

Kom godt igennem cyberkrisen: *En kort guide til virksomhedens beredskab*

Stigning i antallet af cyberangreb mod danske virksomheder

Antallet af hackerangreb mod danske virksomheder er steget voldsomt de sidste par år og slår nye rekorder. På blot ét år (2021 til 2022) er andelen af virksomheders anmeldelser af hackerangreb steget med 64 procent.

En ny undersøgelse fra 2023 viser, at hver anden danske private og knap hver anden offentlige virksomhed ikke har kompetencerne til at håndtere et cyberangreb. Og mere end hver anden større, danske virksomhed har været ramt af mindst én sikkerhedshændelse, der har påvirket virksomheden negativt det seneste år.

Blandt andet den geopolitiske situation betyder, at danske virksomheder er særligt attraktive for cyberkriminelle, hvor en høj grad af digitaliserede arbejdsgange giver flere indgange til at angribe.

Det er ikke længere et spørgsmål om, hvornår cyberkrisen rammer – men at virksomheden skal forberede sig på at kommunikere i en krisetid.



Konsekvenser for virksomhedens omdømme

Et cyberangreb kan have katastrofale økonomiske konsekvenser og skade en virksomheds omdømme fatalt – uanset om der er tale om datalek eller ej.

At sikre sin virksomhed mod cyberangreb er ikke kun et spørgsmål om at have den rette software eller firewall på plads. Det handler i lige så høj grad om at have de rette procedurer og en klar beredskabsplan – og en plan for kommunikation, der passer til.

Seneste tal fra IBM viser, at nordiske virksomheder i gennemsnit bruger hele 335 dage på at håndtere brud på datasikkerheden – herunder 246 dage til at identificere hændelsen.

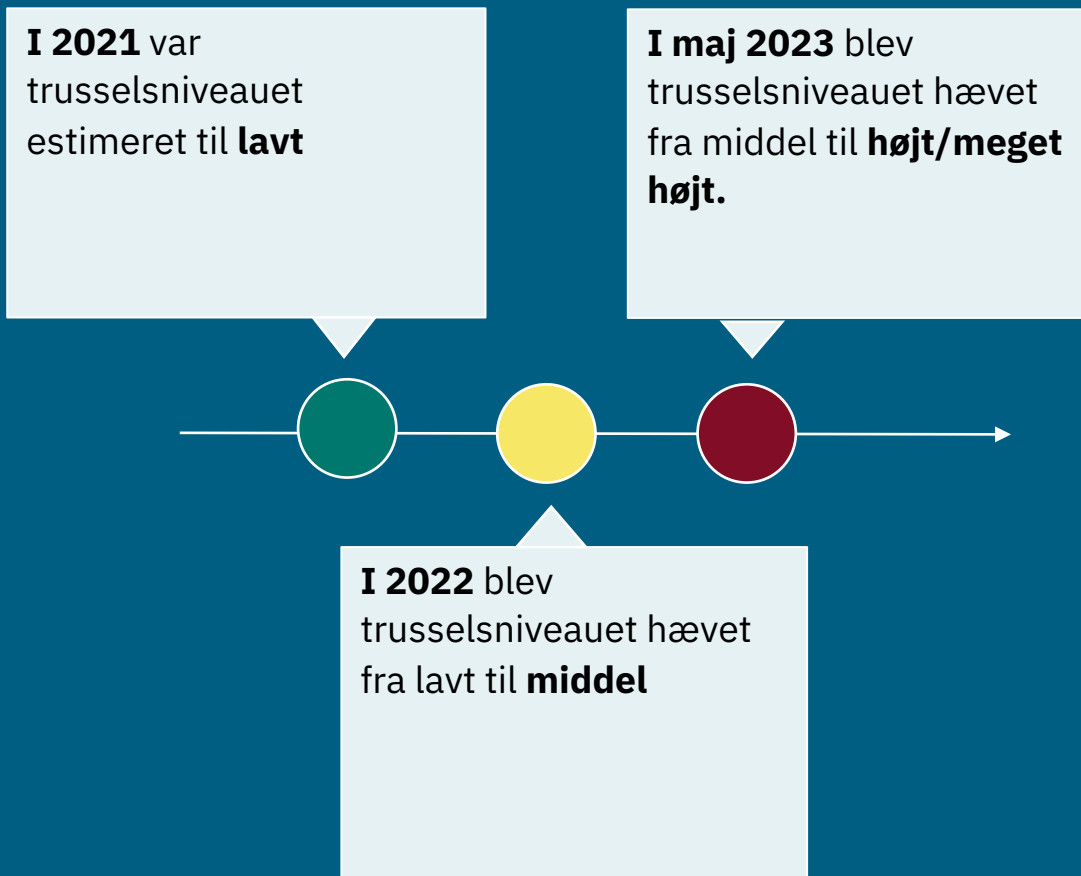
Alt imens kan selv mindre hackerangreb sprede sig til omverdenen med lynets hast med alvorlige konsekvenser til følge – herunder at ansatte kan miste deres arbejde eller at virksomhedens omdømme og virkemulighed lider alvorlig skade.

