

Cybersikkerhed for bestyrelse og direktion

Vejledning og anbefalinger til styrkelse af strategiske cyberkompetencer. September 2023 (V4.3)



Bestyrelsesforeningens
Center for Cyberkompetencer

KROMANN
REUMERT

Dubex:

INDUSTRIENS FOND



CENTER FOR
CYBERSIKKERHED

Denne publikation udgør ikke og kan ikke erstatte professionel rådgivning. Bestyrelsesforeningen eller dens samarbejdspartnere påtager sig ikke ansvar for tab som følge af handlinger eller undladelser baseret på publikationens indhold. Alle rettigheder forbeholdes.

Indhold

| | |
|---|-----------|
| Forord | 4 |
| Kontakt | 6 |
| ANBEFALINGER OG TJEKLISTE | 8 |
| Anbefalinger | 9 |
| Kort tjekliste | 10 |
| INTRODUKTION TIL CYBERSIKKERHED | 12 |
| Digital risiko i en global verden | 13 |
| Et regulatorisk paradigmeskifte | 16 |
| Cyberkompetencer og -ansvar i bestyrelsen | 18 |
| RISIKOSTYRINGSMODEL FOR CYBERSIKKERHED | 20 |
| Cybersikkerhedsstrategi | 21 |
| Opbygningen af en cybersikkerhedsstrategi | 22 |
| GRUNDLÆGGENDE OM CYBERSIKKERHED | 24 |
| Det digitale økosystem | 25 |
| Trusselsbilledet | 28 |
| Angrebsaktører | 30 |
| Cyberkriminalitet | 32 |

| | | |
|---------------|---|-----|
| VÆRKTØJSKASSE | | 34 |
| Tema 1 | Risikovurdering | 35 |
| Tema 2 | Risikoappetit | 38 |
| Tema 3 | Politikker, processer og beredskab | 42 |
| Tema 4 | Rapportering | 46 |
| Tema 5 | Kultur | 48 |
| Tema 6 | Governance | 50 |
| APPENDIKS | | 52 |
| Appendiks 1 | Regulatorisk landskab | 54 |
| Appendiks 2 | Sikkerhedsstandarder | 59 |
| Appendiks 3 | Template til cybersikkerhedsstrategi | 66 |
| Appendiks 4 | Template til bestyrelsesrapportering | 69 |
| Appendiks 5 | Cyberforsikringer | 90 |
| Appendiks 6 | Emner til bestyrelsens årshjul | 93 |
| Appendiks 7 | Leverandørsikkerhed | 96 |
| Appendiks 8 | Basal cyberhygiejne | 103 |
| Appendiks 9 | Personlig cybersikkerhed for bestyrelsesmedlemmer | 108 |
| Appendiks 10 | Akut checkliste ved cyberhændelser | 111 |
| Appendiks 11 | Geopolitiske overvejelser | 114 |
| Appendiks 12 | Ordliste | 117 |

Forord

Denne vejledning med anbefalinger til bestyrelser er udarbejdet som led i projektet ”Styrkelse af strategiske cyberkompetencer i danske virksomheder”.

Projektet, som blev startet i 2019 på initiativ af og med støtte fra Industriens Fond, ledes af Bestyrelsesforeningens Center for Cyberkompetencer A/S, og gennemføres i et tæt samarbejde med erhvervslivet, Forsvarets Center for Cybersikkerhed og CBS samt Aalborg Universitets Cyber Security Group.

Projektet har til formål at samle de stærkeste kompetencer og erfaringer med cybersikkerhed fra forskningen og rådgivningsbranchen og fra praksis i bestyrelseslokaler og direktioner med henblik på at udvikle, samle og distribuere nyeste viden og best practice til bestyrelsesmedlemmer og virksomhedsledere om trusler, risikostyring, modstandsdygtighed, strategi, krisestyring og governance indenfor cybersikkerhed.

Vejledningen er tilstræbt udarbejdet, så den kan favne på tværs af virksomheder uanset størrelse og branche m.v. Det er en eksplicit målsætning, at vejledningen og anbefalingerne skal kunne anvendes af bestyrelser og direktioner i mindre og mellemstore danske virksomheder.

Vejledningen tager udgangspunkt i bestyrelsens opgaver og ansvar for selskabet, dets medarbejdere, forretningsmodel og værdiskabelse.

Formålet med vejledningen er også at etablere en fælles referenceramme for bestyrelsesmedlemmers og direktioners forståelse af og samarbejde om strategi og risikostyring på cybersikkerhedsområdet.

Vejledningen tager, så vidt det har været muligt, højde for NIS2 og de kommende lovkrav til cybersikkerhed.

Styrkelse af strategiske cyberkompetencer i danske virksomheder gennemføres i samarbejde med en partnerkreds bestående af CBS, AAU, CBS Bestyrelsesuddannelserne, CFCS, Kromann Reumert, Dubex, KPMG, PwC, EY, IBM, Tryg, Global Connect, Jyske Bank, Nordea, Improsec, Beierholm, BDO, mfl. Desuden har projektet samarbejde med D-mærket, Dansk Standard, DI og Dansk Erhverv. Projektet har samarbejdsrelationer internationalt, bl.a. til World Economic Forum's Center for Cybersecurity og Global Cyber Alliance.

Bestyrelsesforeningens Center for Cyberkompetencer takker Industriens Fond og den samlede partnerkreds for samarbejdet og værdifulde bidrag til, at danske virksomheder og Danmark bliver blandt de bedste til at håndtere de stadig mere omfattende cybertrusler, og derved styrker konkurrenceevne og værdiskabelse – til gavn for virksomheder, aktionærer, stakeholders og samfund.


Denne vejledning blev første gang udgivet i december 2019, og er opdateret i 2020, 2021, 2022 og 2023. Herved foreligger version 4.3, sep. 2023.

Komitéen for God Fondsledelse henviser til vejledningen og anbefalingerne.

København, september 2023

Bestyrelsesforeningens Center for Cyberkompetencer A/S

Marianne Philip, Jens Stener og Kirsten Hede



Målgruppen er
bestyrelsesmedlemmer i danske
virksomheder, organisationer og
institutioner

Kontakt

Bestyrelsesforeningens Center for Cyberkompetencer A/S



Marianne Philip
Bestyrelsesformand
mp@kromannreumert.com



Jens Stener
Direktør
js@bestyrelsesforeningen.dk



Kirsten Hede
Projektdirektør
khe@bestyrelsesforeningen.dk



Information om uddannelsesdage mm.
www.bcfc.dk
www.bestyrelsesforeningen.dk

Generelle henvendelser:
cybersikkerhed@bestyrelsesforeningen.dk



BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance



**AALBORG
UNIVERSITET**



**CENTER FOR
CYBERSIKKERHED**

**KROMANN
REUMERT**

Dubex:



GlobalConnect

Nordea



JYSKE BANK

BEIERHOLM



ANBEFALINGER OG TJEKLISTE

*Til styrkelse af strategiske
cyberkompetencer i danske bestyrelser*

1. Risikovurdering - værdier og trusler

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året modtager og forholder sig til en opdateret risikovurdering på cyberområdet baseret på virksomhedens vigtigste værdier, it-infrastruktur, forretningsmodel, primære sårbarheder, sandsynlige trusler, mulige tab ved angreb samt mulige konkurrencemæssige vurderinger.

3. Politikker, processer og beredskab - delegering og operationalisering

Det anbefales, at

- bestyrelsen fører kontrol med, at cybersikkerhedsstrategien er operationaliseret i politikker, processer og forretningsgange.
- bestyrelsen fører kontrol med, at virksomheden har implementeret passende cyberhygiejne, herunder en relevant backup, der løbende er testet,
- bestyrelsen fører kontrol med, at virksomheden har testede beredskabs- og kommunikations-planer i tilfælde af alt fra hackerangreb til strømnedbrud.

5. Kultur - mennesker og træning

Det anbefales, at

- medlemmer af bestyrelse og direktion regelmæssigt følger specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift,
- virksomheden regelmæssigt har tilpassede uddannelses- og træningsprogrammer for bestyrelse, direktion og medarbejdere i relation til cybersikkerhed,
- bestyrelsen og daglig ledelse går forrest i at understøtte en stærk og bevidst cybersikkerhedskultur.

2. Risikoappetit - risikoafvejning og risikovillighed

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter virksomhedens cybersikkerhedsstrategi, herunder risikoappetit, baseret på en afvejning af virksomhedens generelle forretningsstrategi, forretningsmål, it-infrastruktur, generelle risikoappetit, sikkerhedsbudget og investeringsvilje m.v.

4. Rapportering - kontrol og tilsyn

Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul på linje med øvrige væsentlige risici,
- bestyrelsen har cybersikkerhed på agendaen på hvert møde, og modtager relevant rapportering forud for mødet med bl.a. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest, awareness aktiviteter og revisionsgennemgange, samt evt. forslag til supplerende tiltag.

6. Governance - kompetencer og organisering

Det anbefales, at

- bestyrelsen forholder sig til, om den har tilstrækkelige kompetencer og erfaring med risikostyring af it- og cyberrisici,
- virksomhedens sikkerhedsorganisation fagligt er direkte forankret på direktionsniveau, og rapporterer direkte til bestyrelsen,
- styrke virksomhedens cybersikkerhed gennem etablering af uafhængige risikostyringskontroller (lines of defence).

Tjeklisten er en opsummering af de væsentligste pointer fra ”værktøjskassen” indenfor hver af de 6 strategiske temaer (s. 34-51)

1. Risikovurdering – værdier og trusler

- ☐ Hvad er vores vigtige License to Operate (LtO) aktiver? (dvs. hvad vil vi gerne beskytte, hvad er vigtigt for vores forretning, hvad er kronjuvelerne?)
- ☐ Hvad truer vores vigtige LtO aktiver (trusselsvurdering)?
- ☐ Hvorfor skulle dette kunne ske (sårbarhedsvurdering)?
- ☐ Hvad er sandsynligheden for, at det sker?
- ☐ Hvad er konsekvensen af, at det sker (konsekvensanalyse)?
- ☐ Hvad har vi gjort for at reducere risikoen (i form af forebyggelse og beredskab)?

2. Risikoappetit – risikoafvejning og risikovillighed

- ☐ Hvad er virksomhedens overordnede digitale strategi og forretningsmål?
- ☐ Hvad er virksomhedens holdning til at prioritere beskyttelse – f.eks. helst at *forebygge* at hændelser kan opstå og/eller at bruge ressourcerne på et stærkt *beredskab*?
- ☐ Er cybersikkerhed en fast del af virksomhedens kvalitetssikringsprocesser (udvikling, indkøb, salg, outsourcing mv.)?
- ☐ Er der mellem forretningen og risiko-/kontrollfunktioner en fælles forståelse for cybersikkerhed og prioriteringer?
- ☐ Er der klarhed over, hvem der er ejer af de enkelte cyber risici?
- ☐ Kunne virksomheden med fordel indgå samarbejdsaftaler omkring cybersikkerhed eller afdække en del af risikoen via forsikring?
- ☐ Ud fra en samlet afvejning af risici >< omkostninger, hvad er virksomhedens tolerance for at påtage sig cyberrisici, herunder toleranceværdien for de enkelte risici, f.eks. risikotype, produkttype, kunder, strategi, målsætninger mv.?

