osv. bliver kun en større trussel i takt med, at bedre danske oversættelser, anvendelse af AI til stemme- og billedemanipulation mm. gør det lettere for svindlere at udgive sig for at være en betroet kilde.

Emerging tech er et tveægget sværd

Udviklingen i nye teknologier som kunstig intelligens og kvantecomputere var også et gennemgående tema i ekspertgruppen. De nye teknologier giver hidtil usete muligheder, men kommer også med store sikkerhedsmæssige udfordringer. **Kunstig intelligens har således revolutioneret cyberkriminelles angrebsmetoder, mens kvantecomputere i fremtiden vil kunne bryde krypteringsmetoder, som vi i dag anser som sikre.** Derfor skal vi oppe vores beskyttelse mod AI-understøttet svindel og forberede os på post-kvantekryptering for at sikre en langsigtet beskyttelse mod nuværende og fremtidige trusler, som udspringer af den teknologiske udvikling.

Både AI og kvantecomputere skal også tænkes ind i en større geopolitisk kontekst, hvor hybride angrebsmetoder kan lamme, forstyrre og stjæle informationer i vores digitaliserede samfund. Inden for de næste 3-5 år vil der være behov for at se nærmere på disse trusler i en langt større og mere sammenkoblet grad, da risikoen samlet set er eksponentielt større, når teknologierne bruges samlet.

Defensiv og offensiv brug af teknologi

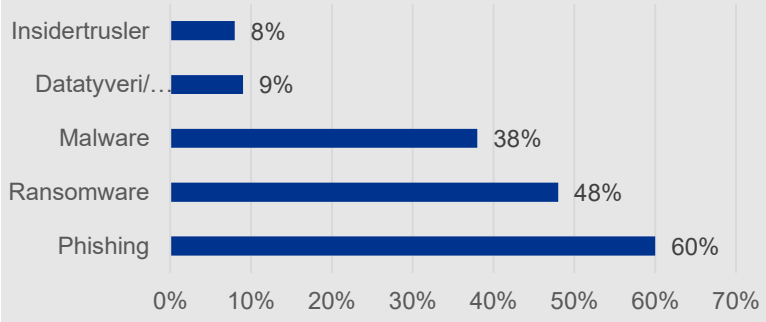
Ekspertgruppen betonede, at **AI både skal tænkes som en defensiv og offensiv ressourcemulighed** – ikke mindst i myndighedernes arbejde. På den defensive side er potentialet bl.a. stort for at reducere respons- og mitigeringstider.

AI-assistenter og agenter implementeres allerede bredt, hvilket bl.a. politiet udnytter til hurtigere dataanalyse, men der er også potentiale for forbedret kontakt med borgere og virksomheder i løbet af et opklaringsforløb.

Offensivt kan AI bruges til at afskrække cyberkriminelle aktører gennem strategisk disruptive handlinger.

En klar udfordring er manglende overblik over trusler på tværs af sektorer, offentlige og private aktører. Flere initiativer er igangsat som led i NIS2, DORA, CER, mv. Det er afgørende, at vi bruger disse regulativer til at sætte skub under delingen af trusselsinformation og letter implementeringen af grundlæggende sikkerhedskrav gennem fælles indsatser og styrkelse af leverandørerne.

Hvilke former for cyberkriminalitet vurderer I som de største trusler mod jeres forretning?



Anm.: Mulighed for op til 2 svar. Kilde: DI's virksomhedspanel

Beredskabet mod cyberkriminalitet

I vores spørgeskemaundersøgelse blev virksomhederne spurgt ind til, hvilke muligheder de har for at reagere på og afbøde et cyberangreb, hvor vi gav dem en række foranstaltninger som svarmuligheder. Den gennemgående trend er, at de store virksomheder har implementeret flere foranstaltninger end de mindre. **Således har halvdelen af virksomhederne med 1-20 ansatte kun implementeret én eller ingen af de opstillede foranstaltninger.** Til sammenligning har 56 % af virksomheder med min.100 ansatte mindst tre foranstaltninger implementeret.

Det var gennemgående for de virksomheder, som deltog i vores fokusgruppeinterview, at man er i gang med at implementere tiltag, der skal sikre bedre cybersikkerhed – særligt med udgangspunkt i ny lovgivning som NIS2. Med en erkendelse af, at man skal starte et sted blev der talt om indsatser for at styrke f.eks. netværkssikkerhed og awareness hos brugere mv. alt efter modenhedsniveauet i de forskellige virksomheder. Det kan dog sagtens forestilles, at virksomheder uden et etableret beredskab ville være mindre tilbøjelige til at deltage i et fokusgruppeinterview om dette emne.