Et proaktivt beredskab mod cyberangreb med fokus på håndtering af kommunikation er derfor en afgørende forudsætning for at klare sig bedst muligt igennem med mindst mulig skadesvirkning.



Udviklingen af trusselsniveauet hos Center for Cybersikkerhed (CFCS) **de sidste tre år**

Gennemsnitsomkostningerne ifm. et databrud var sidste år 4,45 millioner amerikanske dollars, svarende til 30,3 mio. danske kroner – det højeste nogensinde på globalt plan, ifølge IBM.



Center For Cybersikkerheds (CFCS) nyeste rapport for 2023 viser, at truslen fra både cyberspionage og cyberkriminalitet fortsat er **MEGET HØJ**.

Både stater og kriminelle grupper har interesse i at kompromittere virksomheder i sektoren.

Hvem har ansvaret for cybersikkerhed i virksomhedens forretning?

Fra 2024 placeres ansvaret for virksomhedens cybersikkerhed direkte hos topchefen i udvalgte sektorer.

Med indførslen af IT-sikkerhedsdirektivet NIS2 (Network and Information Systems Directive), som blev implementeret i EU i januar 2023, bliver virksomheder i en række udvalgte sektorer fra 2024 pålagt et øget ansvar, da rammerne for IT-sikkerhedsarbejdet ændres.

Direktivet lægger nu ansvaret for misvedligeholdt eller forsømt cybersikkerhed hos virksomhedens ledelse – som skal risikostyre og implementere skadesforebyggende foranstaltninger.

Manglende overholdelse af direktivet, der træder i kraft medio 2024, kan medføre bøder på op til 75 mio. DKK eller to procent af virksomhedens omsætning – alt efter hvad der er højest.



Der er flere måder at forberede sig på et cyberangreb på.