3. Politikker, processer og beredskab – delegering og operationalisering

- ☐ Hvilke processer og værktøjer anvender virksomheden til at identificere sårbarheder og trusler?
- ☐ Har virksomheden et opdateret overblik over systemer og infrastruktur?
- ☐ Har virksomheden implementeret basal cyberhygiejne?
- ☐ Har virksomheden overvågning til at opdage, hvis der sker noget?
- ☐ Har virksomheden logning, og - hvis ja - hvad logger den på og hvor længe?
- ☐ Har virksomheden backup - og er backup beskyttet?
- ☐ Har virksomheden håndteret cybersikkerhedsrisici i kontrakter med leverandører, kunder mv.?

4. Rapportering – kontrol og tilsyn

- ☐ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?
- ☐ Er cybersikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ☐ Modtager bestyrelsen relevant rapportering fra direktionen om virksomhedens cybersikkerhed forud for hvert møde (med bl.a. risici, status, testresultater, investeringer, anbefalinger mv.)?
- ☐ Får virksomheden og/eller dens leverandører udarbejdet ekstern kontrol, f.eks. revisionserklæringer, på it-sikkerhed?

5. Kultur – mennesker og træning

- ☐ Følger medlemmer af bestyrelse og direktion regelmæssigt specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift?
- ☐ Er der et trænings- og uddannelsesprogram for medlemmer af bestyrelse, direktionen og medarbejdere, så de løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- ☐ Går bestyrelse og direktion forrest i at understøtte en stærk og bevidst cybersikkerhedskultur?

6. Governance – kompetencer og organisering

- ☐ Har medlemmer af bestyrelse og direktion tilstrækkelige kompetencer og erfaring med risikostyring af it- og cybersikkerhedsrisici?
- ☐ Holder bestyrelse og direktion sig løbende orienteret om de cybertrusler og aktører, der truer virksomheden, deres metoder og motivation?
- ☐ Har virksomheden en sikkerhedsorganisation, der er fagligt forankret direkte på direktionsniveau, f.eks. CEO, CFO eller CIO?
- ☐ Hvor i organisationen (person/funktion) ligger ansvaret for cybersikkerhed, og rapporterer denne til de rette på ledelsesniveau?
- ☐ Hvem har risikostyringsansvaret?
- ☐ Hvem kontrollerer hvad (lines of defense)? – Kontrollerer risikoejeren sig selv?
- ☐ Hvem holder styr på risikoeksponeringen fra leverandører?
- ☐ Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- ☐ Hvor meget af sikkerheden står virksomheden selv for, og hvor meget er lagt ud til tredjepart?



INTRODUKTION TIL CYBERSIKKERHED

Digital risiko i en global verden

Danske virksomheder er blandt de mest digitaliserede i verden. Selv virksomheder, som ikke ser sig selv som digitale, har i dag digitale løsninger til understøttelse af salgs- og kundeprocesser, økonomi og administration, indkøb, produktion m.v.

Internettet og digitale løsninger er for de fleste virksomheder blevet afgørende for deres forretning og konkurrenceevne.

Virksomhederne har således øget deres sårbarhed overfor digitale nedbrud og angreb. Samtidig er truslen fra cyberangreb steget de senere år. Med den geopolitiske udvikling er der tale om et permanent forhøjet trusselsbillede.

Virksomhedsledere, der har prøvet et cyberangreb, fremhæver, at det har været deres værste mareridt, og at cyberrisici er en af de største og mest fundamentale risici, en virksomhed står overfor i dag.

Det særlige ved cybertruslen er, at den banker på virksomhedens digitale dør til internettet hvert eneste minut - og på tværs af landegrænser. Det er den risiko, man som bestyrelse og direktion skal kunne forstå og forholde sig til.

Cybertruslen *er* reel, og ledelsen er nødt til at have en strategi for at håndtere den.

De fleste virksomheder og organisationer er langt mere sårbare over for cyberangreb, end de (og deres bestyrelse og direktion) er klar over. Der er ofte en falsk oplevelse af tryk og sikkerhed. Dette står i kontrast til, at konsekvenserne af mangelfuld cybersikkerhed kan være særdeles omkostningsfulde og forretningskritiske.

Virksomheders arbejde med cybersikkerhed handler om mere end IT og teknologi. For ledelsen handler det også om governance, ledelse og risikostyring.

Bestyrelse og direktion bør systematisk og løbende arbejde med (klassiske og sædvanlige) discipliner som risikostyring og risikoanalyse for it-sikkerhed, driftskontinuitet, krisestyring, leverandørsikkerhed, ledelses- og kontrolfunktioner – samt basal cyberhygiejne og cybersikkerheds-træning.

Det handler om beskyttelse af virksomhedens "fundament"; dét, der i denne vejledning omtales som virksomhedens "*license to operate*" eller "*LtO*" (se side 18 for yderligere forklaring af LtO-begrebet).

Det er ikke kun i it-afdelingen, at virksomhedens digitale beskyttelse skal ske. De dage er forbi, både fordi bestyrelse og direktion er - og bliver - pålagt væsentlige pligter, og fordi bestyrelse og direktion kan eksponeres for ansvar.

Ledelsesfokus er afgørende for, at der kan opnås et passende og forholdsmæssigt sikkerhedsniveau – både teknisk og organisatorisk.

En klar erkendelse af, at cybersikkerhed er væsentligt og på linje med andre strategiske prioriteter, er i dag en nødvendighed.

Cyberrisikoen kan opleves som diffus, uoverskuelig og kompleks, og risikobilledet udvikler sig hele tiden. Det indebærer, at cyberrisikoen ofte

ikke håndteres effektivt - hverken i virksomheden eller dens ledelse (direktion og bestyrelse).

Arbejdet med en cybersikkerhedsstrategi kræver basal IT-forståelse, men er IKKE en IT-opgave. Det er en ledelsesopgave på øverste niveau. Det er derfor afgørende, at bestyrelse og direktion ved, hvad der er digitalt kritisk for virksomhedens forretning, drift og overlevelse, og at der er strategier, politikker og planer på plads for beskyttelse af de vigtige digitale aktiver og aktiviteter.

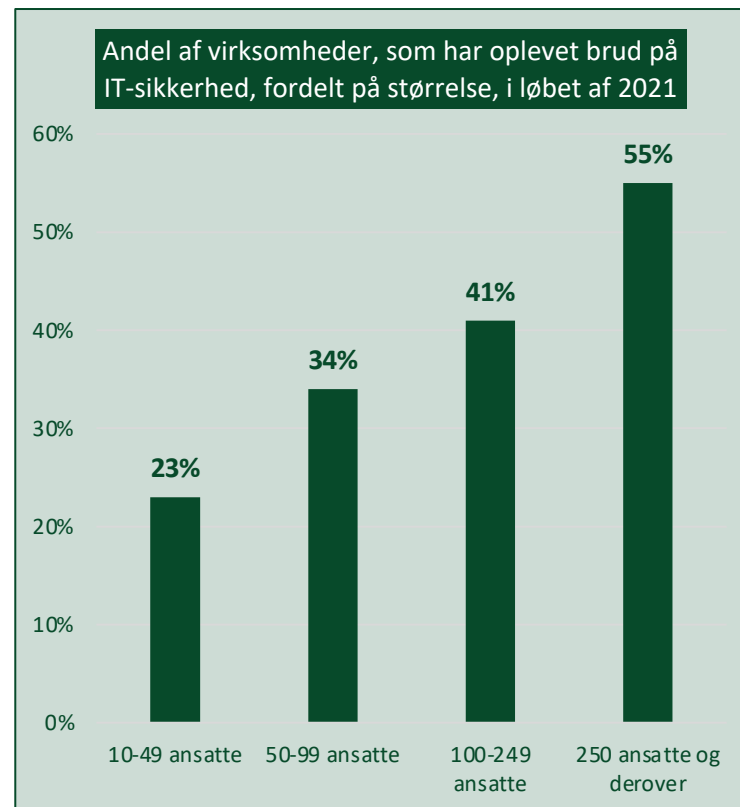
Til dette formål har bestyrelsen ansvar for, at der tilvejebringes, udmøntes og følges op på en strategi for risikostyring af cybersikkerhed. Det er dét, denne vejledning omhandler.

Undersøgelser viser, at det gennemsnitligt kan tage over 200 dage at opdage et brud (time to identify) og 70 dage at reparere og genskabe (time to contain)



Kilde: IBM, Cost of a Data Breach Report 2022

Godt hver fjerde lille virksomhed har oplevet brud på IT-sikkerheden i løbet af 2021



Kilde: Danmarks Statistik og SMV Danmark temaanalyse, 2022

Et regulatorisk paradigmeskifte

Digitalisering og cybersikkerhed er to sider af samme mønt. Det bliver afspejlet i den måde, EU skruer op for ny regulering, der skal beskytte vores digitale aktiver, data og et sikkert globalt internet.

EU har udnævnt 2020'erne til det "digitale årti", og har som mål, at Europa skal være den globale frontløber indenfor digitalisering.

I de kommende år går cybersikkerhed fra at være sparsomt reguleret til at blive detailreguleret.

Nye regler kommer til at skærpe kravene til cybersikkerhed for en lang række virksomheder, og til bestyrelsens rolle og ansvar for at sætte rammerne for at styre cyberrisici i relation til virksomhedens vigtigste systemer, processer og roller (det, vi i denne vejledning omtaler som *License to Operate (LtO)* aktiver).

Således vil bl.a. et nyt net- og informationssikkerhedsdirektiv (NIS2, der er opfølgningen på det første NIS-direktiv, der trådte i kraft i 2018) og en ny forordning om digital modstanddygtighed indenfor den finansielle sektor (DORA – The Digital Operational Resilience Act) øge kravene til cybersikkerhed betydeligt.

NIS2 og DORA blev vedtaget af EU i december 2022, og er gældende i dansk ret (dvs. skal opfyldes fra) den 17. oktober 2024 (NIS2) hhv. den 17. januar 2025 (DORA).

De nye cybersikkerhedsregler stiller bl.a. krav til, at danske virksomheder øger modstanddygtigheden overfor cyberangreb, herunder sikrer en risikobaseret ledelsesforankring.

Således vil NIS2-direktivet bl.a. indeholde skærpede ledelseskrav, krav til uddannelse, minimumskrav til risikostyring og foranstaltninger, underretning af myndigheder om sikkerhedshændelser indenfor 24-72 timer, bøder for overtrædelser og sanktioner i forhold til ledelsen.