Samtidig viser resultaterne med al tydelighed, at der er behov for, at virksomheder prioriterer deres cybersikkerhed højere i fremtiden.

Få har en plan og færre har øvet sig

Beredskabsplaner, som anses som ét de mest centrale foranstaltninger i et beredskab, er et godt eksempel på forskellene mellem store og små virksomheder. Generelt havde 43 % af de adspurgte virksomheder forberedt en beredskabsplan, men tallene rummer væsentlige forskelle afhængigt af størrelse. **Det er således kun hver fjerde virksomhed på mellem 1-20 ansatte, som har en beredskabsplan, mens næsten 3 ud af 4 af de store virksomheder har en beredskabsplan.** Dette er bemærkelsesværdigt, idet virksomheder i alle størrelser og former i dag er eksponerede for cyberangreb. Det hænger dog sammen med, at mindre virksomheder ofte ikke har ressourcerne til at arbejde særskilt med cybersikkerhed, hvorfor de i højere grad er afhængige af, at deres leverandører kan levere sikre løsninger på vegne af dem. Det anbefales, at alle virksomheder uanset størrelse får en beredskabsplan, så man er forberedt, hvis man skulle blive angrebet.

Vores undersøgelse viser samtidig, at det kun er **12 % af de adspurgte virksomheder, som har øvet et cyberangreb** gennem simulationer eller beredskabs-øvelser. Dette er et væsentligt element i ethvert beredskab, da man ikke kan være sikker på, at ens plan fungerer efter hensigten, hvis man ikke har efterprøvet den i praksis.

Ekstern hjælp

43% af de adspurgte virksomheder i DI's medlemskreds har i dag en cyberforsikring, der dækker ekstern hjælp i forbindelse med et cyberangreb.

Undersøgelsen viser, at forsikringen ikke betyder, at virksomheden *ikke* har iværksat andre initiativer for at forebygge cybersikkerhed. Faktisk viser det sig, at de virksomheder, som ikke har en forsikring, har færre initiativer end dem, som har forsikret sig.

0-1
foranstaltninger er implementeret i halvdelen af de mindste virksomheder (1-20 ansatte).

43%
af adspurgte virksomheder har en cyberforsikring. Tallet er lidt mindre for de mindste virksomheder.

1 ud af 4
af de mindste virksomheder har en beredskabsplan.

12%
af alle virksomheder har øvet deres beredskab.

01
02
03
04
05
06
07

Et fælles ansvar

Når det kommer til cybersikkerhed er det i sidste ende altid den enkelte virksomhed, som er ansvarlig for at beskytte sine aktiver. Faktum er dog, at det i praksis er en kæmpe udfordring for virksomhederne på egen hånd at sikre sig selv. Det er ressourcekrævende og komplekst, og hvor skal man i grunden starte? Samtidig spreder cyberangreb sig hastigt på tværs af virksomheder og sektorer, hvilket gør det til et samfundsproblem, som kun kan løses i fællesskab.

Som det fremgik af det foregående tema, kæmper mange virksomheder – særligt de små – med at implementere foranstaltninger til at sikre sig mod cyberangreb. I fokusgruppeinterviewet var der en tydelig erkendelse af nødvendigheden af et stærkt værn mod cybertrusler – enten på grund af dyrt købte erfaringer, eller fordi ny lovgivning kræver det. Men virksomhederne famler stadig i jagten efter de vigtigste og mest effektive tiltag.

Betoningen af virksomhedernes ansvar gik igen hos ekspertgruppen, hvor flere nævnte **vigtigheden af velstrukturerede forretningsprocesser.** Det handler ikke kun om teknik, men om ledelsesforankring og styring. Det kan være svært for små og mellemstore virksomheder, hvor ressourcerne er knappe, og fokus ofte er entydigt på driften.

Cloud som en mulig løsning

Overgangen fra lokale servere til cloudløsninger er en central tendens, især for små og mellemstore virksomheder, og en mulig løsning for mange. **Ved at flytte operationer til skyen kan sikkerhedsindsatsen centraliseres hos cloududbyderen,** hvilket typisk er en fordel for virksomheder, der mangler ressourcer til at anskaffe og implementere nødvendige sikkerheds-teknologier individuelt. På denne måde sikres en mere robust beskyttelse af værdifulde aktiver, men beslutningen bør altid bero på en konkret vurdering af behovene i jeres forretning. En cloudløsning vil ofte komme med en potentiel højere omkostning og behov for et kompetenceløft til at håndtere IT-sikkerhed i skyen.