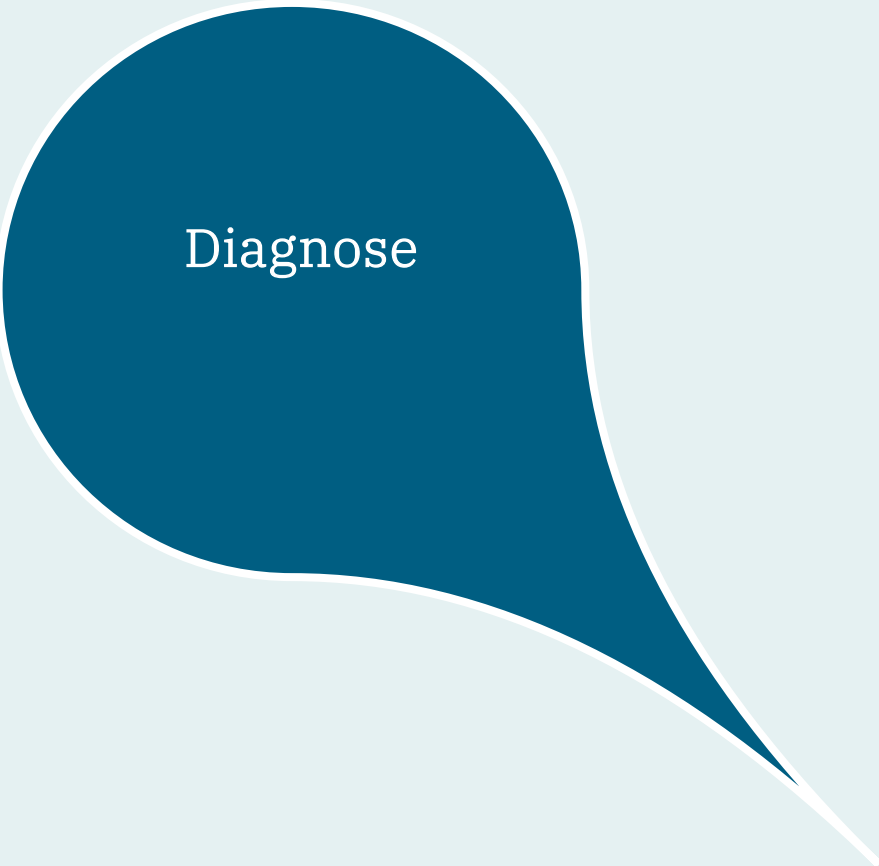
Spørgsmål, virksomheden kan stille sig selv inden et cyberangreb rammer:

Har virksomheden
sammen med
beredskabet en
særsomt plan for
kommunikation?

Er virksomheden
trænet i at
håndtere forskellige
risikoscenarier –
herunder
kommunikationen i
den forbindelse?

Er virksomhedens
talspersoner klædt på
til interviews og dialog
med medier?

Når cyberangrebet rammer virksomheden: **Stil diagnosen trin for trin** – med fokus på kommunikation



Diagnose

1. Beskriv situationen og status

2. Definer krisens root cause

**3. Identificer berørte og påvirkede
personer/afdelinger**

**4. Fastlægg virksomhedens grundlæggende mål og
forpligtelser**

**5. Gå virksomheden igennem med et 360-graders
perspektiv**

Har virksomheden sammen med beredskabet **en særskilt plan for kommunikation?**

En effektiv plan for håndtering af kommunikation hjælper med at beskytte mod skandaler, omdømmebeskadigelse og tab af kundefortrolighed.

Virksomheden kan afklare på forhånd, om der er klare retningslinjer og ansvarsdeling for håndtering af cybertrusler – og sikre, at de rette kommunikationspolitikker og beredskaber er på plads.

Dette kan omfatte alt fra intern kommunikation og kommunikation med interessenter – til rapporteringsforpligtelser og juridiske procedurer.

Kommunikationsberedskabet kan indeholde udvikling af kernefortælling, Q&A's, kernebudskaber samt intern og ekstern plan og timing for kommunikation.



Er virksomheden trænet i at håndtere forskellige risikoscenarier –
herunder kommunikationen i den forbindelse?

Træning af medarbejdere og ledelse
gør en stor forskel i forhold til at sikre,
at virksomheden kommer bedst muligt
gennem krisen.