Anvendelsesområdet for NIS2 udvides i forhold til de gældende regler. Flere sektorer indlemmes under NIS2, og flere virksomheder falder ind under reglerne.

Som udgangspunkt er virksomheder underlagt NIS2's anvendelsesområde, hvis de opererer indenfor én af sektorerne i tabellen ovenfor, og ikke er små virksomheder eller mikro-virksomheder (dvs. virksomheder med under 50 ansatte, og en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. EUR). Det skønnes, at 1.000-2.000 danske virksomheder bliver direkte omfattet af NIS2.

Selv om virksomheden (og dens ledelse) ikke omfattes direkte af NIS2-direktivet, bliver NIS2-kravene en grundlæggende standard, der (helt eller delvist) bliver best practices i markedet.

NIS2 får dermed også en afledt effekt på små virksomheder, selvom de ikke omfattes direkte af reglerne. For mindre virksomheder vil det derfor under alle omstændigheder være fornuftigt at orientere sig imod de kommende NIS2-krav.

Leverandører og underleverandører til virksomheder, der omfattes af NIS2, kan ligeledes blive stillet overfor kontraktuelle og kommercielle krav om overholdelse af sikkerhedskrav som en afledt effekt af NIS2.







De fleste virksomheder arbejder allerede med it-sikkerhed i dag. Det vurderes dog, at de færreste opfylder

NIS2-kravene eller de krav, som allerede følger af almindelig god praksis. Det siger langt det meste erfaring fra arbejdet med ledelsesgrupper.

Med tanke på, at der formentlig ligger en del arbejde for mange virksomheder i at løfte deres sikkerhedsniveau, er det ikke for tidligt at begynde nu. Danske virksomheder har ikke haft mange år til at forstå og styre cyberrisici, og NIS2 (cybersikkerhed) er ikke det samme som GDPR (persondataskyts). Det er forventeligt, at opgaven – tilgang og prioriteter – kan blive vanskelig for mange.

De fleste vil dog være godt på vej, hvis de anvender en systematisk tilgang og principperne i denne vejledning.

Sektorer omfattet af NIS2

| | | | | |
|--|---|--|--|--|
|  Energi |  Transport |  Bank / finans |  Post/pakke |  Digitale serviceudbydere |
|  Sundhed |  Drikkevand |  Spildevand |  Affald |  Kemiske produkter mv. |
|  Digital infrastruktur |  Offentlig administration |  Rumfart |  Fødevarer |  Andre vigtige produkter (pharma, biler, maskiner mv.) |

Cyberkompetencer og -ansvar i bestyrelsen

Det er en klar bestyrelsesopgave og et klart bestyrelsesansvar at behandle, godkende og føre tilsyn med virksomhedens risici, herunder cyberrisici.

Bestyrelsen har ansvaret for at sikre, at der udarbejdes en cybersikkerhedsstrategi til styring af cyberrisici.

Dette skal bestyrelsen bl.a. gøre for at:

1. beskytte og skabe afkast af de aktiver og den forretning, som bestyrelsen er sat til at varetage på vegne af ejerne, og
2. leve op til sit ledelsesansvar, som - for nogle bestyrelser - underlægges skærpede lovkrav fra 2024 (NIS2), herunder krav om uddannelse og bøder for mangelfuld risikostyring.

Bestyrelser og direktioner har derfor behov for løbende viden om og grundlæggende kompetencer til risikostyring indenfor cybersikkerhed.

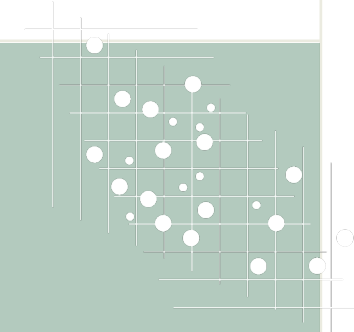
Risikostyring indenfor cybersikkerhed omfatter at forstå, identificere, analysere, prioritere og håndtere risiko (her blot på det strategiske niveau).

Det er vigtigt at holde sig for øje, at alle risici ikke kan fjernes helt og, lige så vigtigt, at risikoen udvikler sig over tid, og løbende skal genvurderes og genanalyseres.

Ved at anvende en systematisk tilgang kan ledelsen fastlægge en solid og forretningsunderstøttende cybersikkerhedsstrategi, herunder beslutte risikoprofil, målsætninger og investeringer, på et oplyst grundlag.

Grundlæggende spørgsmål til cybersikkerheden er bl.a.:

- Har vi overblik over cyber trusselsbilledet?
- Forstår vi i bestyrelsen og direktionen virksomhedens (digitale) værdier og de konkrete cyberrisici?
- Har vi en cybersikkerhedsstrategi og er governance på plads, så vi både kan beskytte vores aktiver og afværge konsekvenser af et angreb, når/hvis det kommer?



Bestyrelsen behøver cyberkompetencer for at:

- ✓ Varetage det generelle bestyrelsesansvar
- ✓ Beskytte virksomhedens aktiver, forretningsprocesser, kunder og samarbejdspartnere.
- ✓ Skabe vækst og udnytte forretningsmuligheder i en digital tidsalder.
- ✓ Drøfte og beslutte virksomhedens risikoprofil og investeringsvilje.

RISIKOSTYRINGSMODEL FOR CYBERSIKKERHED

Cybersikkerhedsstrategi

Arbejdet med en cybersikkerhedsstrategi er en ledelsesopgave for bestyrelse og direktion, og omfatter alle afdelinger og funktioner i virksomheden. Arbejdet med strategien er sammenfattet i denne vejlednings 6 temaer, som bør behandles og besluttet i bestyrelseslokalerne:

Tema 1 - Risikovurdering: Identifikation af virksomhedens *License to Operate* (LtO) aktiver og de risici, som disse aktiver er udsat for.

Tema 2 – Risikoappetit: Fastlæggelse af risikoafvejninger og risikovillighed.

Tema 3 – Politikker, processer og beredskab: Delegering og operationalisering af strategien.

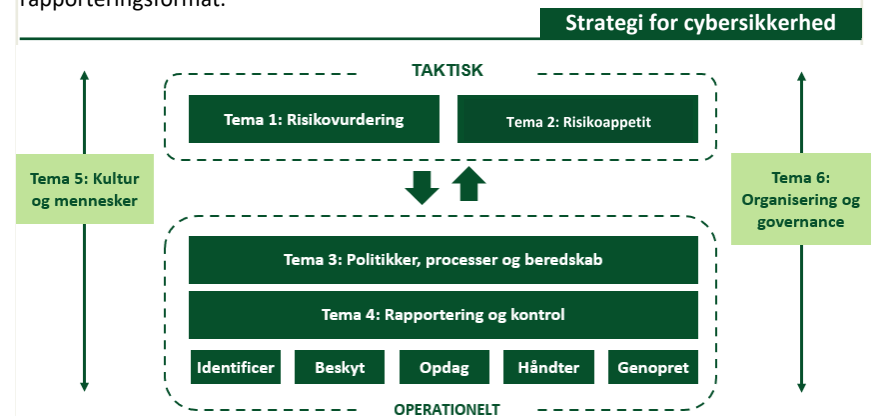
Tema 4 – Rapportering: Implementering af kontroller og rapporteringsformat.

Tema 5 – Kultur: Forankring gennem kultur og mennesker, herunder ved træning af direktion, bestyrelse og medarbejdere; og

Tema 6 – Governance: Etablering af en governancestruktur med klar organisering og afdækning af relevante kompetencer.

Målsætningen med cybersikkerhedsstrategien er at rammesætte de operationelle elementer til at *identificere, beskytte, opdage, håndtere* og *genoprette*. Disse 5 funktioner svarer til internationalt anerkendte rammeværker, herunder det amerikanske NIST-rammeværk.

Opfyldelsen af målsætningen bør løbende behandles i bestyrelsesrapporteringen.



Opbygningen af en cybersikkerhedsstrategi

Forudsætninger – og LtO aktiver

Cybersikkerhedsstrategien bør overordnet handle om at beskytte virksomhedens *License to Operate* ("LtO") aktiver.

Med *LtO aktiver* menes de vigtige og/eller mest beskyttelsesværdige aktiver og aktiviteter, der understøtter virksomhedens drift og indtjening. Dette kan være såvel fysiske som immaterielle aktiver som rettigheder, mennesker, processer, omdømme, regulering, kontraktforpligtelser m.v.

Den grundlæggende forudsætning for at udarbejde strategien er at have et klart billede af bl.a.:

- Virksomhedens overordnede strategi og forretningsmodel,
- Virksomhedens LtO aktiver og konsekvenserne af, at disse kompromitteres,
- Virksomhedens organisatoriske og tekniske opbygning og forudsætninger,
- Virksomhedens minimumskrav til cybersikkerhed, og
- Virksomhedens digitale leverandører, outsourcing og samarbejdspartnere.

Risikoforståelse

Bestyrelsen har ansvaret for, at det samlede risikobillede afspejler de relevante cybersikkerhedsrisici.

Det kræver en ensartet risikoforståelse og en konsistent model eller tilgang for risikohåndtering.

Bestyrelsen bør sætte rammerne for, hvordan virksomheden skal forstå og arbejde med risiko.

Cybersikkerhedsrisici er alle de forhold, som truer virksomhedens LtO aktiver.

Ledelsen bør således – på tværs af virksomheden – skabe et fælles sprog og forståelse af:

- hvad risiko er, og
- hvornår en risiko er væsentlig eller uvæsentlig.

Når der er en fælles forståelse af risiko, kan bestyrelsen for hvert område, herunder de væsentlige LtO aktiver, lave en vurdering af, om risikoen kan accepteres eller bør reduceres.

Governance

Bestyrelsen bør rammesætte governance for beskyttelse af det digitale. Dette kan gøres ved grundlæggende at svare på:

- Hvem gør hvad, hvorfor og hvornår?,
- Hvem kontrollerer hvem?, og
- Er der konfliktende interesser / forhold?

Cyber governance kan med fordel forankres i et årshjul, hvor bestyrelsen i årets gang løbende forholder sig til, hvordan virksomhedens digitale beskyttelse og organisering udmøntes. Virksomheden bør hertil arbejde systematisk med placering af ansvaret for politikker og kontrol heraf (*lines of defence*).

Opbygning af strategien

Ud fra et strategisk og ledelsesmæssigt perspektiv kan cybersikkerhedsstrategien med fordel tage udgangspunkt i de 6 temaer i denne vejledning.

Se Appendiks 3 for yderligere vejledning og forslag til udarbejdelse af en cybersikkerhedsstrategi.