Øget ansvar hos leverandørerne

Netop pga. ovenstående udfordringer betonede flere i ekspertgruppen også, at sikkerhedsansvaret i stigende grad bør flyttes fra den enkelte virksomhed til leverandørerne, således at **software-, tele- og cloud-leverandører (gerne europæiske) påtager sig et større ansvar for et højt teknisk sikkerhedsniveau**.

Idéen om at leverandører, f.eks. teleudbydere, kan forhindre angreb gennem effektiv DNS-beskyttelse er et eksempel på, hvordan leverandørernes rolle kan styrkes.

Der er dog tendenser til ubalance i markedet, hvor løsninger ikke altid er forståelige, overkommelige eller tilgængelige for mindre virksomheder. Fremover er det centralt at modne markedet for cybersikkerhedsløsninger til de mindste virksomheder, så de kan tilbydes enklere løsninger, hvor cybersikkerhed er integreret fra start.

“En tilstrækkelig sikkerhed skal nås i tæt samarbejde med ens leverandører. Det forpligter dem til at levere sikkerhed i deres produkter out-of-the-box.”

Martin Povelsen,
Partner KPMG

Organisering og samarbejde

Myndighederne har påtaget sig en betydelig rolle i at styrke cybersikkerheden i de seneste år. Selvom virksomheder er ansvarlige for deres egen sikkerhed, **har myndighederne også lanceret en række initiativer og strategier, der understøtter virksomhedernes arbejde på området.** Disse indsatser hjælper med at skabe en seriøs og klar retning for styrket cybersikkerhed på tværs af samfundet. I lyset af det stigende trusselsbillede er det vigtigt, at myndighedsindsatser fremover får øget opmærksomhed, og at samarbejdet mellem det offentlige og private styrkes via flere reelle indsatser, der kan imødegå truslens alvor.

Øget koordinering på tværs af sektorer

En væsentlig pointe fra ekspertgruppen var således, at ansvaret for Danmarks cybersikkerhed hidtil har været spredt på tværs af for mange hænder, hvilket har gjort det vanskeligt at mønstre den nødvendige opmærksomhed og handling. Opmærksomheden har dog været stigende i takt med de geopolitiske udviklinger i relation til forholdet til Rusland, hvor man i dag taler om hybridkrig og cyberkrigsførelse. Det er denne udvikling, der har gjort, at man fra politisk side i dag har valgt at samle koordineringen af cyber-sikkerhedsindsatser under Ministeriet for Samfundssikkerhed og Beredskab.

Udviklingen er positiv, men der er fortsat en meget forskelligartet tilgang til cybersikkerhed på tværs af sektorer, og der er behov for mere ensretning og koordinering i fremtiden. Et eksempel på en indsats, der kan skabe mere sammenhæng er en national overbygning til de sektorvise CERT'er, der kan understøtte, at mere information og viden kommer flere sektorer til gavn og styrker den fælles sikkerhed.

Gentænking af cyberindsatsen

En væsentlig pointe fra ekspertgruppen var idéen om at **gentænke cyberindsatsen fra bunden med afsæt i en systematisk gennemgang af de værste former for cyberkriminalitet.** Formålet er at identificere potentialerne for en mere effektiv og innovativ bekæmpelse af truslerne i fremtiden.

Flere deltagere kunne nikke genkendende til manglen på overblik, målretning og prioritering af ressourcer, en uklar arbejdsdeling på tværs af det offentlige og private og lovgivningsmæssige hindringer, der står i vejen for en effektiv beskyttelse, fx anvendelsen af nye teknologier.

Ekspertgruppen påpegede, at kortlægningen skal laves i et stærkt offentligt-privat partnerskab og med aktivering af øvrige EU-lande for at sikre sammenhæng og videndeling på tværs. Ønsket er, at kortlægningen vil give det nødvendige afsæt for en strategisk stillingtagen til, om vi har de rette greb til at håndtere nuværende og fremtidige cybertrusler og give anledning til et langt stærkere samspil mellem offentlige og private indsatser for bekæmpelse af cyberkriminalitet, fordi det bliver tydeligere, hvad der prioriteres, og hvem der gør hvad i den forbindelse.