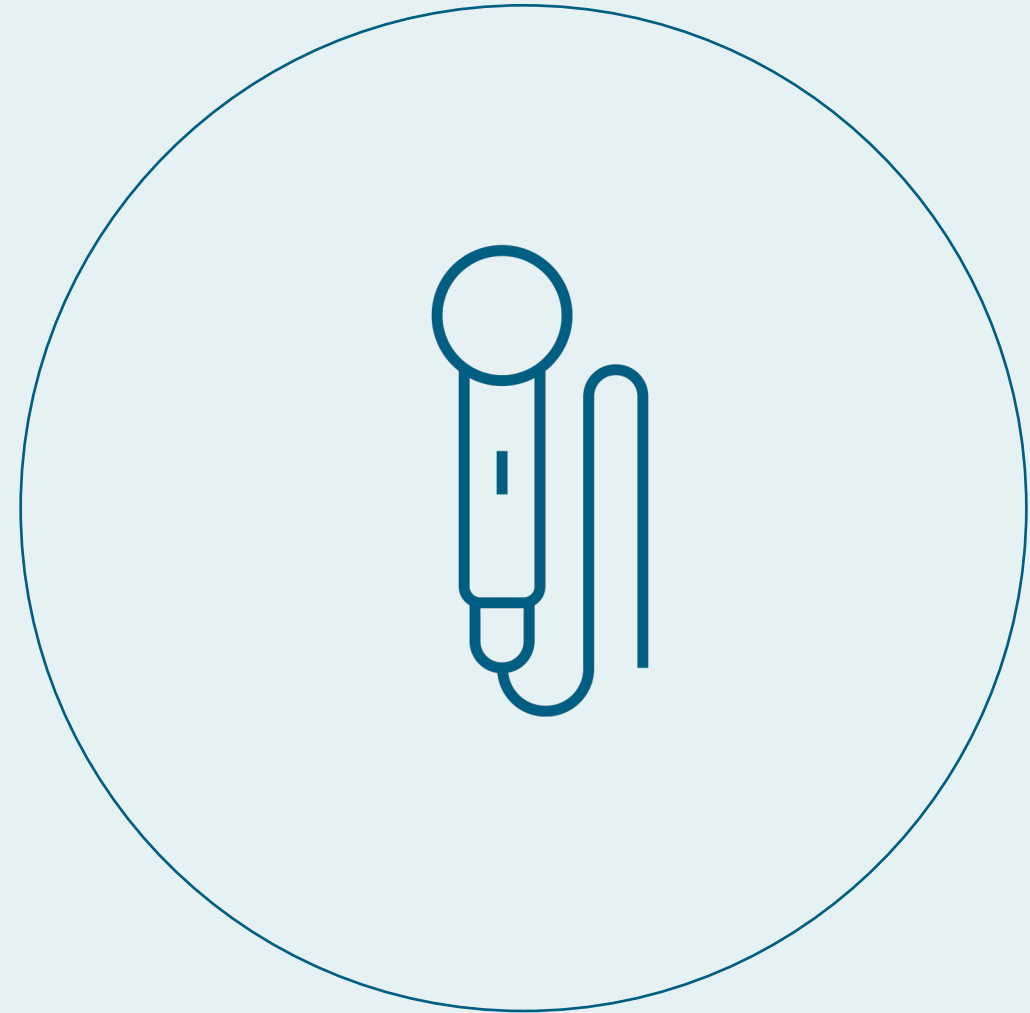
Dette kan indebære interne kriseøvelser, som træner organisationen i
håndteringen af kommunikation ifm. cyberangreb/IT-nedbrud.



Er virksomhedens talspersoner klædt på til **interviews og dialog med medier?**

Medie- og budskabstræning af virksomhedens talspersoner styrker evnen til at styre uden om de væsentligste faldgruber, når medierne henvender sig – og samtidig øge chancerne for at styre narrativet, formidle pointer og fremme mål med kommunikation.

Det kan omfatte træning af både hovedbudskaber såvel som teknikker og konkrete redskaber.



Vores principper for krisekommunikation – de 12 kriseregler

Hos Substantia arbejder vi med 12 kriseregler. Her er tre udvalgte:

- 1. Søg samarbejde og kommuniker direkte med de involverede parter**
Når det er muligt, vælg direkte dialog med de involverede – og undlad kommunikation gennem medierne.

- 3. Det, du giver opmærksomhed, får opmærksomhed**
Pas på med handlinger, der skaber flere nye problemer at løse; jagten på modparten eller opgør med modstandere.