Strategien kan som eksempel bygges op med følgende hovedafsnit:

1. Formål og baggrund, herunder i) hvorfor det er vigtigt at efterleve strategien, ii) bestyrelsens rolle og delegation til direktionen, iii) hvem der er ansvarlig for udmøntning af strategien, iv) operationel og kulturel forankring af strategien, og v) cybersikkerhed ud fra en risikobaseret tilgang.
2. Den samlede risikotilgang, herunder i) hvordan man arbejder systematisk med trusler, sårbarheder, modenhed og LtO aktiver, samt ii) hvordan arbejdet med cybersikkerhed rapporteres og kontrolleres / auditeres.
3. Mest beskyttelsesværdige aktiver og kritiske områder, herunder i) fysisk adgang, ii) teknologi-anvendelse, iii) udvikling og kvalitetssikring, iv) beredskab, samt v) hvordan kontroller, audit og rapportering skal ske.
4. Udarbejdelse af politikker og tilgange, herunder i) politikernes gyldighedsområde og deres ledelsesmæssige godkendelse, og ii) at beslutninger træffes på baggrund af risikoappetit og risikovurdering
5. Den konkrete governance, herunder hvordan projekter og initiativer vurderes, kontrolleres, organiseres og finansieres.

GRUNDLÆGGENDE OM CYBERSIKKERHED

Det digitale økosystem

Moderne virksomheder er digitalt forbundne, og kommunikerer på kryds og tværs. Stort set alle interne som eksterne relationer og afhængigheder har digitale elementer.

Det medfører, at risikovurderingen også må forholde sig til potentielle følgevirkninger fra cyberhændelser hos kunder, samarbejdspartnere mv. For eksempel: *"Hvis nu det system bliver ødelagt, eller vi ikke kan få dette råmateriale, hvordan påvirker det så vores virksomhed?"*

I den kommende tid øges kravene til, hvad virksomheder skal gøre for at beskytte sig mod cybertrusler. Dette kommer bl.a. til at omfatte krav til beskyttelse mod angreb fra forsyningskæden og mod, at virksomhedens ressourcer anvendes til at angribe andre.

Bestyrelse og direktion skal ikke vide alt. For at kunne vurdere sårbarheder, trusler, tiltag og sikkerhedsniveau, er det imidlertid relevant at forstå de hovedelementer, der indgår i et digitalt økosystem, dvs. det, der får en digitalt afhængig virksomhed til at fungere.

Et digitalt økosystem er som et løg: I midten er brugeren, der anvender sin PC, tablet, mobil m.v. til at tilgå data. Vi bruger alle apps, kort for applikation, som er den software, vi bruger til at

oprette, vedligeholde eller omforme data.

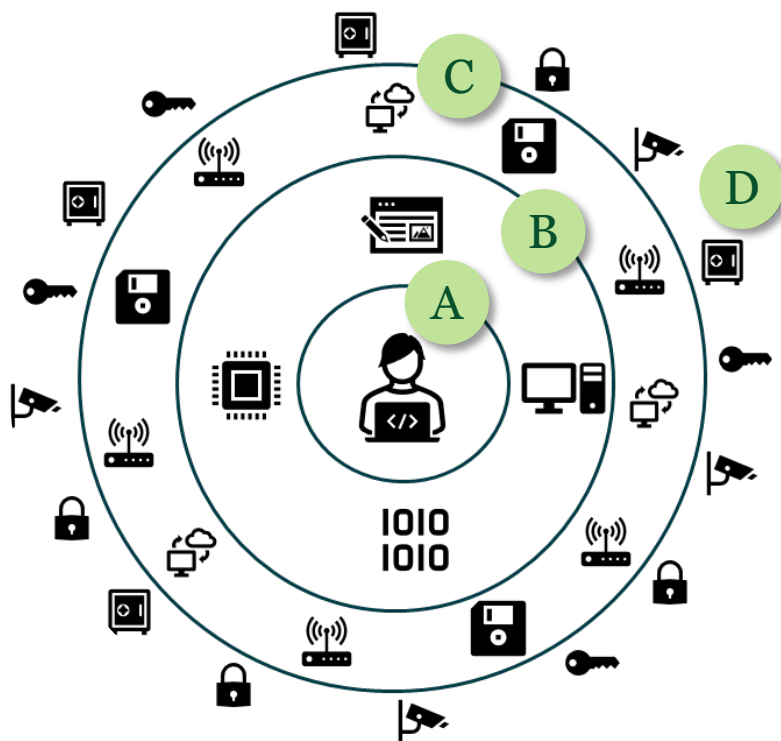
Alle disse data bliver opbevaret, transporteret, beskyttet m.v. af it-udstyr, dvs. servere, data-lagringsudstyr, udstyr til backup, PC'er, tablets, mobiltelefoner, routere, trådløst kommunikations-udstyr, kabling osv. Dette kaldes også hardware.

De programmer, som står for enten at *gemme* data (i databaser), *formidle* data (middleware eller en service-bus), eller *vise* data på internettet (webapplikations-software), bruger hardware.

Grundlæggende kræver et digitalt økosystem både software og hardware. For at gøre det lidt mere komplekst kan man stort set få en hvilken som helst funktion som en service, hvor en tredjepart står for at vedligeholde, opdatere og drifte såvel hardware som software ("as-a-service" løsninger, som f.eks. Software-as-a-Service, og cloud-løsninger er andre ord herfor).

Virksomhedens digitale økosystem hænger sammen med andres digitale økosystemer gennem internettet. Det er vigtigt at forstå, at sårbarheder kan opstå på alle niveauer, og at hackere kan udnytte alle led i kæden. Og de går altid efter det svageste led.

Illustration af et digitalt økosystem



Forklaring

A

Brugerne af virksomhedens it-løsninger er omdrejningspunktet for alt, herunder at man kan tilgå og forandre data og understøtte forretningen gennem de digitale løsninger.

B

Brugerne tilgår programmer, som afvikles på it-udstyr. Bestyrelsen og ledelsen delegerer opgaveansvar for vedligeholdelse af det samlede it-økosystem til it-afdelingen.

C

Placeringen af det digitale it-økosystem kan være internt eller eksternt (on-premises eller outsourcet). Ansvar for at de rigtige valg er truffet vil altid ultimativt ligge hos virksomhedens direktion og bestyrelse.

D

Alle del-elementerne i det digitale økosystem skal beskyttes; det skal overvåges, systemer skal sikkerhedshærdes, og der skal være veldefinerede roller og klar delegering.

Trusselsbilledet

Trusselsbillede

Teknologi og digitalisering giver mulighed for bedre kvalitet, service, effektivitet, funktionalitet og styrket konkurrenceevne. Det introducerer dog også nye alvorlige risici, der kan have stor betydning for virksomheden.

Den øgede digitalisering skaber afhængighed af de digitale løsninger, som dermed er et potentielt mål for cyberangreb.

Virksomheder kan blive ramt af en lang række forskellige former for cyberangreb. Det aktuelle cybertrusselsbillede er alle virksomheder nødt til at indrette sig efter.

Store dele af trusselsbilledet er identisk uanset branche, størrelse og virksomhedstype. Men der er typisk særlige forhold, som den enkelte virksomhed skal forholde sig til afhængig af virksomhedens systemopbygninger og branche. Dvs. virksomheden må også lave sin egen individuelle vurdering af truslerne.

Motiv, metode og mulighed

Et cyberangreb kræver, at tre faktorer er tilstede: *Motiv, Metode og Mulighed for angreb.*

Muligheder for angreb er typisk udtryk for sårbarheder, mens *Motiv* og *Metode* er egenskaber ved truslerne.

Sårbarheder

Sårbarheder er tekniske, operationelle og menneskelige svagheder, som en angriber kan udnytte. Kendetegnende for sårbarheder er, at det er muligt at beskytte sig mod, eller reducere risikoen for, at de udnyttes, ved hjælp af sikkerhedsforanstaltninger.

Trusler

De fleste trusler er eksterne, og afhænger af angrebsaktørernes motiver og metoder (se eksempler på trusler på side 27).

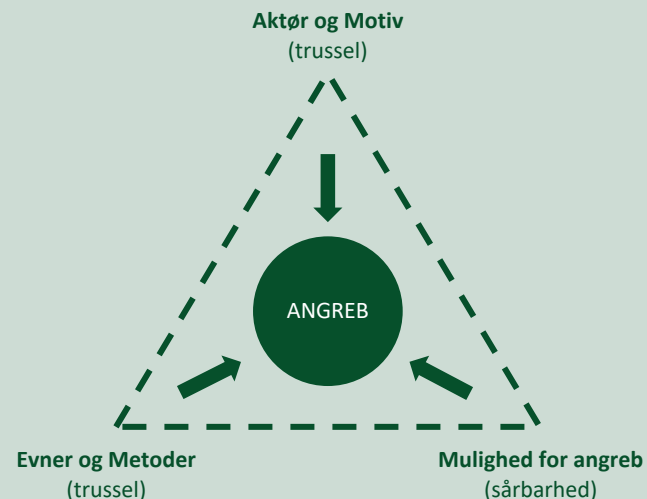
Det *eksterne* trusselsbillede består af to hovedelementer:

- Et alment generelt trusselsbillede som alle virksomheder, uanset branche, skal forholde sig til (typisk økonomisk kriminalitet); og
- Et specifikt trusselsbillede rettet mod enkelte brancher og virksomheder (typisk spionage, sabotage m.v.).

Trusselsvurderinger

Center for Cybersikkerhed (CFCS) udgiver løbende trusselsvurderinger, herunder indenfor specifikke sektorer, som virksomheder kan anvende i deres risikovurdering, når de skal prioritere deres beskyttende indsats.

Se CFCS' hjemmeside:
<https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/>



Angrebsaktører

De væsentligste angrebsaktører er i dag:

1. Cyber kriminelle
2. Fremmede stater (typisk efterretningstjenester)
3. Aktivister
4. Terrorister
5. Insidere

I de senere år har der været en generel tendens til, at angriberne har øget brugen af sløring og maskering af deres angreb.

Det betyder, at mange angreb er blevet vanskelige at beskytte sig mod og opdage, blandt andet fordi angriberne nu meget professionelt og ugenomsksueligt misbruger brugernes tillid til anerkendte virksomheder og organisationer.

De cyberkriminelle driver virksomheder, der gør brug af anonymiserings-platforme, som eksempelvis TOR-nettet der også er kendt som The Dark Net, ligesom de (mis)bruger andre angrebsaktørers værktøjer og metoder. De har kort sagt et professionelt samarbejde, ”Crime-as-a-Service”, der bedst kan sammenlignes med platformsøkonomi.

Dette kan gøre det vanskeligt for både myndigheder, virksomheder og private at fastslå, hvem der egentlig står bag et angreb.

Forskellige angrebsaktører samarbejder, f.eks. kriminelle aktører og fremmede stater, og udveksler viden og metoder.

Særligt har statsaktørerne mange ressourcer til rådighed, og de har i de senere år øget deres offensive kapacitet.

I forlængelse heraf ses en tendens til, at statsaktørernes værktøjer og metoder ”siver” over i de (øvrige) kriminelle miljøer.

Det betyder, at angrebsaktører i dag har adgang til højt udviklede og effektive angrebsværktøjer.