Styrket samarbejde i Norden og Baltikum

En interessant vej til at styrke dansk cybersikkerhed og beredskab er et stærkere nordisk og baltisk samarbejde på området. Ved at dele ressourcer, trusselsinformation og gennemføre flere fælles beredskabsøvelser kan vi opnå bedre resultater i beskyttelsen end ved at handle alene.

Dette forslag havde opbakning hos både ekspertgruppen og fokusgruppen, især fordi cyberkriminalitet sjældent kan løses af en enkelt nation pga. truslens grænseoverskridende karakter.

Awareness og uddannelse

Det er et velkendt faktum, at langt de fleste succesfulde cyberangreb sker pga. menneskelige fejl. Vi kan beskytte os med tekniske foranstaltninger, men i langt de fleste tilfælde vil det være et menneske, som trykker på et link, opsætter en firewall forkert eller overfører penge til det forkerte kontonummer. **Derfor skal både borgere og virksomheder have kendskab til sikker digital adfærd,** ligesom vi bør øge udbuddet af cyberspecialister. Et tema, som blev betonet i både fokusgruppen og ekspertgruppen.

Cybersikkerhed på skoleskemaet

Det er en positiv udvikling, at man fra 2027/28 tilbyder teknologiforståelse som valgfag i folkeskolen. I ekspertgruppen blev det dog fremhævet, at basal kendskab til cybersikkerhed dog ikke bør være et tilvalg, men en del af den almene dannelse i et højt-digitaliseret samfund som det danske. Alle børn bør således kende til vigtigheden af et sikkert password og de normale kendetegn ved phishing mv.

Ekspertgruppen pegede samtidig på et **massivt behov for specialistviden inden for cybersikkerhed.** Cyberspecialister er en mangelvare på globalt plan, og derfor skal Danmark gøre mere ud af at tilbyde uddannelser i cybersikkerhed på videregående uddannelser og indtænke cybersikkerhed på relevante it-uddannelser.

Kompetenceløft i virksomhederne

Kompetenceløftet bør dog ikke kun finde sted blandt danske borgere. Som det fremgår af vores analyse ovenfor, er cybersikkerhed et komplekst felt, som særligt små og mellemstore virksomheder kæmper med at få styr på. Det kan være svært at skabe overblik over, hvor man skal starte, og derfor er der behov for at basal "cyber-hygiejne" på plads.

Der skal være klarere kommunikation og rådgivning af, hvilke foranstaltninger, man som minimum bør implementere. Dette er et af flere initiativer i Cybersikkerhedspagten, der er et samarbejde mellem offentlige og private aktører. Her udvikles en række gode råd til cybersikkerhed særligt målrettet SMV'er, som bl.a. indebærer adgangsstyring, backup mv. Det er afgørende, at myndigheder og virksomheder, herunder leverandører, bidrager til at implementere de gode råd i praksis – ikke mindst i konkrete cybersikkerhedsløsninger, så det bliver nemt at træffe sikre valg.

Tilsvarende er Danmarks mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, D-mærket, et rigtigt godt sted for virksomheder, herunder SMV'er, at gå hen for at få overblik over sin digitale sikkerhed og kunne dokumentere sit arbejde over for sine kunder.

Der er behov for mere målrettet rådgivning

Behovet for klarere rådgivning og kommunikation gik igen hos virksomhederne i vores fokusgruppe. Meget information og mange værktøjer eksisterer allerede, bl.a. på Sikker Digital, men når ikke i tilstrækkelig grad ud til målgruppen og er svære at omsætte i praksis, bl.a. fordi den tilgængelige viden ikke er målrettet nok. Der er samtidig en oplevelse af, at der er behov for mere rådgivning om best practices i implementeringen af udvidede krav til cybersikkerhed, herunder NIS2.

Accepter fejl og del mere viden

En væsentlig forudsætning for at blive bedre til at forsvare os mod cyberangreb er at lære af tidligere erfaringer. Der var derfor også en drøftelse i ekspertgruppen om vigtigheden af, at virksomheder, der har været ramt af cyberangreb, står frem og fortæller om sine erfaringer.

I dag vil langt de fleste virksomheder opleve angreb før eller siden. Det skal derfor være mere risikofrit at stå frem og anerkende sine fejl. Det er et langt sejt træk at ændre på den herskende lukkethedskultur, men hver gang organisationer træder frem, bliver vi klogere i fællesskab.