- 10. Antag, at du i offentlighedens øjne er skyldig og privilegeret, indtil det modsatte er bevist**
Antag, at offentligheden vil se dig som ansvarlig. Vær proaktiv og transparent i din kommunikation for at ændre den opfattelse.

Læs mere

Få en første gennemgang af virksomhedens beredskab:
<https://substantia.dk/kriseklar/>

Cyberangreb og mediestorme

– er din virksomheds kommunikation kriseklar?

Virksomheder i Danmark er under alvorlige angreb fra cyberkriminelle. Den internationale politiske udvikling forstærker truslen.

Samtidigt rammer mediestorme, når markeder, forventninger og værdier støder sammen, og alle hensyn bliver svære at forene.

Det skaber kriser for virksomheder med pres på forretningen, driften og organisationen. Det kræver et stærkt beredskab at være klar til at stå imod og stille om.

Et beredskab for it, drift og organisation gør det ikke alene. Klare politikker og tydelig kommunikation er afgørende for at minimere krisens skadevirkninger.

Substantia har i år rådgivet adskillige virksomheder og institutioner, der har været udsat for ransomware og andre cyberangreb. Vi har startet topledelsen og interne kommunikationsteams under mediestorme – og forbedret beredskaber med metodisk gennemgang og øvelser.

Er din virksomhed kriseklar?

- Hver anden større danske virksomhed har været ramt af mindst en sikkerhedshændelse, der har påvirket virksomheden negativt i det seneste år*
- 6 ud af 10 virksomheder vil være ude af stand til at udføre deres primære opgaver ved et cyberangreb.
- Substantia styrker virksomheder og topledelsen med kriseøvelser, risikovurderinger og forbedrer beredskabsplaner.
- Vores erfarne seniorteam af kriserådgivere bistår før, under og efter krisen.

Vi kan ikke forudsige fremtiden. Men vi kan forberede os på den. Vi har en unik og gennemtestet metode til kriserådgivning og risikostyring. Book os til en første gennemgang og find ud af, hvordan din virksomhed er rustet:

📍 substantia.dk/kriseklar

Substantia er et strategisk kommunikationsbureau med fokus på supporteret kommunikation, branding & positionering samt kampagner. Når virksomheder økonomiske problemer støder sammen med det brede offentlige, får Substantia skærpe og ikke griber fat, er vi med til at finde fælles løsninger og skabe flere vindere. Vi rådgiver virksomheder, organisationer og den offentlige sektor og styrker tekniske kommunikationsressourcer inden for dybvideregående brancher og arbejder i Fordi nødder løsninger og værdiskabelse kræver forståelse for substantien.

*PwC Cybercrime Survey 2023

Risikostyring og krisekommunikation

Systematiseret risikovurdering

Kommunikationsberedskab 360 grader

De tolv kriseregler

Substantia
Fra strategi til løsning

PwC's Cybercrime Survey:
<https://www.pwc.dk/da/publikationer/2023/cybercrime-survey.html>

Cybercrime Survey 2023

Nye udfordringer kræver nyt fokus

Cybersikkerhed har høj prioritet i danske private og offentlige virksomheder, og stadig flere sætter ind over for cybertruslen. Det er nødvendigt, da nye lovgivnings- og sikkerhedsmæssige forandringer skærper kravene til virksomhedernes indsats inden for cybersikkerhed.

Hvordan kriser driver fundamentale forandringer:
<https://www.linkedin.com/pulse/farvel-til-kriseh%C3%A5ndtering-peter-goll/?originalSubdomain=dk>

Vil du høre mere om, hvordan vi kan hjælpe?



Peter Goll

Partner & Managing Director

E-mail
Peter.goll@substantia.dk

Telefon
+45 40 34 44 50



Louise Helstrup Guldager

Partner, Director of PR & Crisis
Management

E-mail
Louise@substantia.dk

Telefon
+45 29 90 93 25

Substantia
Pakhus 11
Dampfærgevej 2,
2100 København Ø

contact@substantia.dk
+45 31 35 69 79

CVR 39252783