Medmindre man som virksomhed har særlige forsknings- eller forretningshemmeligheder, udfører særligt samfundskritiske eller følsomme opgaver, eller har en anden særlig samfundsmæssig betydning, har fremmede stater og efterretningstjenester som regel ikke interesse i måltettet at angribe virksomheder. Man skal imidlertid være opmærksom på følgevirkninger ved outsourcing, leverandørforhold og lignende.

Illustration af et trusselsbillede

| | |
|-----------------------------------|---|
| Aktører | Organiserede kriminelle |
| | Stater og regeringer (efterretningstjenester) |
| | Politiske aktører (aktivister og terrorister) |
| | Vandaler |
| | Interne |
| Motiver | Cyber kriminalitet / økonomisk kriminalitet |
| | Cyber spionage / industrispionage |
| | Cyber aktivisme / politisk motiveret |
| | Cyber terror |
| | Destruktive cyberangreb (vandalisme) |
| Mulighed for angreb (sårbarheder) | Sårbarheder i software |
| | Dårlige passwords / manglende multifaktor |
| | Manglende opmærksomhed/træning |
| | Fejlkonfiguration |
| | Forkerte rettigheder |
| | Usikre produkter / designs |
| | Dårlige processer |
| Metoder | Phishing |
| | Malware |
| | Ransomware |
| | DDoS |
| | Hacking |
| Angreb | Internetsvindel (CEO fraud) |
| | Tyveri af kreditkortinformation |
| | Identitetstyveri og tyveri af ressourcer |
| | Denial of business (DDoS og ransomware) |
| | Målrettede angreb efter fortrolig information |
| | Informationslækage |
| | Sabotage |

Cyberkriminalitet

Blandt angrebsaktørerne er de cyberkriminelle de mest aktive, og de står bag mere end 80% af alle eksterne angreb.

De kriminelle driver en forretning, og motivet for deres angreb er simpelt økonomisk vinding - så nemt og så hurtigt som muligt. De er derfor meget opportunistiske med hensyn til hvem, de angriber.

De mest professionelle kriminelle er organiseret i mafia- eller virksomhedslignende organisationer med flere hundrede ansatte. De befinder sig ofte i lande, hvor myndighederne ikke har interesse i at stoppe deres aktiviteter, og/eller som helt/delvist støtter deres aktiviteter.

Den aktuelt største trussel mod de fleste danske virksomheder kommer således fra kriminelle, der angriber for at tjene penge. Angreb sker primært indenfor to områder: 1) Ransomware og 2) økonomisk bedrageri.

1) Ransomware er "digital gidseltagning", hvor kriminelle låser virksomhedens data, og kræver en løsesum for den nøgle, der kan låse data op igen. Ofte kombineres angrebet med tyveri af data, som de kriminelle truer med at lække, hvis løsesummen ikke betales.

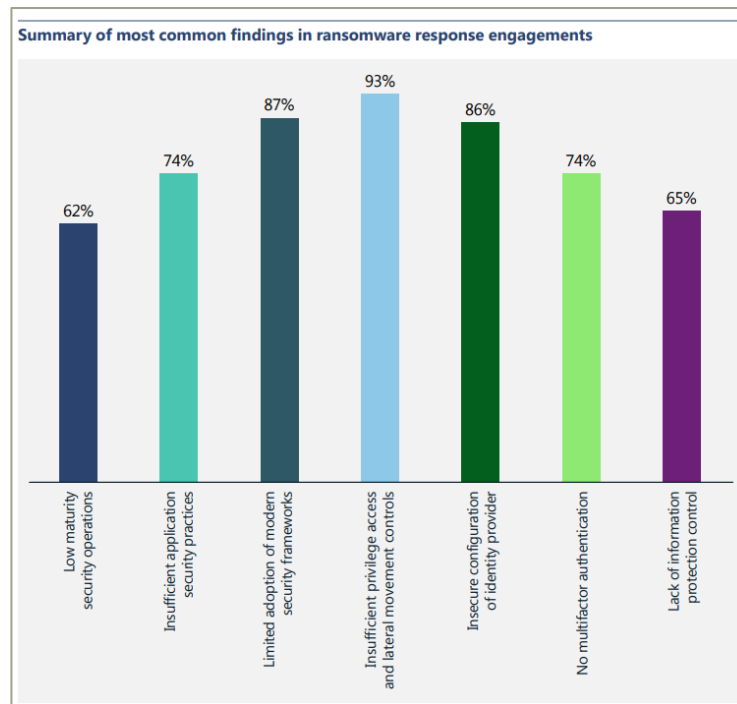
Et ransomware angreb:

- kan være lammende for al aktivitet i virksomheden i en længere periode;
- er typisk forbundet med store omkostninger og tab (tabt arbejde, undersøgelser, genetablering, oprydning, evt. betaling af løsesum mv.);
- går som regel også ud over virksomhedens kunder og samarbejdspartnere, der ikke kan serviceres; og
- medfører kompromittering af fortrolige oplysninger.

2) Økonomisk bedrageri er avancerede svindelangreb, hvor de kriminelle søger at narre virksomheden til at overføre penge til svindlerne. Her udnyttes f.eks. menneskelige fejl hos den enkelte medarbejder og svage processer ofte kombineret med hackerangreb mod virksomhedens e-mail systemer og leverandører med social engineering,

Økonomisk bedrageri kan omfatte store pengebeløb, da de kriminelle går målrettet efter de mest lukrative overførsler. Sammenlignet med ransomware angreb er konsekvenserne ved økonomisk bedrageri som regel mere begrænsede.

En af de hyppigste årsager til ransomwareangreb er "insufficient privilege access" og "lateral movement controls" – dækker kort fortalt over mangelfuld styring af bruger- og adgangsrettigheder



Kilde: IBM, Cost of a Data Breach Report 2022

VÆRKTØJSKASSEN

Tema 1: Risikovurdering – værdier og trusler

Risikovurderingen bør tage udgangspunkt i, hvad der er vigtigst for virksomhedens forretning: Hvad er de mest beskyttelsesværdige aktiver.

Når man – på tværs af de forskellige forretningsområder – har afdækket hvilke processer, systemer og/eller personer, hvis fravær ville udgøre en risiko for virksomhedens LtO (Licence to Operate), kan man lave en gennemgang af, hvordan de forretningskritiske aktiver kan påvirkes (trusselsvurdering).

I trusselsvurderingen bør man kigge på, hvilke aktører, herunder deres metoder og motiver, der kan påvirke forretningskritiske systemer. Man skal forholde sig til, om det overhovedet er muligt, og - hvis ikke - om der er andre sårbarheder, som kan udnyttes. I denne proces bør man gennemtænke, om og hvordan trusler, sårbarheder og virksomhedens egen evne – eller modenhed – er tilstrækkelig til at skærme virksomheden mod de relevante aktører (f.eks. cyberkriminelle).

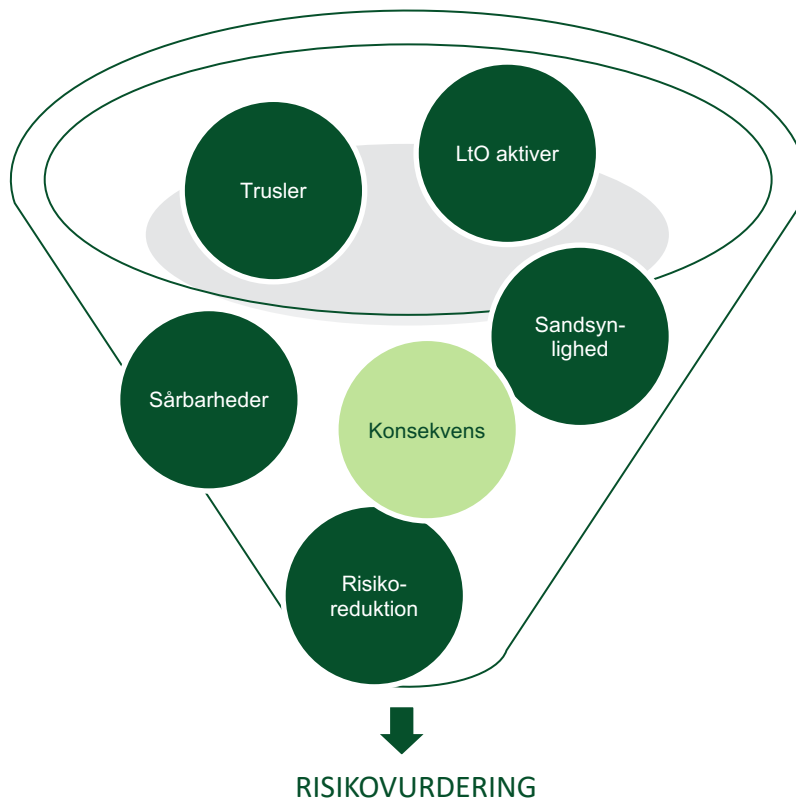
Når man har et velbeskrevet trusselsbillede, vurderes sandsynlighederne for, at det sker, og de konkrete konsekvenser, såfremt det sker. Indenfor risikovurderinger taler man om "likelihood" og "impact", altså sandsynlighed og konsekvens.

Den samlede risikovurdering danner udgangspunkt for, at virksomhedens ledelse – og dermed bestyrelsen – kan træffe beslutning om, hvilke tiltag, der skal prioriteres og investeres i, for at imødegå de identificerede risici. Overvejelserne i denne forbindelse er bl.a., hvordan man forebygger, hvordan man opbygger et effektivt beredskab, og hvordan virksomheden får mest sikkerhed i forhold til de behov, den har, og den risikoprofil, ledelsen ønsker.

Det er vigtigt, at risikovurderingen opdateres løbende i takt med ændringer, herunder i trusselsbilledet og virksomhedens teknologianvendelse.

Til at kontrollere, om bestyrelsen modtager tilstrækkelig information, kan listen på side 37 være til inspiration.

Risikovurderingen kan forstås som en tragt, hvor flere elementer indgår



1. Hvad er de vigtige (LtO) aktiver? (dvs. hvad vil vi helst beskytte, hvad er vigtigt for vores forretning, hvad er kronjuvelerne, hvad er det mest beskyttelsesværdige?)

- Hvad er vores LtO aktiver, herunder
- Hvad er det for aktiviteter, processer og data vi har?
- Hvad vil vi helst beskytte - hvad er vigtigt for vores forretning? Note: Det kan være materielle aktiver (f.eks. systemer), immaterielle aktiver (f.eks. data og IP) og renommé.
- Hvilke LtO aktiver er vigtige ifht. vores strategi, mål og forretningsmodel?
- Hvad har/kræver de af digital understøttelse?
- Hvor befinder det sig? (insourcet / outsourcet / Danmark / udlandet)?
- Hvilke leverandører leverer det / er det hos?