01
02
03
04
05
06
07

Netværk og overvågning

Det er et faktum, at cyberkriminalitet er en international udfordring, hvor cyberkriminelle fra hele verden kan gemme sig bag VPN'er, forskellige lovgivninger og i visse tilfælde med opbakning fra stater. Det giver landets politimyndigheder ringe vilkår for at efterforske og retsforfølge kriminelle og kræver langt større samarbejde og koordinering, som også er set ved flere lejligheder i Europa og Interpol. Det gælder også på tværs af sektorer i vores tekniske løsninger.

Nationale tekniske løsninger skal i spil

Et af de centrale spørgsmål på ekspertworkshoppen var, hvad man teknisk kan gøre på for at styrke beskyttelsen og skabe mere sammenhæng i indsatser på tværs af sektorer. **En potentiel løsning, der blev fremhævet, er et nationalt cyberfilter, designet til at beskytte mod digitale trusler via DNS-beskyttelse og netværkssegmentering**.

En sådan løsning vil mindske angrebsfladen betydeligt og sikre mere tværgående information om tendenser i angreb. Løsningen skal være frivillig, og der skal investeres i en høj beskyttelse af infrastrukturen, da dette netværk kunne udgøre et single-point-of-failure ved afbrydelser og angreb.

Mere sammenhæng på tværs af sektorer

Flere deltagere i ekspertgruppen nævnte samtidig muligheden for at etablere et nationalt Security Operations Center (SOC), dvs. et nationalt center, der på tværs af sektorer overvåger, opdager og håndterer cyberangreb. Fordelene ved en sådan løsning er mulighederne for at samle ressourcer og kompetencer ét sted samt at sikre hurtigere respons og videndeling. Den konkrete konstruktion vil skulle udbores nærmere, men den nationale SOC vil skulle bygge videre på de sektorvise CERT'er, der allerede eksisterer i dag.

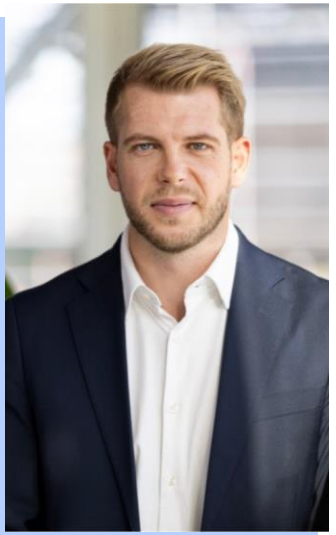
Nej tak til øget overvågning og logning

Som modsvar til dialogen i ekspertgruppen nævnte flere virksomheder i fokusgruppen imidlertid, at **der ikke var et ønske om øget overvågning** eller tekniske løsninger, der kan spores og logges fra centralt hold.

Vores fokusgruppe blev afholdt i en periode, hvor der var særlig fokus på et politisk forslag om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn, herunder screening af digital kommunikation, hvilket potentielt kan være en medvirkende årsag til, at dette har været på sinde for flere deltagere.

Flere deltagere pegede derfor på, at tekniske løsninger, der kan sikre dansk infrastruktur er en god ide, men at det ikke må være på bekostning af privatlivet.

Som et teknisk forslag til en langsigtet løsning kan ideen om et nationalt cyberfilter være med til at starte drøftelser af, hvordan vi bygger tekniske løsninger, der balancerer behovet for strukturelle løsninger og videndeling og respekten for privatlivets fred såvel som net-neutraliteten og ytringsfriheden.



"Cyberangreb stopper ikke ved virksomheders hoveddør, men rejser ubesværet på tværs af sektorer. Derfor skal vores cybersikkerhed også tænkes bedre sammen – både i tekniske løsninger og det bredere samarbejde."

Andreas Holbak Espersen, branchedirektør, DI Digital

Tak...

… til de mange deltagere, som har valgt at bidrage til udgivelsen af denne publikation. Foruden de virksomheder, som deltog i virksomhedspanelet og vores fokusgruppeinterview, vil vi rette en særlig tak til vores ekspertgruppe.

Kontakt os

Marc Bærentzen

Manager, KPMG

mbaerentzen@kpmg.com

Michael Mærsk-Møller

Manager, KPMG

mihansson@kpmg.com

Johan Rask Sønderborg

Konsulent, KPMG

jsoenderborg@kpmg.com

Maja Friis Henriksen

Chefkonsulent, DI Digital

mafh@di.dk