2. Hvad truer de vigtige (LtO) aktiver? (trusselvurdering)

- Hvem er de sandsynlige angribere?
- Hvad er deres mål / motiv (f.eks. stjæle penge, IP, informationer, digital identitet)?
- Hvilke metoder bruger de til at nå det mål (f.eks. phishing, social engineering, DDoS, malware mv.)?

3. Hvorfor skulle det kunne ske? (sårbarheder)

- Hvor er virksomheden mest udsat for sikkerhedsbrud? (Sårbarheder kan være tekniske (dårlige passwords, mangelfuld softwareopdatering mv.), i processer der mangler eller ikke følges (f.eks. fejl i konfigurerings af firewalls), ved manglende awareness hos medarbejdere, i forsyningskæden og lign.).

- Har virksomheden implementeret basal cyberhygiejne (se Appendiks 8 for uddybning heraf)
- Tager risikovurderingen højde for nye kendte sårbarheder, herunder i lyset af udviklingen i angrebsmønstre?

4. Hvad er sandsynligheden for, at det sker?

- Hvor sandsynlige er disse trusler overfor virksomhedens sårbarheder? Note: afhænger af bl.a. sektor, branche, eksponering for omverdenen, antal digitale interfaces, teknologianvendelse, digitaliseringsgrad, geopolitisk situation (se Appendiks 11), hvem angriberne er m.v.;
- Husk, at det er bestyrelsens opgave at rammesætte, hvordan sandsynlighed skal fastsættes.

5. Hvad er konsekvensen af, at det sker?

- Går det ud over fortrolighed, integritet, og/eller tilgængelighed af systemer og data?
- Hvad er kausalitetspåvirkningen af en given hændelse?
- Hvad er den sandsynlige økonomiske konsekvens? (*cyber risk quantification*)

6. Hvad er gjort for at reducere risikoen?

- Tekniske, operationelle og organisatoriske foranstaltninger?
- Forebyggende foranstaltninger?
- Krisberedskab?
- Kontroller?
- Organisering og mennesker?
- Mennesker?
- Processer?

Tema 2: Risikoappetit

– risikoafvejning og risikovillighed

Som led i strategien for sikring af cybersikkerhed bør bestyrelsen så ofte som relevant og mindst én gang om året fastlægge virksomhedens cybersikkerhedsstrategi, herunder risikoappetit på cybersikkerhedsområdet forstået som den risiko, bestyrelsen er villig til at acceptere for at opnå virksomhedens strategiske målsætninger.

Risikoappetitten er generelt et vigtigt redskab til at koble de strategiske målsætninger sammen med den operationelle drift. Det er bestyrelsens opgave at forholde sig til virksomhedens generelle risikoappetit for alle forretningsområder - og således også risikoappetit i forhold til virksomhedens eksponering overfor cyberrisici.

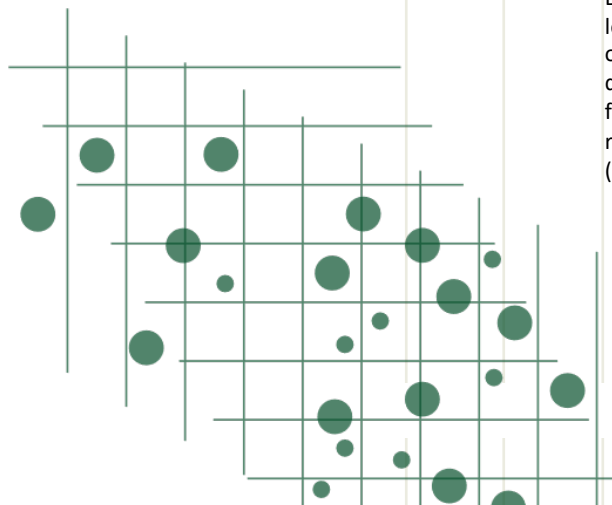
Risikoappetit bør fastsættes bl.a. ud fra virksomhedens forretningsmål, risikobillede og omkostninger ved at investere i et højere sikkerhedsniveau.

Cyberrisici er komplekse og uforudsigelige i deres natur og udvikling, og det er i de langt de fleste tilfælde urealistisk helt at eliminere dem.

Risikoappetit i forhold til cybersikkerhed er et abstrakt begreb, som dog kan tilføre stor værdi og være af afgørende betydning, såfremt det konkretiseres og operationaliseres med både værdiskabelse og sikring af aktiver og aktiviteter for øje.

Det er nærliggende at konkludere, at der ikke er nogen appetit på cybersikkerhedsrisici set i lyset af, at der alene er negative konsekvenser af cybersikkerhedshændelser. Derfor anvendes i denne vejledning også udtrykket risiko "accept".

Bestyrelsen skal via fastsættelse af risikoappetitten (/accepten) og formulering af tolerancen overfor cyber risici hjælpe ledelse og medarbejdere til at kunne koble de strategiske målsætninger sammen med den operationelle drift.



Det vil normalt være mest nyttigt at formulere risikoappetitten i form af konkrete generelt genkendelige forretningsmæssige mål. Det kan eksempelvis være:

- Vi må ikke være uden adgang til ordresystemet i mere end X timer;
- Det er kun autoriserede medarbejdere, der må kunne få adgang til vores forretningskritiske database med produkt specifikationer;
- Vi skal kunne genskabe alle driftskritiske systemer på baggrund af vores backup på højst X timer; og
- Vores outsourcingpartnere og underleverandører skal som minimum overholde X.

Det er derefter den operationelle ledelse og de relevante medarbejders opgave at identificere og implementere de forholdsregler, der er nødvendige for, at virksomhedens samlede cyber risici er indenfor dens risikoappetit (risikoaccept).

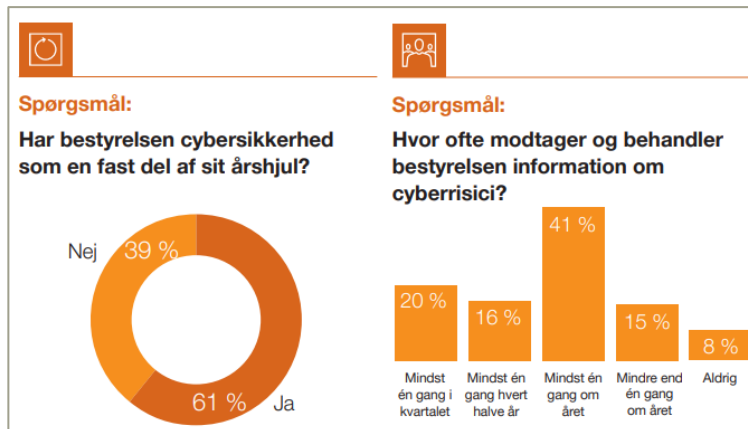
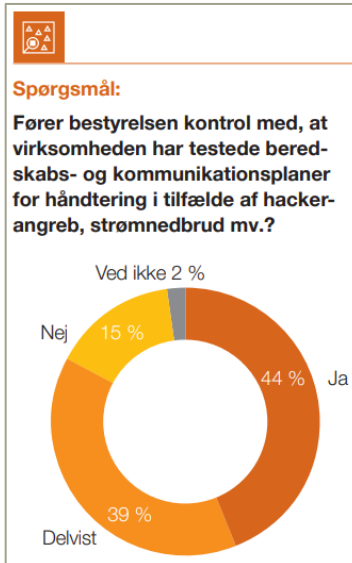
Til at fastsætte risikoappetitten og føre tilsyn med virksomhedens eksponering kan bestyrelsen bruge listen på side 41 og rapporteringstemplaten i Appendiks 4 til inspiration.

Rapporteringstemplaten i Appendiks 4 kan bl.a. bruges til at efterprøve, om bestyrelsen får den (relevante) information til at fastsætte risikoappetitten, herunder:

- Relevante LtO aktiver;
- Tiltag til at reducere risiko (forebyggende og beredskab);
- Konsekvenser i forhold til fortrolighed, integritet og tilgængelighed (C-I-A);
- Økonomiske konsekvenser;
- Risikoejerens vurdering;
- Kontrolfunktionens vurdering;
- Direktionens (samlede) vurdering; og
- Anbefalinger til forbedringer herunder investeringsbehov.

Undersøgelser indikerer, at danske bestyrelser ikke gør nok i dag

Kilde: PwC Cybercrime Survey 2022



Risikotilgang

- Hvad er virksomhedens overordnede strategi og forretningsmål? Særligt indenfor digitalisering, teknologianvendelse, time-to-market, mål i forhold til marked og kunder, leverandørpræferencer, strategiske samarbejder, produktionsteknologi og andre konkurrenceforbedrende elementer.
- Hvordan er virksomhedens strategi sammenholdt med og afspejlet i virksomhedens IT-infrastruktur og sikkerhedsforanstaltningerne omkring denne?
- Hvad er virksomhedens holdning til, om man skal prioritere indsats og tiltag i forhold til at forebygge at hændelser kan opstå og/eller skal man bruge ressourcerne på at sikre at virksomheden har et stærkt beredskab, hvis/når man rammes?
- Hvad er virksomhedens holdning til virksomhedens specifikke risici – skal man stoppe, reducere, outsource eller acceptere risikoen?
- Er cybersikkerhed en fast del af virksomhedens kvalitetssikringsprocesser, herunder i relation til udvikling, indkøb, salg og outsourcing?

Risikoforståelse

- Er der mellem forretningen og risiko-/kontrollfunktionerne en fælles forståelse for cybersikkerhed og prioriteringer (f.eks. hastighed i forhold til sikkerhed)?

- Er det relevant at lave en økonomisk kvantificering af cyberrisiko eksponeringen?
- Er der klarhed over, hvem der er ejer af de enkelte cyber risici?
- Hvordan laves der en afvejning mellem cyber risici og andre forretningskritiske risikotyper fx råvarekvalitet, renterisiko, osv.?

Risikofafvejning

- Hvad er virksomhedens afvejning i forhold til fortrolighed, integritet hhv. tilgængelighed, dvs. skal virksomheden vægte fokus på 1) at sikre fortrolighed omkring data; 2) at man kan stole på data og/eller 3) at data er tilgængelige?
- Kunne virksomheden med fordel indgå samarbejdsaftaler omkring cybersikkerhed?
- Hvordan er virksomheden forsikret i forhold til cyberrisici – og hvad er kravene på forsikringen?
- Hvor ligger virksomhedens sikkerhedsniveau- og budget sammenlignet med andre virksomheder?
- Hvad er de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet?
- På baggrund af en samlet vurdering, hvad er virksomhedens tolerance for at påtage sig cyberrisici, herunder toleranceværdien for de enkelte risici, f.eks. risikotype, produkttype, kunder, strategi, målsætninger mv.?

Tema 3: Politikker, processer og beredskab

- delegering og operationalisering

Alle virksomheder er under konstant forsøg på cyberangreb. Det er vigtigt, at virksomheden har passende sikkerhedsforanstaltninger på plads, og har det rette beredskab, hvis den alligevel bliver ramt. Bestyrelsen skal spørge ind til de etablerede sikkerhedsforanstaltninger, og om der foreligger politikker og velafprøvede planer og processer til at forebygge og håndtere cybersikkerhedshændelser.

Virksomhedens sikkerhedspolitikker og beredskabsplaner skal sikre, at virksomheden kan identificere, beskytte, opdage, håndtere og genoprette i tilfælde af angreb. Det er vigtigt at sikre, at disse funktioner er implementeret i et tilstrækkeligt og passende omfang, der matcher virksomhedens risikoappetit.

Sikkerhedshændelser kan medføre store omkostninger til udredning, genopretning, driftstab, kompensation til kunder mv. En hurtig og effektiv håndtering vil ofte kunne begrænse omkostningerne væsentligt. Det er derfor vigtigt at have dokumenterede og afprøvede beredskabsplaner samt være sikker på, at man hurtigt og effektivt kan genetablere driften efter et angreb.

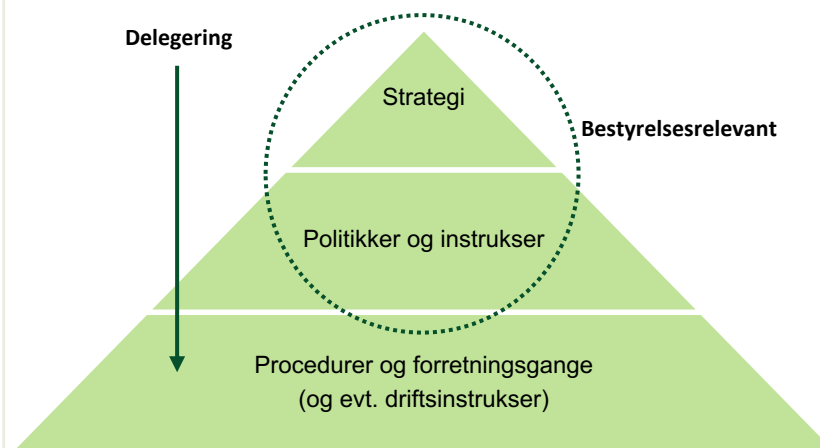
Den billigste sikkerhedshændelse er den, som ikke sker. For at sikre et passende og dækkende niveau anbefales, at virksomheden følger en anerkendt standard eller et rammeværk for styring og etablering af informationssikkerhed.

Et sådan rammeværk kan f.eks. være 1) (principperne i) ISO27001, der er en international standard for styring af informationssikkerhed, som følges af større organisationer og statslige institutioner, og hvis krav generelt er udtryk for best practice, og/eller 2) sikkerhedskontrollerne i CIS18, der indeholder en række retningslinjer baseret på best practice fra Center for Internet Security.

Virksomheden kan også overveje at blive certificeret indenfor sikkerhed f.eks. via en ISO27001 eller D-mærke certificering, således at virksomheden kan dokumentere, at den har et passende sikkerhedsniveau.

Til at føre kontrol med om virksomheden har etableret et passende sikkerhedsniveau og beredskab, eventuelt baseret på anerkendte standarder, kan bestyrelsen bruge listen til højre og de næste sider til inspiration.

Strategien rammesætter politikker og instrukser (taktisk), der rammesætter procedurer og forretningsgange (operationelt).



Centrale overvejelser i et bestyrelseslokale

Bestyrelsen skal føre tilsyn med, hvordan virksomheden har operationaliseret risikostyring af cybersikkerhed.

Dette kan bestyrelsen gøre indenfor 5 funktioner, der udtrykker virksomhedens cyberforsvar: Identificer, beskyt, opdag, håndter og genopret (Identify, Protect, Detect, Respond, Recover).

Bestyrelsen skal overordnet forholde sig til:

- om der er de rigtige **politikker, processer, forretningsgange og instrukser** i organisationen, der understøtter risikovurderingen,

- om virksomheden har taget de nødvendige **forebyggende foranstaltninger** til at undgå nedbrud, tab af data mv., og
- om virksomheden har et **testet beredskab** til at håndtere og komme tilbage i tilfælde af en krisesituation.

Se uddybende om delegering og operationalisering på side 44-45.

DELEGERING

- Har ledelsen taget det, der er besluttet i Tema 1 (Risikovurdering) og Tema 2 (Risikoappetit), og sikret, at det lever i organisationen?
- Er cybersikkerhedsrisici forankret i instrukser og forretningsgange og politikker?
- Er der sket de rigtige delegeringer?
- Er der mandater, bestyrelsen skal forholde sig til?
- Hvad er instruksen fra bestyrelse til direktion og fra direktion til organisation?
- Hvordan er politikker, instrukser og forretningsgange forankret?
- Hvem har mandater og beføjelser?

OPERATIONALISERING

Identificere

- Metode/værktøjer til identificering af sårbarheder og trusler (f.eks. Mitra)?
- Hvordan afgør man, hvilke trusler man anser for sandsynlige og hvordan vurderer man sandsynlighed?
- Hvis X aktiv er vigtigst, er der så overblik over, hvilke systemer der understøtter det? Er der single point of failure?
- Er der overblik over hvilke systemer og processer, der hænger sammen, og hvordan det er påvirket af beslutninger, der er truffet på strategisk niveau?

- Har organisationen en CMDB (database) til at sikre overblik og transparens over infrastrukturen? (dvs. hvad er hvor, og hvad hænger sammen med hvad?)
- Gælder det overblik både egne og indkøbte/outsourcete systemer?
- Understøttes selskabets strategi af den infrastruktur, man har?
- Hvilke sikkerheds- og sårbarhedsscanninger udføres?

Beskytte

- Har organisationen en politik for risikoanalyse?
- Har organisationen en informationssikkerhedspolitik?
- Hvad er de vigtigste foranstaltninger taget til at reducere risici?
- Hvordan kører virksomheden awareness og træning?
- Har virksomheden implementeret basal cyber hygiejne, som fx zero-trust, patching, device konfigurering, netværkssegmentering og IAM? (se også Appendiks 8)
- Har organisationen politikker for brug af kryptografi og kryptering?
- Har organisationen håndteret og reduceret cybersikkerhedsrisici i forbindelse med anskaffelse, udvikling og vedligehold?
- Har organisationen politikker og processer til at vurdere effektiviteten af foranstaltningerne (f.eks. efterprøvet gennem tests)?

Opdage

- Har virksomheden overvågning til at opdage, hvis der sker noget?
- Har virksomheden logning, og hvis ja, hvad logger den på (f.eks. hvilke systemer er med som del af logning og hvor længe)?
- Har virksomheden testet evnen til at opdage cyberangreb?

Håndtere

- Har organisationen en beredskabsplan for hændeshåndtering (incident handling)?
- Har organisationen en beredskabsplan for driftskontinuitet (business continuity), herunder back-up og disaster recovery?
- Har organisationen en beredskabsplan for krisestyring, herunder kommunikationsplan?
- Fastlægger planerne, at der skal føres en hændelseslog til dokumentation af forløb og beslutningsgrundlag?
- Har organisationen en sikker kommunikationslinje til en krisesituation (hvor outlook f.eks. er utilgængelig)?
- Bliver planerne testet, og hvad er resultatet af seneste test?
- Har virksomheden aftaler med eksterne?
- Har bestyrelse/direktion gjort sig overvejelser om fx løsesumbetaling og det dilemma, ledelsen kan stå i?
- Kan virksomheden overholde evt. krav (lovkrav eller kontraktkrav) til rapportering og meddelelse til myndigheder og kunder?

Genoprette

- Er der backup, og hvis ja, er den 1) testet, 2) hvor tit, 3) hvad er retention time, 4) på hvilke systemer, og er backup "full" eller "incremental"?
- Er backup beskyttet (f.eks. en offline eller ekstern backup service)?
- Understøtter backup politikken den fastsatte risikoappetit?
- Hvad er prioritering og restore, f.eks. 1) kan de kritiske ting genskabes først, 2) er der runbooks til det, og 3) hvor lang tid vil det ville tage i et worst case scenarie?
- Kan der laves recovery uden at ødelægge bevispor, dvs. kan driftssystemer genskabes uden at slette bevispor?

Kontrakter og tredjeparter:

- Har organisationen håndteret og mitigeret cybersikkerhedsrisici i sin forsyningskæde, herunder i relation til direkte leverandører og kvaliteten i deres produkter, services, sikkerhedsforanstaltninger og udviklingsmetoder?
- I det omfang ydelser er indkøbt hos eller outsourcet til tredjepart, hvilke krav stilles til dem, og hvilke kontroller er der?

Forsikring:

- Er der tegnet en cyberforsikring, og hvis ja, dækker den så de større / mest sandsynlige tab, og har forsikringssselskabet en "retained service" – enten forebyggende eller i en krise?

Tema 4: Rapportering

– kontrol og tilsyn

Bestyrelsen skal modtage forståelig og målbar rapportering om cybertrusler, -risici og sikkerhedshændelser for at kunne føre kontrol med virksomhedens cybersikkerhed og integrere arbejdet med cybersikkerhed som en naturlig del af sin tilsyns- og kontrolopgave.

Tilstrækkelig og relevant rapportering er altafgørende, da bestyrelsen ikke kan udfylde sin tilsynsopgave uden at forstå de potentielle trusler og risici.

Bestyrelsen bør tænke rapporteringen ind i sit årshjul. Et eksempel på hvordan dette kan gøres, er vist i Appendiks 6.

Den løbende rapportering skal tilpasses de karakteristika virksomheden har. Ét aspekt gælder dog uanset sammenhængen i øvrigt: Rapporteringen skal være retvisende, fyldestgørende og muliggøre konkrete tiltag.

Det betyder, at rapporteringen ikke alene skal identificere problemområder. Den skal også anviser, analysere og anbefale forholdsregler til ledelse og bestyrelse. Set i lyset af de konsekvenser, der kan følge af

utilstrækkelig implementering af forholdsregler mod angreb fra aktører, der permanent udsøger sig de "svageste dyr i flokken", er det afgørende, at rapporteringen er klar og forståelig for modtagerne.

Det er kun, hvis modtagerne kan agere relevant på rapporteringen, at den er værdiskabende.

Det er bestyrelsens ansvar at organisationen tilvejebringer tilstrækkelig og tilgængelig information i et omfang, der er passende for håndtering af den strategiske risiko for eksponering mod cyber hændelser.

Der findes ikke én standard for rapportering på cybersikkerhedsområdet, og rapporteringen kan nemt blive subjektiv. Et eksempel på en generisk rapporteringstemplate fremgår i Appendiks 4.

Til at vurdere, om bestyrelsen modtager tilstrækkelig information, kan listen til højre samt Appendiks 4 være til inspiration.

Rapportering

Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed fra direktionen, herunder:

- Aktuell risikostatus (sammenfatning af risikostatus);
- Aktuelt trusselsbillede samt udvikling/trends siden sidst;
- Observationer og kommentarer fra revisorer/rådgivere;
- Lovgivning og myndighedskrav (og aktuelle/kommende ændringer hertil);
- Resultater fra test af beredskabsplaner og kritiske systemer;
- Eventuelle fravigelser fra de af bestyrelsen fastsatte risikotolerancer;
- Interne sikkerhedshændelser, herunder hændelser rapporteret til myndighederne;
- Eksterne sikkerhedshændelser – f.eks. leverandører og outsourcing partnere;
- Projekt status (status på implementering af sikkerhedstiltag);
- System status, herunder: Væsentligste generelle (tekniske) risikoområder, risiko og kontrol oversigt (tekniske) og heat map status med top X (tekniske) risici;
- Status personale / medarbejdere og organisering;
- Status på sikkerhedskategorier generelt (NIST-rammens 5 funktioner);
- Krisehåndtering - ansvar og bemyndigelse;
- Begrænsninger og udeladelser; og
- Anbefalinger til forbedringer og investeringer forbundet hermed.

Årshjul

- Har bestyrelsen implementeret cybersikkerhed som en fast del af et årshjul, der sikrer opfølgning, kontrol og revision på sikkerhed som en fast del af bestyrelsens arbejde, og sikrer rette rapportering i rette tid?
- Får virksomheden udarbejdet revisorerklæringer i forhold til it sikkerhed, f.eks. ISAE3402 eller ISAE3000 erklæringer?
- Stiller virksomheden krav om, at dens kunder og/eller leverandører får udarbejdet sådanne erklæringer?
- Er der opmærksomhedspunkter fra disse rapporter/erklæringer, og hvis ja, en plan for udbedring?

Et eksempel på et årshjul med cyberaktiviteter er vist i Appendiks 6.

Tilsynsmyndigheder

- Er virksomheden i en branche eller sektor, der kræver løbende dialog og forventningsafstemning med nationale myndigheder (f.eks. virksomheder der leverer kritisk infrastruktur)?
- Har virksomheden en proces for opbevaring og gennemgang af data til brug for eventuelle tilsynsbesøg?

En inspirationsliste til rapportering er vist i Appendiks 4.

Tema 5: Kultur

– mennesker og træning

Strategier og planer er én ting, men hvis de ikke følges af ledelse og medarbejdere, er man lige vidt. Medarbejderne er én af de vigtigste kilder til en god sikkerhedskultur og dermed til et højt sikkerhedsniveau. Inden længe bliver det desuden et lovkrav for ledelser i en lang række virksomheder, at de regelmæssigt skal følge cyberspecifikke kurser.

Der er et behov for træning og awareness programmer for medarbejderne i danske virksomheder og deres ledelser, både i forhold til at dele viden, øge viden og ændre adfærd. Der skal ikke mere end én uopmærksom medarbejder, som trykker på et forkert link, for at der opstår en sikkerhedshændelse.

Den eksplosive vækst i phishing-mails, malware og ransomware, der er rettet mod ledelse og medarbejdere, stiller ikke bare store krav til virksomhedens Sikkerhedsforanstaltninger, men også til den digitale adfærd.

Det kan synes banalt, men for hackere er det meget nemmere at komme ind via (dårlige) IT-vaner, end at skulle hacke sig ind via den "digitale hoveddør".

Insiderproblematikken er reel. Det

estimeres, at 25-35% af alle hændelser kan skyldes medarbejdere – både ubevidst (fejl, offer for social engineering mv.) og bevidst (utilfredse medarbejdere, opportunist, svindlere, uheldige samarbejder mv.).

Der er behov for, at bestyrelsen går forrest i at støtte op om en kultur i virksomheden, hvor sikkerhed kan diskuteres åbent, hvor medarbejderne kan rapportere fejltagelser og brud på sikkerheden, og hvor man lærer af sine fejl. Arbejdet med awareness kan foregå på forskellige niveauer, f.eks. i form af at dele viden internt, øge kendskab/viden og ændre adfærd.

Bestyrelse og direktion behøver ikke kende cybersikkerhed i detaljer, men de bør regelmæssigt følge specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og styringspraksisser samt deres indvirkning på virksomhedens drift. Dette bliver også et krav i den kommende NIS2-lovgivning, der vil gælde for en lang række virksomheder.

Som forberedelse til at sparre med og udfordre direktionen indenfor kultur og digital adfærd, kan listen til højre til være til inspiration.

Uddannelse, træning og awareness

- Er der et træningsprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- Er der et uddannelsesprogram for, at medlemmer af bestyrelse og direktion samt medarbejdere løbende modtager uddannelse i cyberrisici, f.eks. gennem deltagelse i kurser, konferencer og seminarer med fokus på cyberrisiko, cyberkriminalitet og trends og udvikling indenfor virksomhedens branche?

Nøglepersoner

- Baggrundstjekker virksomheden nøglepersoner ved ansættelse?
- Modtager nøglepersoner målrettet træning og uddannelse indenfor cybersikkerhed?
- Er der et specifikt cybersikkerheds awareness program for nøglepersoner eller personer med kritiske funktioner, f.eks. en rejsepolitik i relation til bestemte lande eller en politik for nøglepersoners brug af sociale medier, BYOD (bring your own device)?

Kultur og videndeling

- Foregår der et samarbejde på tværs af organisationen, hvor der deles viden?
- Opfordrer virksomheden sine tekniske specialister til at udveksle viden og erfaringer med medarbejdere fra lignende organisationer for at drage fordel af the 'wisdom of the crowd'?

indenfor forebyggelse?

- Benytter den IT ansvarlige sig af netværk og eksterne samarbejder, der kan styrke viden og kompetencer?
- Understøtter ledelsen en positiv sikkerhedskultur, f.eks. ved løbende at informere om cybersikkerhedsstrategien, typen af trusler, og hvordan virksomheden er beskyttet?
- Har virksomheden medarbejdere, den sjældent ser, og ikke har fysisk kontrol over, og som måske har mindre loyalitet?

Tema 6: Governance

– kompetencer og organisering

Ledelsesmedlemmer forventes i dag at være i stand til at forholde sig til væsentlige forhold i relation til virksomhedens cybersikkerhed, herunder om de rette kompetencer og den rette organisering er til stede, og at kunne medvirke til at stille spørgsmål til direktionen og forholde sig til svarene.

Cybersikkerhed er for vigtigt og komplekst til, at forståelsen ligger på få hænder, og IT er for kritisk og risikoen for stor til, at bestyrelsen ikke holder sig tæt på området.

Det strategiske og operationelle smelter sammen ved en kritisk sikkerhedshændelse. Bestyrelsen må derfor være tættere på sikkerhedsområdet end på mange andre operationelle forhold.

Bestyrelsen er i sidste ende ansvarlig for at sikre, at de rette kompetencer er til stede i bestyrelsen og virksomheden – uanset uddelegering og outsourcing.

Hvis de rette kompetencer ikke er til stede direkte i bestyrelsen, bør den

sikre sig, at både bestyrelse, direktion og organisation faktisk har eller har adgang til de nødvendige kompetencer og ressourcer på cybersikkerhedsområdet – om nødvendigt gennem aftaler med eksterne samarbejdspartnere og specialister.

Hertil bør virksomheden overveje, om ansvaret for og kontrollen med cybersikkerhed er placeret hos én og samme funktion i forretningen, eller om virksomhedens risikostyring af cybersikkerhed med fordel kan styrkes gennem etablering af uafhængige risikostyringskontroller (lines of defence).

Til at vurdere om de rette kompetencer og rolledeling er på plads, kan bestyrelsen bruge listen til højre til inspiration

Bestyrelsen

- Har bestyrelsen kompetencer og erfaring med risikostyring af it- og cyberrisici, f.eks. cybersikkerheds- og risikovurderingsprocesser, leverandørstyring, sikkerhedskrav og lignende?
- Er der behov for at udskille noget til f.eks. et særskilt risikostyringsudvalg?
- Holder bestyrelsen sig løbende orienteret om de cybertrusler og aktører, der truer virksomheden, deres metoder og motivation?
- Deltager bestyrelsen aktivt i diskussioner om cybersikkerhed?
- Er bestyrelsen opmærksom på, at den selv kan være et oplagt mål for cyberangreb (f.eks. CEO fraud)?

Direktionen

- Har direktionen kompetencer og erfaring med risikostyring af it- og cyberrisici?
- Har virksomheden en sikkerhedsorganisation, der er fagligt forankret direkte på direktionsniveau, f.eks. CEO, CFO eller CIO?
- Rapporterer denne funktion direkte til bestyrelsen eller gennem en anden rapporteringsproces?
- Hvordan er sikkerhedsarbejdet organiseret og delegeret?

Organisationen (og lines of defense)

- Hvor i organisationen (person/funktion) ligger ansvaret for cybersikkerhed?
- Rapporterer denne sikkerhedsfunktion til de rigtige på ledelsesniveau?
- Hvem har risikostyringsansvaret?

- Hvem har overblikket over risici på tværs af organisationen? (f.eks. en "Chief Digital Risk Officer"-rolle der rapporterer direkte til bestyrelsen)
- Hvem kontrollerer hvad (lines of defense)?
- Kontrollerer risikoejeren sig selv?
- Er risikovurderingen alene forankret i forretningen, eller er der også en risiko/kontrollfunktion?
- Hvem holder styr på risikoeksponeringen fra leverandører?
- Bør andre forretningsområder involveres i arbejdet med cybersikkerhed, f.eks. ledere af afdelinger, der udvikler produkter og services?
- Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- Hvor meget af sikkerheden står virksomheden selv for, og hvor meget er lagt ud til tredjepart?

Eksterne

- Har virksomheden de rette tekniske kompetencer inhouse, eller er der behov for ekstern hjælp?
- Har bestyrelsen brug for hjælp til tilsynsopgaven fra rådgivere eller en komité?
- Kan bestyrelsen have gavn af at få eksterne eksperter til at præsentere best practices for at give cybersikkerhed et ekstra perspektiv?

APPENDIKS

| APPENDIKS | Side |
|--------------|---|
| Appendiks 1 | Regulatorisk landskab 54 |
| Appendiks 2 | Sikkerhedsstandarder 59 |
| Appendiks 3 | Template til cybersikkerhedsstrategi 66 |
| Appendiks 4 | Template til bestyrelsesrapportering 69 |
| Appendiks 5 | Cyberforsikringer 90 |
| Appendiks 6 | Emner til bestyrelsens årshjul 93 |
| Appendiks 7 | Leverandørsikkerhed 96 |
| Appendiks 8 | Basal cyberhygiejne 103 |
| Appendiks 9 | Personlig cybersikkerhed for bestyrelsesmedlemmer 108 |
| Appendiks 10 | Akut checkliste ved cyberhændelser 111 |
| Appendiks 11 | Geopolitiske overvejelser 114 |
| Appendiks 12 | Ordliste 117 |



BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance