Cybersikkerhed for bestyrelse og direktion

Vejledning og anbefalinger til styrkelse af strategiske cyberkompetencer. December 2022 (V4.0)

BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance

KROMANN REUMERT

Dubex:

INDUSTRIENS FOND

FE CENTER FOR CYBERSIKKERHED

Indhold

2

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 direktionsgange 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, medarbejdere, forretningsplatform og værdiskabelse.

Formålet med vejledningen er også at etablere en fælles referenceramme for bestyrelsesmedlemmers og direktioners forståelse af og arbejde med strategi og risiko indenfor cyberområdet, herunder give inspiration til rapportering og spørgsmål om virksomhedens sårbarheder og sikkerhed.

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 Bestyrelses-uddannelserne, 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 Cyberkompetencers 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.

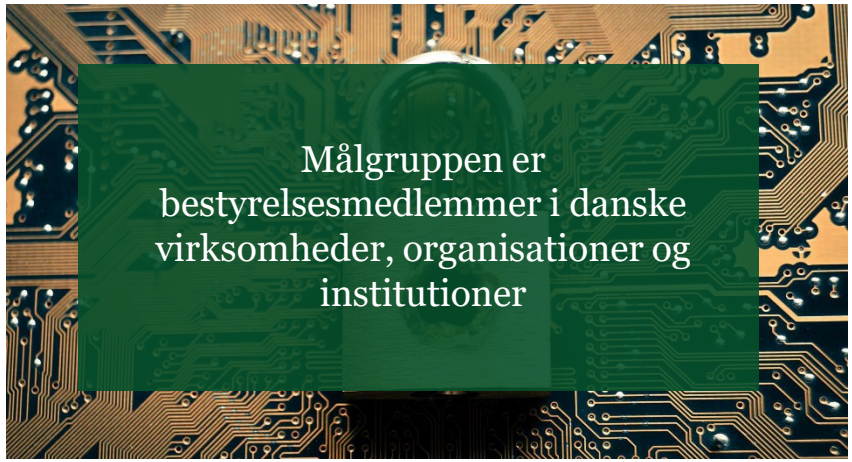
Denne vejledning blev første gang udgivet i december 2019, og er opdateret i 2020, 2021 og i 2022. Herved foreligger version 4.0, december 2022.

Komiteen for God Selskabsledelse og Komitéen for God Fondsledelse henviser til vejledningen og anbefalingerne.

København, december 2022

Bestyrelsesforeningens Center for Cyberkompetencer A/S.

Marianne Philip, Tom Jacobsgaard og Kirsten Hede.



Kontakt

Bestyrelsesforeningens Center for Cyberkompetencer

Marianne Philip
Bestyrelsesformand
mp@kromannreumert.com

Tom Jacobsgaard
Direktør
tj@bestyrelsesforeningen.dk

Kirsten Hede
Projektdirektør
khe@bestyrelsesforeningen.dk

Jørgen Bardenfleth
Formand for Advisory Board
joergen@bardenfleth.dk

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 direkte digitale, har i dag digitale løsninger til understøttelse af operationelle processer og funktioner.

IT og digital understøttelse er for langt de fleste virksomheder afgørende for, at de kan udføre deres kerneopgaver og være konkurrencedygtige.

Efterhånden som virksomheder bliver mere afhængige af internettet, og på grund af det forhøjede trusselsbillede, er virksomheder blevet markant mere udsatte over for cyberangreb.

Virksomhedsledere, der har prøvet et cyberangreb, fremhæver, at det har været deres værste mareridt, og at cyberrisici måske er den største og mest fundamentale risiko for en virksomhed i dag.

Cyberangreb er blandt de største forretningsrisici, virksomheder står overfor. Det særlige ved cyberrisici er, at denne trussel banker på virksomhedernes digitale dør hvert eneste minut - og på tværs af landegrænser. Det er dén risiko, man skal forstå og forholde sig til i bestyrelse og direktion.

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 tryghed 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).

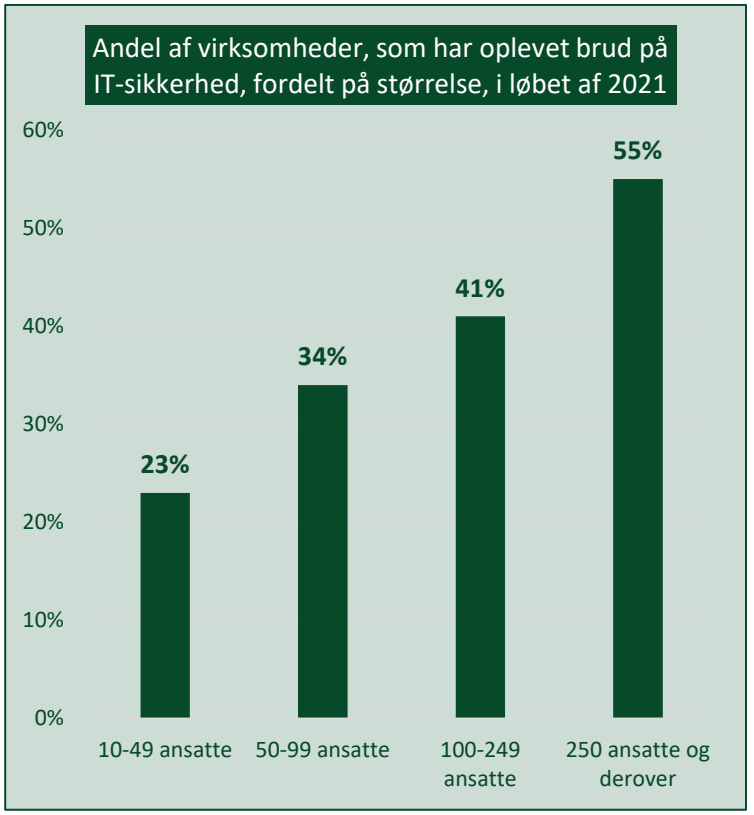
Arbejdet med en cybersikkerheds-strategi kræver basal IT-forståelse, men er IKKE en IT-opgave. Det er en ledelsesopgave på øverste niveau. Det er derfor afgørende, at bestyrelse og direktion ved, hvad der er digitalt kritisk for virksomhedens forretning, drift og overlevelse, og at der er strategier, 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 i 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 modstandsdygtighed indenfor den finansielle sektor (DORA – The Digital Operational Resilience Act) øge kravene til cybersikkerhed betydeligt.

NIS2 og DORA forventes vedtaget i løbet af Q4 2022, og vil formentlig træde i kraft i dansk ret fra medio til ultimo 2024.

De nye cybersikkerhedsregler stiller bl.a. krav til, at danske virksomheder øger modstandsdygtigheden 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 generel hovedregel bør en privat virksomhed få undersøgt, om den bliver omfattet af NIS2, hvis den opererer indenfor én af de i figuren overfor oplistede sektorer, og ikke er en "små-" eller "mikro"-virksomhed forstået som en virksomhed med færre end 50 ansatte og en årlig omsætning eller en årlig balance på under 10 mio. euro.

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

NIS2 får dermed efter alt at dømme 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 (persondatabeskyttelse). 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

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 cybersikkerheds-strategi 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, også på ledelsesniveau, 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 cybersikkerheds-strategi 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 besluttes 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.

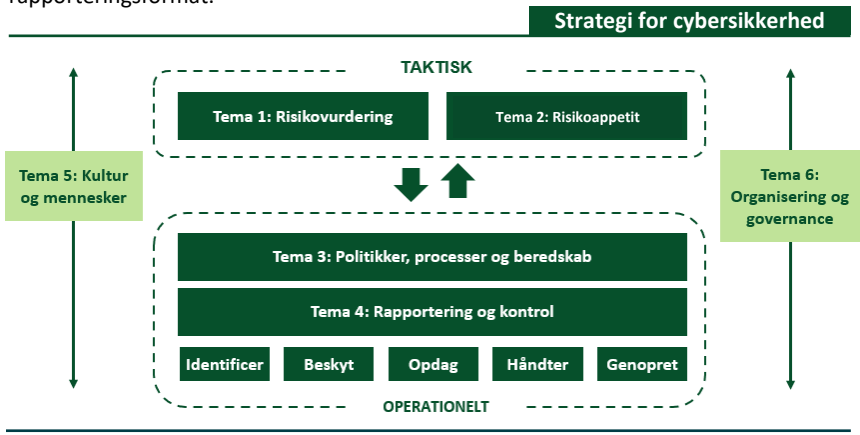
Tema 3 – Politikker, processer og beredskab: Delegering og operationalisering af strategien.

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 governance-struktur med klar organisering og afdækning af relevante kompetencer.

Målsætningen med cybersikkerheds-strategien er at rammesætte de operationelle elementer til at *identificere*, *beskytte*, *opdage*, *håndtere* og *genoprette.* Disse 5 funktioner svarer til internationalt anerkendte rammeværker, herunder NIST. Opfyldelsen af målsætningen bør løbende behandles i bestyrelses-rapporteringen.



Opbygningen af en cybersikkerhedsstrategi

Forudsætninger – og LtO aktiver
Cybersikkerhedsstrategien bør overordnet handle om at beskytte virksomhedens *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 fortrolighed, 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 forretningsmål,
- 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 - på tværs af virksomheden – således 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 cybersikkerheds-strategien 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) politikkernes 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 dét 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. Men for at kunne vurdere sårbarheder, trusler, tiltag og sikkerhedsniveau, er det 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.

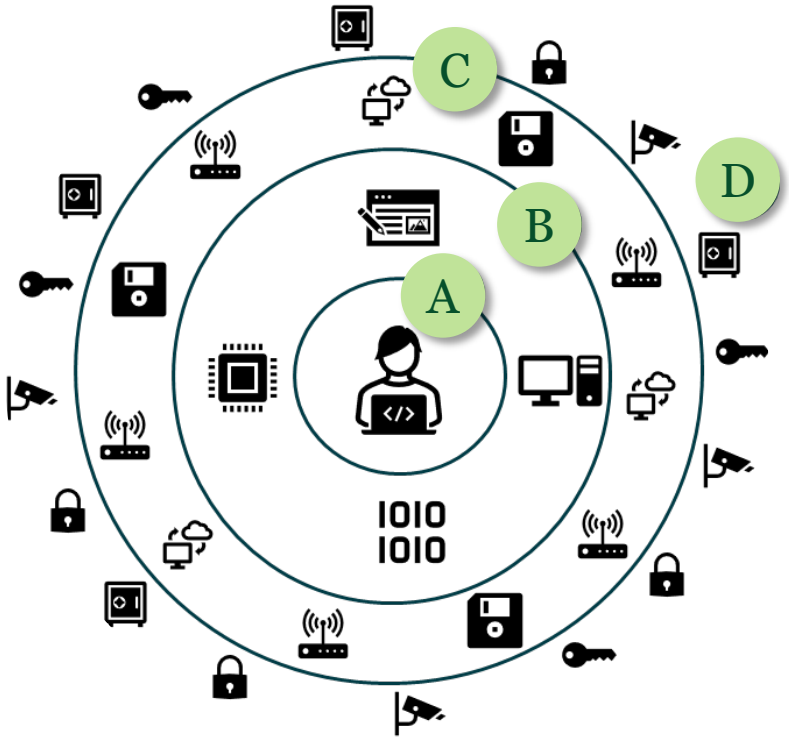
Al denne data bliver opbevaret, transporteret, beskyttet m.v. af it-udstyr, dvs. servere, data-lagringsudstyr, udstyr til backup, PC'er, tablets, mobiltelefoner, routere, trådløst kommunikations-udstyr, kabling osv. Dette kaldes også hardware.

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 og 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-premise eller outsourcet). Ansvaret 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 muligheder 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 cyber-trusselsbillede 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 i forhold til virksomhedens system--opbygninger og branche. Dvs. virksomheden må også lave sin egen individuelle vurdering af trusler.

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 at sikkerhedsforanstaltninger.

Trusler
De fleste trusler er eksterne, og afhænger af angrebsaktørernes motiver og metoder (se eksempler på trusler på side 15).

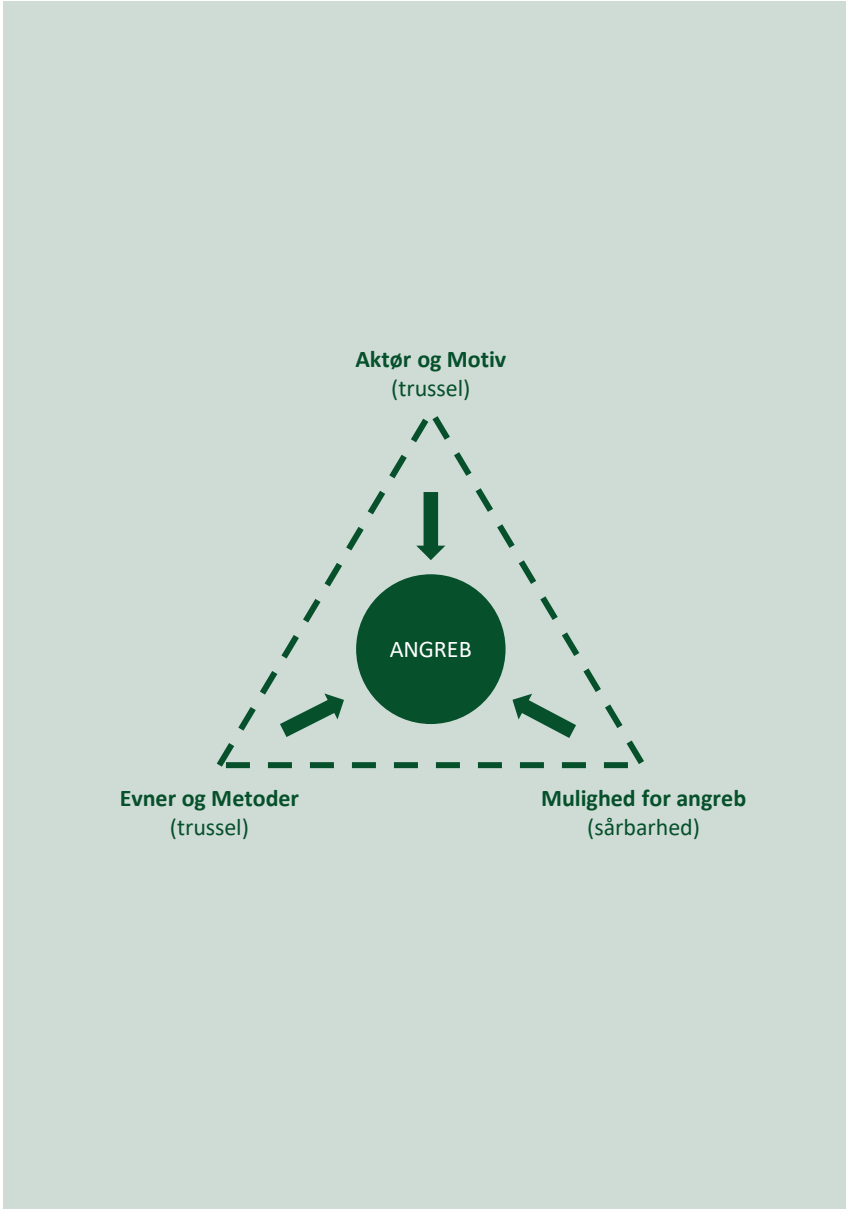
Det *eksterne* trusselsbillede består af to hovedelementer:

- 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 trussels-vurderinger, 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 på nuværende tidspunkt er:

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 ugennemskueligt 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 kapaciteter.

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 målrettet at angribe virksomheder. Men man skal 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 står bag mere end 80% af alle eksterne angreb.

De kriminelle driver en forretning, og motivet for deres angreb er simpel, 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:
Ransomware og 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.

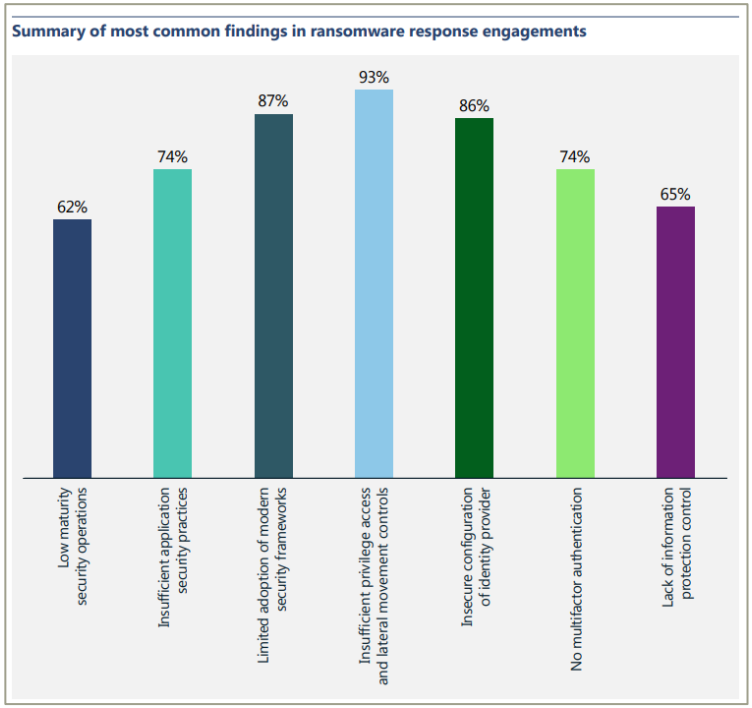
Et ransomware angreb:

- 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, ofte kombineret med hackerangreb mod virksomhedens e-mail systemer og leverandører med social engineering, søger at narre virksomheden til at overføre penge til svindlerne. Her kan f.eks. udnyttes menneskelige fejl hos den enkelte medarbejder og svage processer.

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 begrænset.

En af de hyppigste årsager til ramsomwareangreb 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

ANBEFALINGER OG TJEKLISTE

Til styrkelse af strategiske cyberkompetencer i danske bestyrelser

1. Risikovurdering
- værdier og trusler

Det anbefales, at

- bestyrelsen mindst to gange 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.

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.

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.

4. Rapportering
- kontrol og tilsyn

Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul og, 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.

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.

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

1. Risikovurdering – trusler og sårbarheder

- ❑ 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 kvalitets-sikringsprocesser (udvikling, indkøb, salg, outsourcing mv.)?
- ❑ Er der mellem forretningen og risiko-/kontrolfunktioner 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. Planer, politikker og beredskab

- ❑ 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, at medlemmer af bestyrelse, direktionen og medarbejdere 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 kontroller 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?

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).

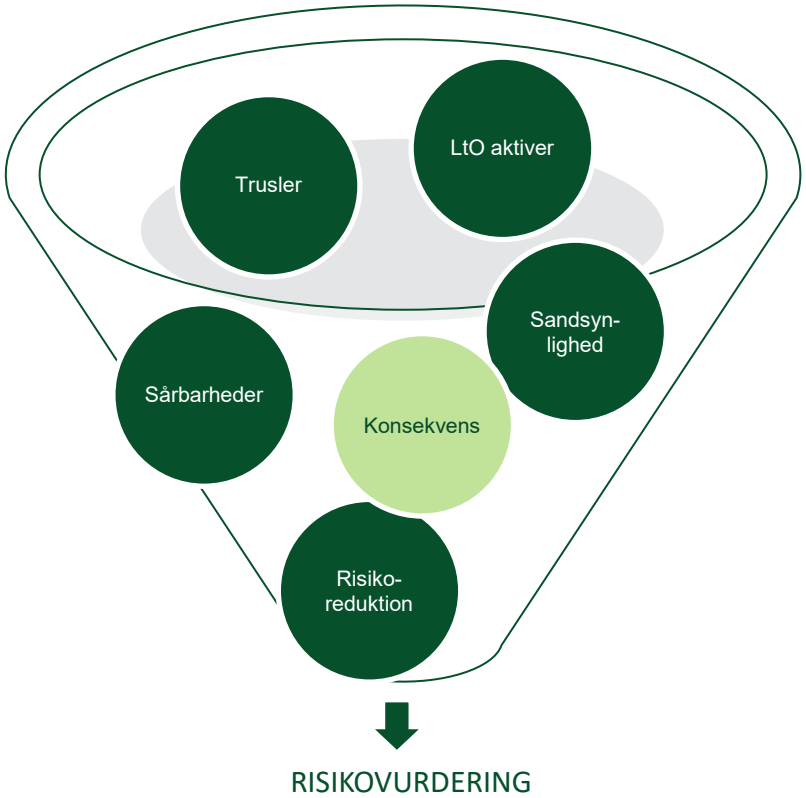
I trusselsvurderingen bør man kigge på, hvilke aktører, herunder deres metoder og motiver, der kan påvirke forretningskritiske systemer. Man skal forholde sig til, om det overhovedet er muligt, og - hvis ikke - om der er andre sårbarheder, som kan udnyttes. I denne proces bør man gennemtænke, om og hvordan 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 – er med til at 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, at bestyrelsen modtager tilstrækkelig information, kan listen på næste side være til inspiration.

Risikovurderingen kan forstås som en tragt, hvor flere elementer indgår



1. Hvad er vores 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 af LTO aktiver er vigtige ifht. vores strategi, mål og forretningsmodel?
- Hvad har/kræver de af digital understøttelse?
- Hvor befinder det sig? (insourcet / outsourcet / Danmark / udenlands)
- Hvilke leverandører leverer det / er det hos?

2. Hvad truer vores vigtige (LtO) aktiver? (trusselsvurdering)

- Hvem er de sandsynlige angribere?
- Hvad er deres mål / motiv (f.eks. stjæle penge, IP, informationer, digital identitet)?
- Hvilke metoder bruger de til at 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 (fx fejl i konfigurering 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 bl.a. sektor, branche, eksponering for omverden, antal digitale interfaces, teknologianvendelse, digitaliseringsgrad, geopolitisk situation (se Appendiks 12), hvem angriberne osv.;
- Husk, at det er bestyrelsens opgave at rammesætte, hvordan sandsynlighed skal fastsættes

5. Hvad er konsekvensen ved at det sker?

- Mister virksomheden Fortrolighed, integritet, og/eller tilgængelighed?
- Hvad er kausalitetspåvirkningen af en given hændelse?
- Hvad er den sandsynlige økonomiske konsekvens? (*cyber risk quantification*)

6. Hvad har vi gjort for at reducere risikoen?

- Tekniske, operationelle og organisatoriske foranstaltninger?
- Forebyggende foranstaltninger?
- Kriseberedskab?
- 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 og herunder risikoappetit på cyber- og informationssikkerhedsområdet forstået som den risiko, bestyrelsen er villig til at acceptere for at opnå virksomhedens strategiske målsætninger.

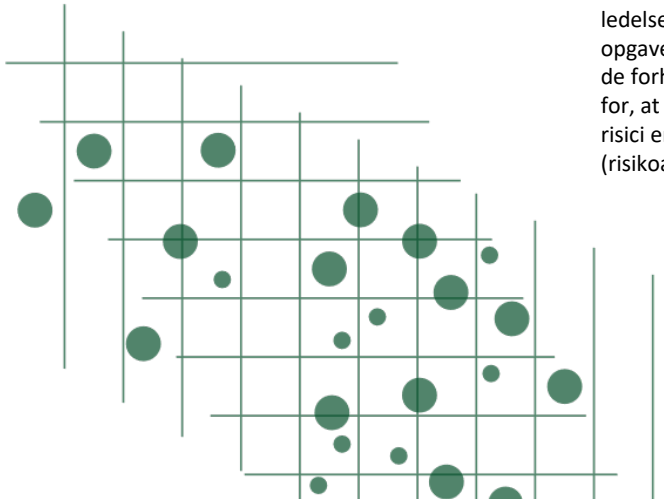
Risikoappetitten er generelt et vigtigt redskab til at koble de strategiske målsætninger sammen med den operationelle drift. Det er bestyrelsens opgave at formulere virksomhedens generelle risikoappetit for alle forretningsområder - og således også risikoappetit i forhold til virksomhedens eksponering 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 højest X timer,
- Vores outsourcingpartnere og underleverandører skal som minimum overholde X.

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

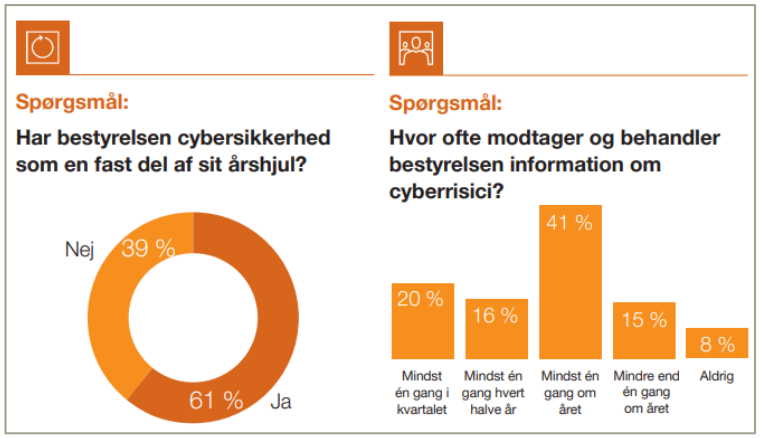
Til at fastsætte risikoappetitten og føre tilsyn med virksomhedens eksponering kan bestyrelsen bruge listen til højre og rapporteringstemplaten i Appendiks 4 til inspiration

Rapporteringstemplaten 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
- 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 indsatser 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-/kontrolfunktionerne en fælles forståelse for cybersikkerhed og prioriteringer (fx hastighed ift 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.?

Risikoafvejning

- Hvad er virksomhedens afvejninger i forhold til fortrolighed, integritet hhv. tilgængelighed, dvs. skal virksomheden vægte fokus på at 1) sikre fortrolighed omkring data – at man 2) kan stole på data eller at 3) 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 er implementeret i et tilstrækkeligt og passende omfang, der matcher virksomhedens risikoappetit.

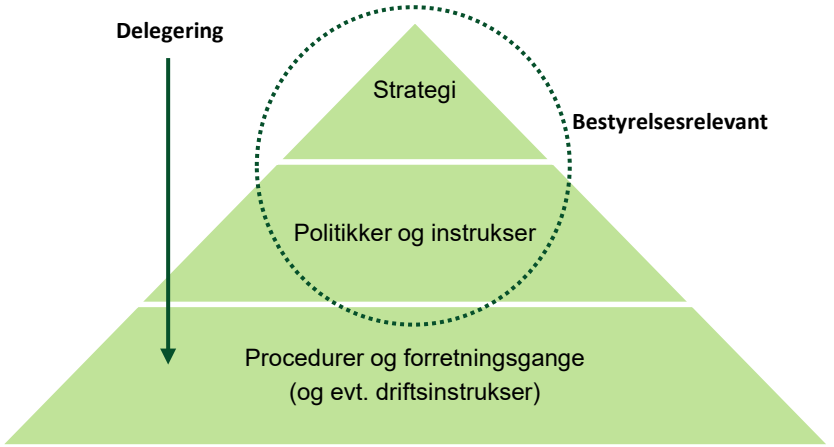
Sikkerhedshændelser kan medføre store omkostninger til udredning, genopretning, driftstab, kompensation til kunder mv. En hurtig og effektiv håndtering vil ofte kunne begrænse omkostningerne væsentligt. Det er derfor vigtigt at have dokumenterede og afprøvede beredskabsplaner, samt være sikker på, at 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. Dette kan eksempelvis være at basere styring af informationssikkerheden på (principperne i) ISO27001, en international standard for styring af informationssikkerhed, der følges af større organisationer og statslige institutioner, og hvis krav generelt er udtryk for best practice, og/eller implementerer sikkerhedskontroller i forhold til CIS18 – 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 føre tilsyn med, hvordan virksomheden har operationaliseret risikostyring af cybersikkerhed indenfor de 5 funktioner: Identificere, beskytte, opdage, håndtere og genoprette (Identify, Protect, Decect, Respond, Recover) – altså virksomhedens samlede cyberforsvar. 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 næste side

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 er forankret i en 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? (fx Mitra?)
- Hvordan afgør man hvilke trusler man anser for sandsynlige og hvordan vurderer I sandsynlighed?
- Hvis X aktiv er vigtigst, har I så et overblik over hvilke systemer der understøtter det? Er der single point of failure?
- Er der et overblik over hvilke systemer og processer der hænger sammen og hvordan er det påvirket af beslutninger der er truffet på strategisk niveau?
- Har organisationen en CMDB (database) til at sikre overblik og transparens over infrastrukturen? (hvad er hvor og hvad hænger sammen med hvad?)
- Gælder det overblik både egne og indkøbte/outsourcede systemer?
- Understøttes selskabets strategi af den infrastruktur man har?
- Hvilke sikkerheds- og sårbarhedsscanninger udføres der?

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 Appendiks 8)
- Har organisationen politikker for brug af kryptografi og kryptering?
- Har organisationen håndteret og mitigeret cybersikkerhedsrisici i forbindelse med anskaffelse, udvikling og vedligehold?
- Har organisationen politikker og processer til at vurdere effektiviteten i 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 hændelseshåndtering (incident handling)?
- Har organisationen en beredskabsplan for driftskontinuitet (business continuity), inklusive back-up og disaster recovery?
- Har organisationen en beredskabsplan for krisestyring, inklusive 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 bestyrelsen/direktion gjort sig overvejelser om fx løsesumsbetaling 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. 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) har I en idé om hvor lang tid det ville tage worst case?
- Kan der laves recovery uden at ødelægge bevisspor, dvs. kan driftsystemer restores uden at slette bevisspor?

Kontrakter og tredjeparter:

- Har organisationen håndteret og mitigeret cybersikkerhedsrisici i sin forsyningskæde, herunder direkte leverandører og kvaliteten i disses produkter og services, sikkerhedsforanstaltninger og udviklingsmetoder?
- I det omfang ydelser er indkøbt / outsourcet hos tredjepart, hvilke krav stiller vi 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 forsikringsselskabet 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, men der er ét aspekt, der gælder 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 anvise, 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 cyber- og informationssikkerhedsområdet, og rapporteringen kan nemt blive subjektiv. Et eksempel på en generisk rapporteringstemplate er vist i Appendiks 4.

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

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

- Aktuel 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 – fx 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)
- Krisehåndtering - ansvar og bemyndigelse
- Begrænsninger og udeladelser
- Anbefalinger til forbedringer og investeringer forbundet hermed
- En inspirationsliste til rapportering er vist i Appendiks 4.

Årshjul

- Har bestyrelsen implementeret cybersikkerhed som en fast del af et årshjul, der sikrer opfølgning og kontrol som en fast del af bestyrelsens arbejde, og sikrer rette rapportering i rette tid?
- Et eksempel på et årshjul med cyberaktiviteter er vist i Appendiks 6.
- Kontrol og revision (på sikkerhed)
- Får virksomheden udarbejdet revisorerklæringer i forhold til it sikkerhed, f.eks. ISAE3402 eller ISAE3000?
- Stiller virksomheden krav om, at dets kunder eller leverandører får udarbejdet disse erklæringer?
- Er der opmærksomhedspunkter fra disse rapporter, og hvis ja, en plan for udbedring?

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?

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 højere 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 til at trykke på et forkert link, der kan føre til 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 – ubevidst (fejl, offer for social engineering mv.) eller bevidst (utilfredse medarbejdere, opportunister, 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, direktionen og medarbejdere løbende modtager uddannelse i cyberrisici, f.eks. gennem deltagelse i eksterne kurser, arrangementer, 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 er 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 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 bestyrelsen, direktion og organisationen faktisk har eller har adgang til de nødvendige kompetencer og ressourcer på cyberområdet – om nødvendigt gennem aftaler med eksterne samarbejdspartner 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 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 kontroller hvad? (lines of defense) - kontrollerer risikoejeren sig selv?
- Er risikovurderingen alene forankret i forretningen eller er der også risiko/kontrolfunktion?
- 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 og best practices for at give cybersikkerhed et ekstra perspektiv?

APPENDIKS

Appendiks 1

Regulatorisk landskab

Cybersikkerhedsregulering

Cybersikkerhedsområdet er de seneste år blevet mere reguleret, især drevet af EU-samarbejdet.

I 2016 vedtog EU-kommissionen det første direktiv om net- og informationssikkerhed (*NIS1*). NIS1 er EU's første horisontale lovgivning om håndtering af cybersikkerhedsudfordringer, dvs. det gælder på tværs af forskellige sektorer i samfundet (konkret 7 sektorer).

NIS1 har – sammen med persondataforordningen (GDPR) – indtil videre været det vigtigste lovgivningsmæssige tiltag for at øge sikkerhedsniveauet og modstandsdygtigheden over for cyberangreb og databrud.

Bortset fra GDPR har cybersikkerhedsområdet dog været sparsomt reguleret. NIS1 og dets tilhørende sektorvise danske regler er primært rettet mod nationale myndigheder og kritisk infrastruktur. Den finansielle sektor er hertil underlagt regler indenfor outsourcing. På øvrige, uregulerede områder i den private sektor, herunder SMV-segmentet, varierer krav og praksis betydeligt, og er langt fra standardiseret. Det ændres nu.

Medio december 2022 bliver et nyt NIS-direktiv (NIS2) vedtaget i EU. NIS2 træder i kraft i dansk ret september-oktober 2024. En lang række virksomheder indenfor ca. 16 sektorer bliver omfattet af NIS2. NIS2 vil bl.a. indeholde skærpede krav til ledelsen, minimumskrav til styring af cyberrisici, underretning af myndigheder om sikkerhedshændelser indenfor 24-72 timer og bøder for overtrædelser.

NIS2 er en del af EU's digitale strategi, der udmøntes i en lang række initiativer og regulering de kommende år, bl.a. indenfor cybersikkerhed, blockchain kvanteteknologi, kunstig intelligens, 5G/6G netværk og IoT.

På cybersikkerhedsområdet omfatter det bl.a. følgende regulering:

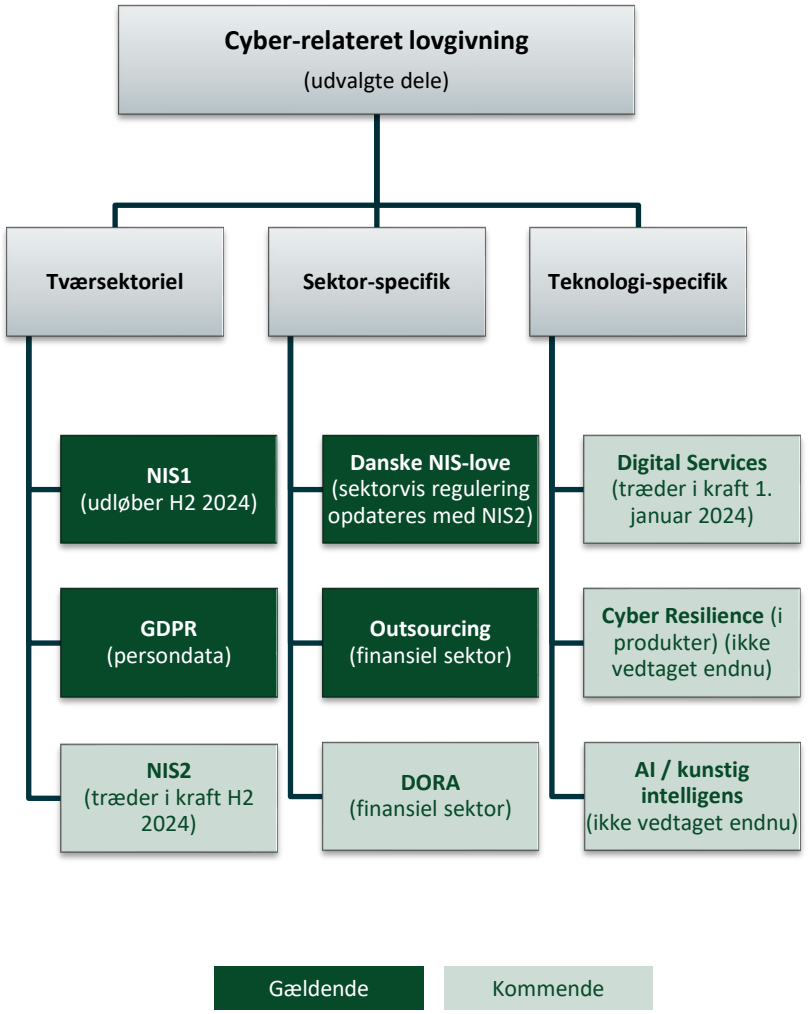
- **NIS2-direktivet**; og
- **DORA-forordningen** om digital operationel modstandsdygtighed i den finansielle sektor.

Indenfor konkrete digitale teknologier omfatter det bl.a. følgende regulering:

- **Digital Services Act Package** med regulering af digitale tjenester og markeder (gældende 1. jan. 2024);
- **Cyber Resilience forordning** om cybersikkerhed i produkter med digitale elementer (ikke vedtaget);
- **AI forordning** om en fælles europæisk tilgang til kunstig intelligens (ikke vedtaget).

For langt de fleste virksomheder (små som store) vil reglerne i NIS2 og GDPR være de primære lovkrav, de enten skal opfylde eller orientere sig mod.

Udvalgt regulering indenfor cybersikkerhed



Ledelsesansvar

I Danmark er ledelsens ansvar for cyber- og informationssikkerhed først og fremmest baseret på et civilretligt ansvar, hvorefter en direktør eller et bestyrelsesmedlem kan ifalde erstatningsansvar, hvis personen har handlet uagtsomt, herunder manglende overholdelse af selskabslovens §115 om etablering af "fornødne procedurer for risikostyring og interne kontroller".

Ansvarsnormen, som ledelsesmedlemmer vurderes efter, følger dansk rets almindelige culpaansvar. Culpabedømmelsen er baseret på en adfærdsstandard og er dermed relativ. Standarden stiller overordnet krav om en "forsvarlig adfærd", der ikke er "uagtsom".

Ved bedømmelsen af om der er handlet culpøst, vil den grundlæggende ansvarsnorm være en pligt til at præstere en god faglig indsats, hvilket vil sige en indsats, der opfylder de krav, man kan stille til et professionelt ledelsesmedlem i den pågældende type virksomhed.

I teori og retspraksis er det anerkendt, at domstolene er tilbageholdende med at tilsidesætte beslutninger, der hviler på et forretningsmæssigt skøn (også kendt som "Business Judgment Rule").

Business Judgment Rule indebærer, at der er en bred margin for ledelsens forretningsmæssige handlinger, forudsat at de er baseret på et forsvarligt beslutningsgrundlag. Hvis et forretningsmæssigt skøn således er truffet på et forsvarligt beslutningsgrundlag, er det ikke ansvarspådragende, hvis beslutningen senere viser sig at være forkert eller ugunstig, medmindre der er tale om et alvorligt fejlskøn.

Business judgment rule
eksempler indenfor cybersikkerhed

Overholdelse af minimumskrav i lovgivning er ikke underlagt et skøn, og er dermed heller ikke underlagt Business Judgment Rule.

For eksempel er det ikke et skøn eller et valg:

- om ledelsen skal udarbejde en **strategi** for cybersikkerhed,
- om ledelsen skal udarbejde en **risikovurdering,** der tager højde for bl.a. eksponering, størrelse, sandsynlighed og konsekvens,
- om bestyrelsen skal fastlægge **risikoappetitten** indenfor cybersikkerhed,
- om ledelsen skal **godkende** sikkerhedsforanstaltninger (i lyset af den konkrete risikovurdering),
- om foranstaltningerne skal opfylde minimumskravene i **lovgivning** (som virksomheden er omfattet af), og
- om ledelsen løbende skal føre **tilsyn** med strategiens gennemførelse.

Det er derimod et vidt forretningsmæssigt skøn:

- *hvordan* strategien nærmere skal se ud,
- *hvor omfattende* risikovurderingen skal være,
- *hvor meget* risiko virksomheden er villig til at tage,
- *hvilke* sikkerhedsforanstaltninger der konkret skal anvendes (når lovens minimumskrav er opfyldt),
- *hvordan* risikostyringsarbejdet skal tilrettelægges, og
- *hvilke* kontroller der skal måles på,

– forudsat, at beslutningen et truffet på et forsvarligt grundlag.

Appendiks 2

Sikkerhedsstandarder

Indledning

Et effektivt cyberforsvar kan ikke klares med tekniske løsninger alene. Det kræver en overordnet, bestyrelsesgodkendt cybersikkerhedsstrategi, løbende risikovurderinger, politikker og testede handlingsplaner, rapportering og kontrol samt uddannelse og awareness. For at kunne tilgå og styre denne opgave på en struktureret og ensrettet måde, er det relevant at kende de mest gængse rammeværk indenfor cybersikkerhed.

Rammeværk forstås og opfattes generelt ens, hvilket gør cybersikkerhedsarbejdet og forståelsen af IT-anvendelsen mere ensrettet og transparent. Rammeværker er også med til at lette samarbejdet mellem kunder og leverandører, og understøtter overholdelse af regulatoriske og kontraktuelle krav, bl.a. indenfor NIS- og databeskyttelseslovgivningen.

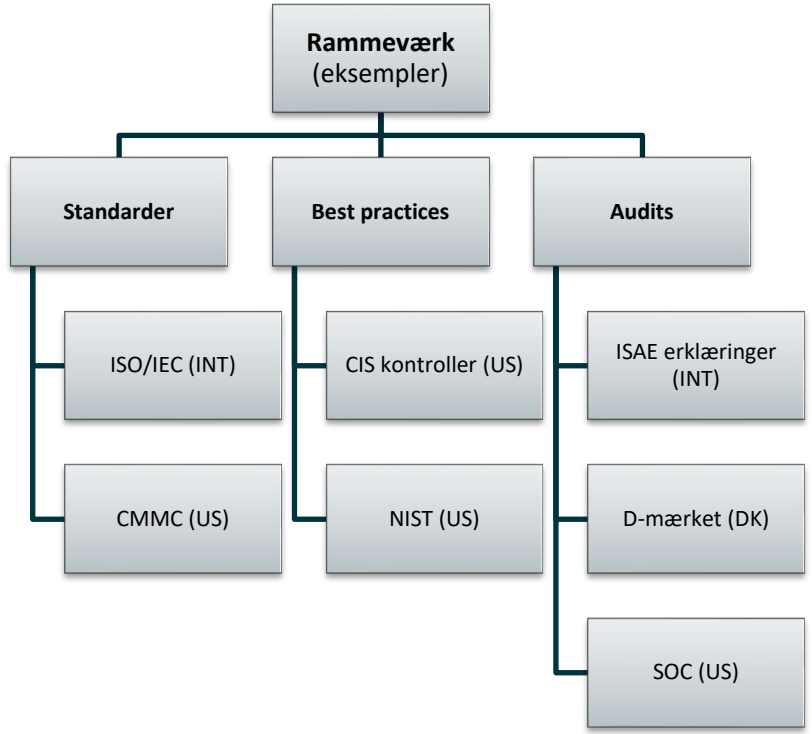
Der findes efterhånden en del rammeværk inden for cybersikkerhed. Formålet med dette appendiks er at give et overblik over nogle af de mest udbredte og anerkendte rammeværk i Danmark og internationalt.

Det er vigtigt at understrege, at der er stor forskel på, *hvilke* rammeværk der anvendes, *hvordan* de anvendes og i hvilken udstrækning, samt om virksomheder lader sig *certificere eller auditere* efter dem (helt eller delvist) eller blot følger (nogle af) principperne i dem. Dette afhænger først og fremmest af den enkelte virksomheds størrelse, ydelse, marked og de krav, der stilles til den gennem såvel lovgivning og myndigheder som kunder og samarbejdspartnere.

Uanset den enkelte virksomheds situation og kontekst, er rammeværkerne dog gode at kende til og orientere sig mod - ikke mindst i lyset af, at anvendelsen af standarder og certificeringer må forventes at stige i de kommende år.

Generelt kan rammeværkerne inddeles i ***1)*** egentlige standarder, ***2)*** best practices og ***3)*** audits. De i dette appendiks nævnte sikkerhedsstandarder fordeler sig i de tre kategorier som vist i figuren til højre, og beskrives på de følgende sider.

Udvalgte rammeværk indenfor cybersikkerhed



Standarder

ISO27001 (INT)

ISO 27001 (formelt kendt som ISO/IEC 27001) er en international standard for et informationssikkerhedsstyringssystem (ISMS). Et ISMS er en ramme af politikker og procedurer, der omfatter alle de juridiske, fysiske og tekniske kontroller, der indgår i en organisations risikostyringsprocesser.
ISO27001 beskriver kravene til etablering, implementering, vedligeholdelse og løbende forbedring af et ISMS. Organisationer, der opfylder standardens krav, kan vælge at blive certificeret efter ISO27001, eller hvilke at dele af forretningen certificeres, hvilket kræver gennemførelse af en revision/audit og årlige re-certificeringer.

ISO27002 (INT)

ISO 27002-standarden indeholder retningslinjer for informationssikkerhed, der er beregnet til at hjælpe en organisation med at implementere, vedligeholde og forbedre sin informationssikkerhedsstyring. ISO 27002 anviser en lang række potentielle kontroller og kontrolmekanismer, der understøtter ISO 27001.

IEC 62443 (INT)

IEC 62443 er en international serie af standarder for cybersikkerhed i operationel teknologi (altså produktionsudstyr) i automatiserings- og kontrolsystemer såkaldte OT/ICS-systemer (OT = Operational Technology og ICS = Industrial Control Systems).

Standarden, der udgives og vedligeholdes af den internationale elektrotekniske standardiseringsorganisation, IEC, er opdelt i forskellige sektioner, og beskriver både de tekniske og procesrelaterede aspekter af cybersikkerhed i OT-systemer.

CMMC (US)

Cybersecurity Maturity Model Certification (CMMC) er et nyere, amerikansk rammeværk indenfor IT-sikkerhed udviklet i samarbejde mellem en række universiteter, forsvarsindustrien og det amerikanske forsvarsministerium. CMMC er inddelt i tre niveauer (levels), hvor 1 er det laveste og 3 er det højeste, og er et krav til leverandører til det amerikanske forsvar.

Best practices

CIS-kontrollerne (CIS18) (US)

CIS18-kontrollerne består af 18 prioriterede, praktiske og konkrete kontroller (sikkerhedstiltag), som er udviklet og vedligeholdes af Center for Internet Security (en non-profit organisation grundlagt i USA).

CIS18 vejledningen kommer med konkrete anvisninger til, hvordan kontrollerne kan implementeres samt konkrete anvisninger til, hvordan deres implementering kan måles.

Til forskel fra ISO27001 kan man ikke blive certificeret efter CIS18, bl.a. fordi kontrollerne løbende opdateres, men det er muligt at måle implementeringen f.eks. i form af en CIS18 modenhedsvurdering.

CIS18 bestod tidligere af 20 kontroller (og blev derfor kaldt CIS20), og er oprindeligt udviklet af SANS Institute, og var tidligere betegnet SANS Critical Security Controls (SANS Top 20). Disse navne ses stadig refereret.

NIST Cybersecurity Framework (US)

NIST Cybersecurity Framework (CFS), ofte blot betegnet NIST CFS, er et rammeværk for implementering af cybersikkerhed udviklet af National Institute of Standards and Technology (NIST) i USA.

NIST rammeværket består af fem hovedområder, som virksomheden skal have styr på: Identificer, Beskyt, Opdag, Håndter og Genopret.

Anbefalingerne fra Bestyrelsesforeningens Center for Cyberkompetencer A/S er bl.a. bygget op omkring NIST rammeværket.

Audits

ISAE 3000 (INT)

ISAE står for ”International Standard on Assurance Engagements”, og udgives af International Federation of Accountants (IFAC).

ISAE 3000 er en ramme for revision af ikke-finansielle oplysninger, dvs. ISAE3000 indeholder ikke specifikke sikkerhedskrav, men retningslinjer for selve revisionen. Det er derfor vigtigt at læse, hvad en specifik ISAE3000 erklæring rent faktisk omfatter. ISAE 3000 udstedes efter et audit af en ekstern auditor/revisor.

ISAE 3000 fastlægger to typer af audit rapporter: 1) Type I, der er et "øjebliksbillede" af organisationens implementering af sikkerhedskontroller, og 2) Type II, der efterviser overholdelse og efterlevelse typisk i en periode på 12 måneder.

ISAE 3402 (INT)

ISAE 3402 er en international revisionsstandard, som anvendes ved revision af serviceleverandører, herunder særligt it-serviceleverandører. Revisionserklæringerne anvendes ofte som dokumentation for overholdes af et passende sikkerhedsniveau. Som ved generelle ISAE3000 erklæringer er det vigtigt at undersøge, hvad erklæringen rent faktisk omfatter.

D-mærket (DK)

D-mærket er en dansk mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse. Målet med D-mærket er at tydeliggøre hvilke virksomheder, der udviser digital ansvarlighed og dermed giver både forretningsværdi til virksomhederne, tryghed til forbrugere og kunder og skaber et stærkere digitalt Danmark.

D-mærket tildeles virksomheder efter en certificeringsproces, hvor virksomheden skal opfylde en række krav til bl.a. processer og sikkerhedstiltag. Kravene til virksomheden fastsættes ud fra en række kriterier bl.a. størrelsen af virksomheden.

Audits

SOC (US)

SOC står for ”Service Organization Control”, og er rammer, der er oprettet af American Institute of Certified Public Accountants (AICPA) til rapportering om den interne kontrol inden for en organisation.

Certificeringen sker på baggrund af en gennemgang af en ekstern auditor/revisor.

SOC1 (US)

SOC1 anvendes til certificering af service organisationer, så de kan vise, at de særligt lever op til en række organisatoriske sikkerhedskrav med fokus på sikring af finansiel rapportering.

SOC2 (US)

SOC2 er en certificering fokuseret på drift og compliance og er særligt rettet mod (større) serviceudbydere, særligt indenfor cloud computing, outsourcing og datasikkerhed.

SOC2 definerer kriterier for styring af kundedata baseret på sikkerhed, tilgængelighed, behandlingsintegritet, fortrolighed og privatliv.

Appendiks 3

Template til cybersikkerhedsstrategi

Indledning

Bestyrelsen og ledelsen har ansvaret for den overordnede forretningsstrategi, herunder hvordan denne realiseres gennem en digital strategi. Formålet med en cybersikkherhedsstrategi er både at beskytte forretningen og at understøtte den digitale strategi, der skal bruges til at realisere forretningsstrategien.

Som beskrevet i vejledningen (side 16-20), er der en række overvejelser, som bestyrelsen bør gøre sig i forbindelse med udarbejdelse af en cybersikkerhedsstrategi. Når bestyrelsen har sat hegnspælene for cybersikkerhedsstrategien, er det virksomhedens opgave at gennemføre de konkrete handlinger og kontroller, der er påkrævet for at implementere den sikkerhed, der passer til virksomheden og den bestyrelsesgodkendte risikoappetit.

Til at udarbejde eller opdatere cybersikkerhedsstrategien kan bestyrelsen lade sig inspirere af de grundlæggende spørgsmål nedenfor og overvejelserne til højre.

Hvis bestyrelsen ikke tidligere har arbejdet (særligt grundigt) med en cybersikkerhedsstrategi, kan det være en god idé at sætte ekstra tid af til punkt 1-3 nedenfor, f.eks. et halvdags-seminar med bistand fra eksterne rådgivere, og at bestyrelsen derefter regelmæssigt får lejlighed til at følge virksomhedens arbejde med at implementere og gennemføre de prioriterede tiltag.

Inspiration til, hvordan bestyrelsen kommer i gang med at udarbejde en cybersikkerhedsstrategi:

1. Overblik – hvad gør vi i dag – hvad har vi i dag? Hvordan arbejder vi med trusler, sårbarheder, modenhed og beskyttelsesværdige aktiver? Hvordan ser vores samlede risikobillede ud?
2. Hvilke nøglekomponenter har direktionen forberedt til bestyrelsen – hvad er vores kronjuveler, trusselsvurderinger, sårbarhedsanalyser, kompetence-gab og tværgående risikovurderinger?
3. Samlet prioriteringsplan og investeringsplan – skal vi satse på forebyggelse eller på, at vi kan genoprette alle systemer på få timer? Hvad er vores prioritering, og hvad koster de forskellige valg og hvilken afdækning af risiko giver de os?
4. Årshjul – hvor ofte skal vi genbesøge strategien og de enkelte komponenter i den? Skal vi have et bestyrelsesudvalg, der har fokus på det eller er det revisionsudvalget? Hvilke kompetencer skal bestyrelsen have?

Centrale overvejelser til udarbejdelse af en cybersikkerhedsstrategi

1. **Hvorfor er denne strategi vigtig for os?**
    a) Forretningskontekst – hvad er på spil for os – hvorfor er det digitale så afgørende vigtigt for os?
    b) Ledelse og Governance – hvordan beslutter vi strategien og dens implementering – hvem gør hvad hvornår hvordan (og hvordan delegeres)?
    c) Definitioner – hvad forstår vi ved de begreber vi burger – vi skal alle tale det same sprog?
    d) Hvilket rammeværk anvender vi – ISO 27001, NIST, CIS eller et andet?
2. **Hvad er vores License to Operate (LtO)-aktiver?**
    a) Hvordan har vi identificeret og rangordnet vores mest værdifulde virksomhedskomponenter (LtO-aktiver, jf. vejledningens side 18)?
    b) Hvorfor er disse så vigtige, at vores forretning tager væsentlig skade, hvis vi mister dem?
3. **Hvad truer os – og hvorfor er vi sårbare overfor truslerne?**
4. **Risiko og håndtering af risiko**
    a) Hvordan arbejder vi med risikoniveauer – hvordan sikrer vi at vi på tværs af organisationen forstår risiko på den samme made?
    b) Hvordan udarbejder vi vores risikovurdering?
    c) Hvordan skabes der en klar plan for imødegåelse af risiko. Hvordan ser investeringsplanen og prioriteringsplanen ud?
5. **Rapportering**
    a) Hvordan skal der rapporteres på strategien – og til hvem og hvornår?
    b) Hvilke krav stilles til vores leverandører – hvordan rapporterer de på deres risikoafdækning og deres "impact" på vores forretning?

Appendiks 4

Template til bestyrelsesrapportering

Indhold

Indledning

Dette bilags formål er at indkredse, hvilke områder og emner, der typisk bør indgå i cyberrisiko rapportering. De enkelte afsnit indeholder derudover skabeloner, der kan inspirere til en ramme for rapporteringen på de enkelte emner.

Indholdet i rapporteringseksemplerne tager udgangspunkt i en fuldstændig fiktiv virksomhed, der ikke præsenteres nærmere. Der er angivet eksempler på rapporteringstekst i kursiv. Eksemplerne skal tjene til inspiration samt som en indikation af den foreslåede detaljeringsgrad. Det er relevant at inkludere rapportering af såvel status og ændringer, hvilket der ligeledes er eksempler på. Den relative vægt afhænger af virksomhedens og bestyrelsens profil.

Der gøres opmærksom på, at det konkrete indhold, emner og eksempler således ikke må ses som fuldstændigt og udtømmende, men altid skal tilpasses den aktuelle virksomhed og dens opbygning, aktiver, aktiviteter og trusselsbillede mm.

1. Aktuel risiko status
– *sammenfatning af risikostatus*

Kortfattet beskrivelse af væsentligste hændelser siden seneste rapport og den aktuelle risikostatus – samt sammenfatning og konklusion (executive summary).

Eksempel til inspiration:

Samlet vurderes det, at selskabet er indenfor/udenfor den risiko der hidtil har været vurderet acceptabel (1). Vurderingen baseres på:

1. Udviklingen i den samlede risikovurdering

2. Hændelser i perioden
- a. Eksternt
- b. Internt
- c. [øvrig]

3. Status for porteføljen af cyber sikkerhedsrelaterede projekter

4. Teknologirelaterede risici

5. Personalesituationen

6. Status på sikkerhedskategorierne

Den samlede risikoprofil vurderes at eksponere selskabet for tab op til [X].

Beløbet fremkommer ved at sammenlægge et overslag over omkostningerne til at genskabe de væsentligste aktiver (”License to Operate”-aktiverne, ”kronjuvelerne” osv.) med effekten fra manglende/reduceret drift i en genopretningsperiode.

Kommentar:

Det anerkendes, at det er overordentligt vanskeligt at vurdere virksomhedens potentielle tab. Det er ikke desto mindre særdeles vigtigt at lave et kvalificeret estimat, idet det er væsentligt for at kunne prioritere anvendelsen af virksomhedens ressourcer, der naturligt måles økonomisk.

(1) Den ”acceptable risiko” omtales også ofte som ”risikoappetitten”. Den udtrykker den risikoprofil bestyrelsen accepterer, at virksomhedens strategi medfører. Det kan være udsagn som: ”Det maksimale antal kunde reklamationer er XX pr. måned”; eller ”Den længste acceptable periode med utilgængelighed til vores XX er YY.” Risikoappetit er et bredt begreb, og de angivne udsagn er alene indikationer af, hvad der kan være relevant. Det er naturligvis helt afhængigt af virksomhedens konkrete prioriteter.

Eksempel på en skematisk rapportering af status
(fra både forretningen og kontrolfunktion):

Alle	(Forretnings)-Risikoejer						Kontrol	Direktion/ledelse			Bestyrelse
LtO- aktiver /aktiviteter (ikke tekniske)	Brutto risiko*	Risikotiltag* (forebyggelse)	Risikotiltag* (beredskab)	Netto risiko*	C-I-A	Økonomisk konsekvens pr. dag/event/xx	Risiko-vurdering	Samlet risiko nettorisiko	Anbefaling** ift anbefalet risikoaccept (penge-tid-tab, kundedata…)	Investerings-behov	Risikoappetit / investerings-beslutning
Aktiv/proces/ forretnings-område 1	[1-5]			[1-5]	C	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 2	[1-5]			[1-5]	I,A	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 3	[1-5]			[1-5]	A	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 4					C,A						
…					…						

Eksempel på rapporttemplate

Nedenstående er et eksempel på en fremgangsmåde for risikovurdering og -rapportering af en samlet risikooversigt til bestyrelsen. Eksemplet er udarbejdet med udgangspunkt i forretningskritiske aktiver (LtO aktiver)

---

1. Identifikation af LtO-aktiver:
- Beskrivelse af, hvilke dele af forretningen, der er særlig væsentlig (***Identificér***).
- Vurderingen af virksomhedens LtO aktiver bør fastlægges af alle stakeholders = bestyrelsen, direktion, forretning og kontrolfunktioner.
- Skal sammenholdes med virksomhedens strategi, forretningsmål og forretningsmodel.

2. Vurdering af risikoejeren
- Risikoejerens vurdering af sikkerhedssituationen for LtO-aktivet. Dette kan være en begrundet evaluering af sikkerhedssituationen baseret på risikoejerens professionelle vurdering.
- Vurdering af den iboende bruttorisiko for dette aktiv/denne aktivitet (trusselsbilledet, systemopbygning, afhængigheder osv)
- Risikoeliminerende tiltag for LtO aktiv (Beskyt).
- Vurdering af den aktuelle ”netto”-risiko = den risiko, som aktiviteten (LtO-aktiv) vurderes at tilføre virksomheden.

De fem ovenstående faktorer kan vurderes under ét med angivelse af en samlet score på en skala, der passer til virksomheden. Typisk vil en 1-5 skala være en relevant mulighed. Den samlede score bør begrundes, og den samlede vurdering (f.eks. 4) kan derefter evt. begrundes.

3. Fortrolighed-Integritet-Tilgængelighed
Den konkrete vurdering for LtO aktiv kan være:
- Fortrolighed er afgørende for LtO aktiv
- Integritet (troværdighed) er afgørende for LtO aktiv
- Tilgængelighed er afgørende / ikke afgørende for LtO aktivet.

Fortsættes…

4. Økonomisk risiko

- Vurdering af det økonomiske tab, hvis LtO aktiv er utilgængelig og/eller der sker tab af indhold eller troværdighed. Omend en økonomisk konsekvensanalyse kan være forbundet med usikkerhed, er en kvantificering ofte et vigtigt element for at kunne styre risici forholdsmæssigt.

5. Vurdering af risikokontrolfunktionen

- Risikokontrolfunktionens (der bør være uafhængig af risikoejeren og evt. ekstern afhængigt af virksomheden og dens størrelse) evaluering af sikkerhedssituationen for LtO aktiv tillagt en begrundet score (f.eks. på en 1-5 skala).

6. Samlet vurdering af den rapportansvarlige

- Den samlede risikovurdering bør fastlægges af den rapportansvarlige, som kan være den ansvarlige i direktionen. Der kan med fordel bruges en farvekodning til den samlede vurdering for visuelt at tiltrække opmærksomheden til de områder, der er mest udfordrede.
- Det bør i sig selv være en advarselslampe, hvis der er forskel på den risikoansvarliges og kontrolfunktionens vurdering

7. Anbefaling af risikoappetit

- En samlet vurdering af LtO aktivets anbefalede risikoappetit – igen baseret på virksomhedens strategi, forretningsmål, samlede risikoprofil og risikoappetit.

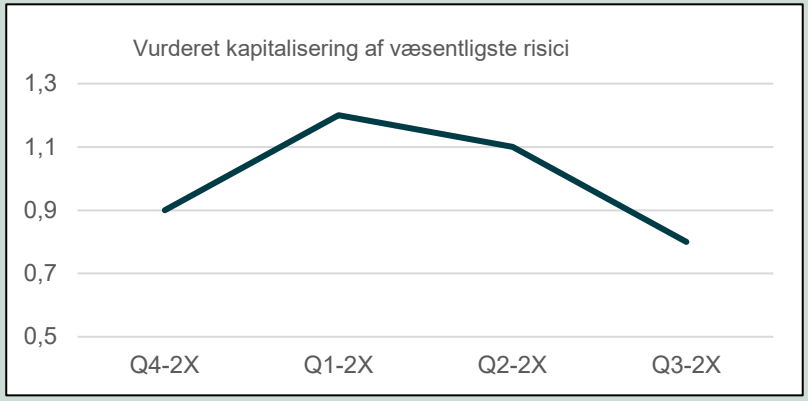
8. Investeringbehov

- Anbefalingen af den tilhørende investeringramme med henblik på at opnå en tilfredsstillende ramme for risikoappetitten/accepten.

9. Bestyrelsens risikoappetit/accept

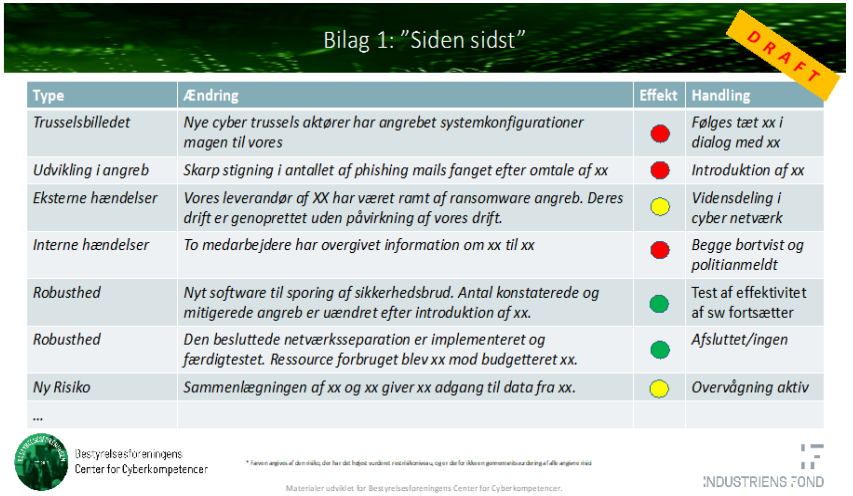
…samt afledte investeringsbeslutninger

Eksempel på grafik til illustration af kapitalisering af væsentligste risici:



2. Aktuelt trusselsbillede

Beskrivelse af udviklingen i trusselsbilledet, spirende risici og virksomhedens sårbarheder. Sårbarhederne kan eksempelvis være anvendelse af digitale løsninger, der har vist sig sårbare i angreb på andre virksomheder. Det kan også være en intern erkendelse af, at en kombination af systemer eller tredje parts løsninger potentielt åbner for misbrugsmuligheder, der er foretaget ændringer i IT-løsninger i virksomheden, etableret integrationsløsninger med nyt datterselskab, nyt markedsområde osv.



Type	Ændring	Effekt	Handling
Trusselsbilledet	*Nye cyber trussels aktører har angrebet systemkonfigurationer magen til vores*	🔴	*Følges tæt xx i dialog med xx*
Udvikling i angreb	*Skarp stigning i antallet af phishing mails fanget efter omtale af xx*	🔴	*Introduktion af xx*
Eksterne hændelser	*Vores leverandør af XX har været ramt af ransomware angreb. Deres drift er genoprettet uden påvirkning af vores drift.*	🟡	*Vidensdeling i cyber netværk*
Interne hændelser	*To medarbejdere har overgivet information om xx til xx*	🔴	*Begge bortvist og politianmeldt*
Robusthed	*Nyt software til sporing af sikkerhedsbrud. Antal konstaterede og mitigerede angreb er uændret efter introduktion af xx.*	🟢	Test af effektivitet af sw fortsætter
Robusthed	*Den besluttede netværksseparation er implementeret og færdigtestet. Ressource forbruget blev xx mod budgetteret xx.*	🟢	*Afsluttet/ingen*
Ny Risiko	*Sammenlægningen af xx og xx giver xx adgang til data fra xx.*	🟡	*Overvågning aktiv*
…			

3. Observationer og kommentarer fra revisorer/rådgivere

Oplistning af modtagne observationer fra rådgivere, interne eller eksterne revisorer, samt status på håndtering af disse. Rapporteringen kan bestå af en systematisk oplistning af observationer i tabelform med en omhyggelig vurdering af hvilke forholdsregler, der er taget for at imødegå disse.

Tabellen kan eksempelvis tage følgende form:

Rådgiver	Observation	Forebyggende tiltag	Udbedrende tiltag	Beskrivelse af status	Status
Sikkerhedsrådgiver	*…Manglende netværkssegmentering*	*…Følgende kontroller er implementeret for at imødegå svaghederne*	*…beskrivelse af forholdsregler der er taget for at reducere risiko eller potentiel effekt.*	*Verbal beskrivelse af status på projektet*	
Intern Revision	*…Adgangskontrol*	*…digital adgangskontrol suppleres med…*	*…implementering af …*	*Verbal beskrivelse af status på projektet*	
Ekstern Revision	*…Mangelfuld test af interne IT-sikkerheds kontroller*	*…Manuelle processer supplerer de automatiserede test kontroller*	*… beskrivelse af den permanenter løsning på problemstillingen*	*Verbal beskrivelse af status på projektet*	

4. Lovgivning og myndighedskrav

Kort beskrivelse af cybersikkerhedsrelevante ændringer i lovgivning, myndighedskrav og –praksis, officielle vejledninger m.v. Formen kan være en systematisk oplistning af væsentlige ændringer i lovgivning, myndighedskrav, praksis, vejledninger m.v. Relevans og væsentlighed af ændringerne kan med fordel beskrives i både en generel og en virksomhedsspecifik sammenhæng reflekterende virksomhedens strategi og forretningsmodel.

5. Interne sikkerhedshændelser

Beskrivelse af de typer af sikkerhedshændelser, der er relevante for virksomheden.

Der kan eksempelvis inkluderes statistik for de seneste 5 rapporteringsperioder samt gennemsnittet af de 4 foregående rapporteringsperioder. Udviklingen i sikkerhedshændelser kan med fordel indeholde data for foregående rapporteringsperioder. Det vil synliggøre udviklingen over tid og give en illustration af eventuelle mønstre i udviklingen.

Der kan eksempelvis udarbejdes en oversigtstabel med:

- Antal sårbarheder
    - Konstateret i kvartalet
    - Elimineret i kvartalet
- Antal svindel- og bedrageriforsøg
- Antal indbrud på platformen(e)
    - Kendte adgange
    - Nye adgange
- Antal phising/adgangskode fangstforsøg, inklusive historik
- Antal malware konstateret
- Antal ransomware konstateret

Relevansen af opdelingen afhænger naturligvis af virksomhedens størrelse og digitale kompleksitet.

5.1 Hændelser rapporteret til myndighederne

Denne beskrivelse er alene en informationsrapportering, der sikrer, at bestyrelsen er informeret om eventuel(le) rapportering(er), der er afsendt til relevante myndigheder både i forhold til antal og type af hændelser. Det vil ofte være relevant at afrapportere dette til bestyrelsen, også selvom der ikke har været deciderede sikkerhedshændelser.

6. Eksterne sikkerhedshændelser

– fx leverandører og outsourcing partnere

Beskrivelse af de typer af sikkerhedshændelser, der er relevante for virksomheden.

Der kan eksempelvis inkluderes statistik for de seneste 5 rapporteringsperioder samt gennemsnittet af de 4 foregående rapporteringsperioder. Udviklingen i sikkerhedshændelser kan med fordel indeholde data for foregående rapporteringsperioder. Det vil synliggøre udviklingen over tid og give en illustration af eventuelle mønstre i udviklingen.

Der kan eksempelvis udarbejdes en oversigtstabel med:

- Antal sårbarheder
    - Konstateret i kvartalet
    - Elimineret i kvartalet
- Antal svindel- og bedrageriforsøg
- Antal indbrud på platformen(e)
    - Kendte adgange
    - Nye adgange
- Antal phising/adgangskode fangstforsøg, inklusive historik
- Antal malware konstateret
- Antal ransomware konstateret

Relevansen af denne rapportering afhænger af den enkelte virksomheds brug af outsourcingpartnere og underleverandører samt de lovgivningskrav, virksomheden er underlagt i relation til styring af og kontrol med outsourcingpartnere og underleverandører.

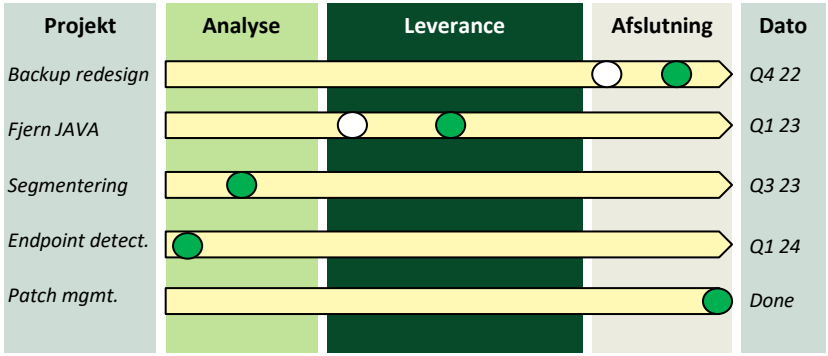
Rapporten vil kunne afsløre en eventuel stigende eksponering samlet set og – væsentligt - skærpe underleverandører og outsourcingpartneres fokus på deres cybersikkerhed. Det er naturligvis afhængigt af relationens størrelse og kritikalitet samt eventuelle lovgivningskrav (f.eks. indenfor den finansielle sektor), om der med relevans og rimelighed kan og skal stilles krav om cybersikkerhedsinformation fra underleverandører og outsourcing partnere.

7. Projekt status

Kortfattet (potentielt grafisk) beskrivelse af hvor langt virksomheden er med forskellige prioriterede projektleverancer, eksempelvis:

"… Project A er fuldendt og betyder at vi nu kan overvåge xxx … Det har ført til … … Antallet for uvedkommende penetrationer af vores firewalls er faldet til XX efter vi har ændret procedure YY …"

En konkret grafik kan med fordel indeholde status og udvikling, hvorfor både den seneste og aktuelle status kan rapporteres. Der kan med fordel anvendes en farvekode på den aktuelle status (eksempelvis rød-gul-grøn). En illustrativ grafik er vist nedenfor:



8. System status

Beskrivelse af det overordnede systemlandskab, herunder systemernes forventede restlevetid og andre relevante forhold, der kan indikere en aktuel eller kommende sikkerhedsudfordring (illustrative eksempler uddybes i de følgende afsnit 8.1 - 8.3).

8.1. Væsentligste generelle (tekniske) risikoområder

	Risiko	Risiko niveau	Trend
Adgangskontrol	*Beskrivelse af risikoen*	Høj	▲
Informations sikkerhed	*Beskrivelse af risikoen*	Høj	▽
Asset Management (2)	*Beskrivelse af risikoen*	Lav	□
IT system risiko	*Beskrivelse af risikoen*	Mellem	▽
Kriseplaner/-håndtering	*Beskrivelse af risikoen*	Lav	▲
Tredje parts risiko	*Beskrivelse af risikoen*	Høj	□

8.2. Risiko- og kontroloversigt (tekniske)

	Risikoejer *(eksempel salg, produktion, HR, osv)*					**Kontrolfunktionen**	
'Kronjuvel'	Proces Beredskab	C-I-A(3)	Kontrol foranstalt-ninger	Økonomisk risiko (DKK)	Vurdering Risikoejer	Vurdering Risiko-kontrol	Samlet
R&D Database	2	C-I	4	110 mio.	2	4	
E-handels hjemme-side	1	A	2	2 mio.	1	2	
…							
…							

Der kan eksempelvis anvendes en skala på 1-5 til at illustrere omfanget af ikke-håndteret risiko, hvor 1 angiver, at alle risici er håndteret, og 5 angiver, at risici er meget mangelfuldt håndteret. Ovenstående tabel er illustrativ. En uddybende beskrivelse af modellens mulige anvendelse er i **afsnit 13** i dette appendiks.

(2) Asset management dækker registrering og opfølgning på hvilke (fysiske og ikke-fysiske) enheder virksomheden har, herunder deres anvendelse, vedligehold og anvendelses, samt håndtering af eventuelle afhændelser. Formålet er at sikre, at der er overblik over, hvilke digitale aktiver der er i virksomheden og deres anvendelse.

(3) C-I-A står for fortrolighed (confidentiality), integritet (integrity) og tilgængelighed (availability), og beskriver hvilke kvaliteter, der er væsentlige ved "License-to-Operate"-aktivet ("kronjuvelen"). Skemaet er opbygget ud fra det overordnede risikooverblik vist i afsnit 8.1 lige ovenfor.

Eksempel på rapporttemplate

Eksempel på en fremgangsmåde for risikovurdering og -rapportering af et "License to Operate"-aktiv, der kan indgå i en samlet risikooversigt til bestyrelsen, for eksempel i en oversigt tilsvarende den i afsnit 8.2 i dette appendiks.

Eksemplet er udarbejdet med udgangspunkt i en forretningskritisk database for produktudvikling (også kaldet en "R&D database") i en fiktiv virksomhed.

1. Procesberedskab:
- Beskrivelse af, hvilke dele af databasen, der er særlig væsentlig (Identificér)
- Forholdsregler for adgangskontrol og eventuelt identifikation af brugere (Beskyt).
- Angivelse af, hvilke metoder der anvendes til identificering af eventuelle forsøg på indbrud (Opdag)
- Beskrivelse af, hvordan en situation hvor databasen er konstateret angrebet, håndteres (Håndtér)
- Vurdering af, hvordan og hvor hurtigt databasen kan genskabes (Genopret)

De fem faktorer kan vurderes under ét med angivelse af en samlet score på en skala, der passer til virksomheden. Typisk vil en 1-5 skala være en relevant mulighed. Den samlede score bør begrundes, og den samlede vurdering (f.eks. 4) kan derefter overføres til oversigten (vist i afsnit 8.2).

2. Fortrolighed-Integritet-Tilgængelighed
Den konkrete vurdering for databasen kan være:
- Fortrolighed er afgørende for databasens anvendelighed
- Integritet af indholdet i databasen er afgørende for dens anvendelighed
- Tilgængelighed er ikke afgørende, idet databasen ikke anvendes i tidskritiske processer.

3. Kontrolforanstaltninger
Vurdering af tilstrækkeligheden af tilgængelige kontrolforanstaltninger til sikring af databasens procesberedskab (1) og C-I-A profil (2).
Vurdering kan eksempelvis lyde:
"*Foranstaltningerne vurderes på baggrund af [x, Y, Z] at være utilstrækkelige, og tildeles en score på 2.*"

4. Økonomisk risiko
Vurdering af det økonomiske tab, hvis databasen er utilgængelig og/eller der sker tab af databasens indhold eller troværdighed. Omend en økonomisk konsekvensanalyse kan være forbundet med usikkerhed, er en kvantificering ofte et vigtigt element for at kunne styre risici forholdsmæssigt.

5. Vurdering af risikoejeren
Risikoejerens vurdering af sikkerhedssituationen for databasen. Dette kan være en begrundet evaluering af sikkerhedssituationen baseret på risikoejerens professionelle vurdering.

6. Vurdering af risikokontrolfunktionen
Risikokontrolfunktionens (der bør være uafhængig af risikoejeren og evt. ekstern afhængigt af virksomheden og dens størrelse) evaluering af sikkerhedssituationen for databasen tillagt en begrundet score (f.eks. på en 1-5 skala).

6. Samlet vurdering af den rapportansvarlige
Den samlede risikovurdering bør fastlægges af den rapportansvarlige, som kan være den cyberrisiko ansvarlige i kontrolfunktionen. Der kan med fordel bruges en farvekodning til den samlede vurdering for visuelt at tiltrække opmærksomheden til de områder, der er mest udfordrede. Det bør i sig selv være en advarselslampe, hvis der er forskel på den risikoansvarliges og kontrolfunktionens vurdering.

Andet eksempel på kontrol:

Forretningssystem	Relaterede risici*	Status på implementering pr. CIS-kontrol område (udvalgte kontroller)							
		Kontrol 3 Data protection		Kontrol 6 Access control management		Kontrol 11 Data recovery		Kontrol 16 Application software security	
		Gennemsnits-vurdering	Antal svar	Gennemsnits-vurdering	Antal svar	Gennemsnits-vurdering	Antal svar	Gennemsnits-vurdering	Antal svar
System A	2, 3, 4, 5	3,8	5/6	2,0	1/1	3,0	4/4	1,1	7/8
System B	2, 3, 4, 5	2,0	1/6	0,0	0/1	3,0	4/4	1,1	8/8
System C	1, 2, 3, 4, 5	3,0	0/6	3,0	0/1	3,0	4/4	1,0	7/8
System D	1, 2, 3, 4, 5	0,0	0/6	5,0	0/1	3,0	4/4	1,0	7/8
System E	1, 3, 4, 5	2,7	3/6	3,0	1/1	3,0	1/4	1,7	6/8
System F	1, 4, 7	2,8	6/6	2,0	1/1	3,0	4/4	2,3	4/8
System G	1, 4, 7	2,0	6/6	0,0	0/1	3,0	4/4	1,6	4/8
System H	4	2,0	1/6	2,0	1/1	3,0	4/4	1,1	8/8
System I	6	N/A	N/A	N/A	N/A	3,0	N/A	N/A	N/A
System J	1, 2, 3, 7	2,2	5/6	2,0	1/1	3,0	4/4	1,8	8/8
System K	2, 4	0,0	0/6	0,0	0/1	3,0	4/4	1,0	8/8
System L	2, 4	1,5	2/6	0,0	0/1	3,0	4/4	1,1	7/8
System M	2, 5	1,5	2/6	2,0	1/1	3,0	4/4	0,0	0/8
System N	1, 2, 7	3,8	6/6	2,0	1/1	3,0	4/4	1,6	7/8
System O	2, 4, 6	N/A	N/A	N/A	N/A	3,0	4/4	N/A	N/A
System P	2, 4, 6	N/A	N/A	N/A	N/A	3,0	4/4	N/A	N/A
System Q	2	1,0	1/6	0,0	0/1	3,0	4/4	1,4	7/8

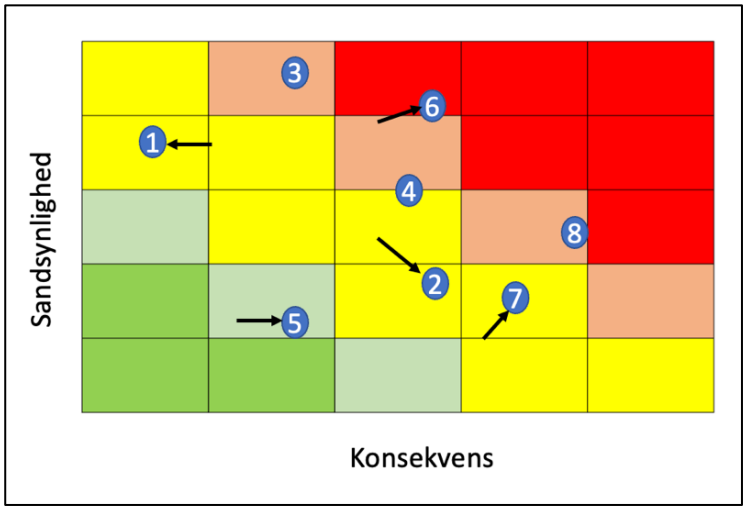
Risici mappes til forretningssystemer, og forretningssystemernes "helbredstilstand" kan måles ud fra CIS-kontrollerne, således at svagheder kan prioriteres efter hvor kritisk systemet er for virksomheden og hvilke risici, det er relateret til.

CIS-kontrollerne består (for nuværende) af 18 prioriterede, praktiske og konkrete kontroller (sikkerhedstiltag) som er udviklet og vedligeholdes af Center for Internet Security. Se mere herom i Appendiks 2 (Sikkerhedsstandarder) til bestyrelsesvejledningen.

8.3. Heat map status med top-X (tekniske) risici

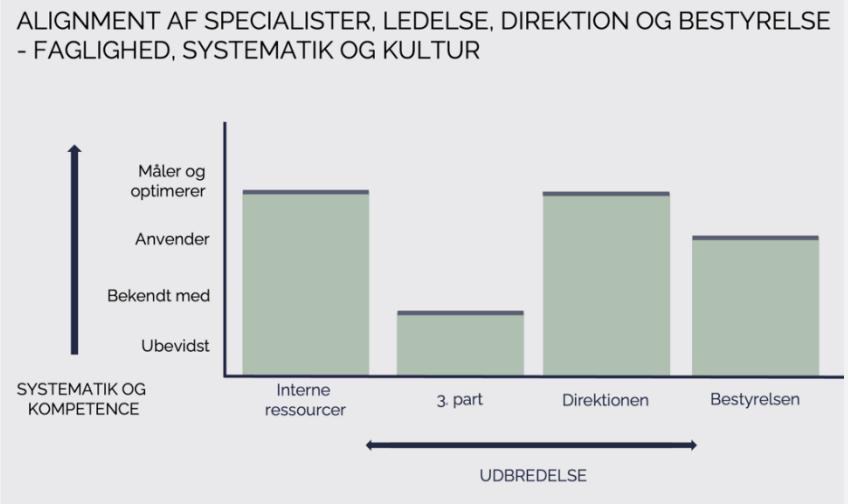
Arbejdet med cybersikkerheds problemstillinger bør inkludere identifikation af de væsentligste virksomhedsrelevante risici og deres potentielle konsekvenser samt en vurdering af sandsynligheden for, at disse risici materialiserer sig.

De resulterende kombinationer af sandsynligheder og konsekvenser kan med fordel indarbejdes i en "heat map" for de aktuelle trusler og risici. Oversigten kan opdateres med den foregående og den aktuelle rapporteringsperiodes observationer og forbindes således, at periodens udvikling illustreres grafisk, som vist i eksemplet nedenfor.

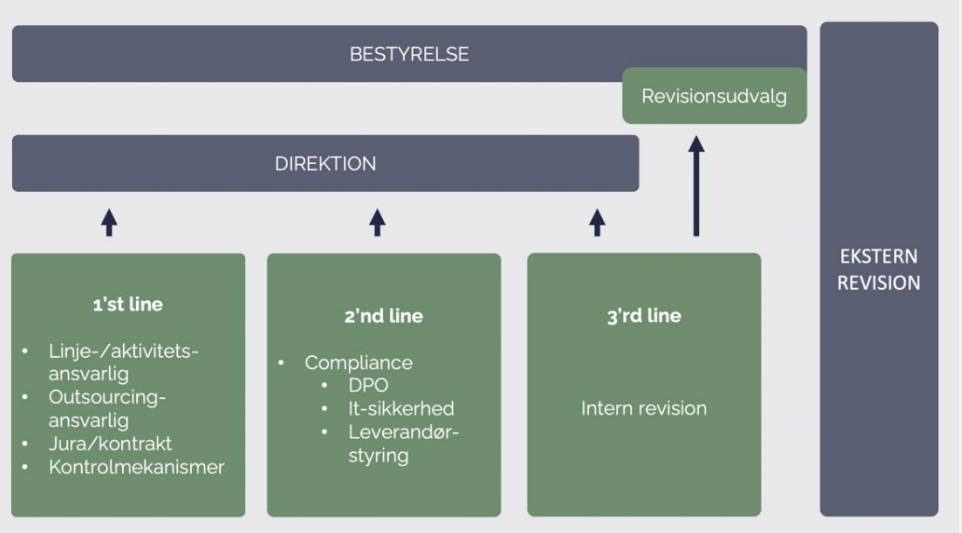


9. Status personale, medarbejdere og organisering

Beskrivelse af eventuel risiko på personaleområdet såsom medarbejderafgang, genbesættelsesmuligheder ved ledige stillinger, personafhængighed osv. Eksempel indsat nedenfor.



Oversigt over organisering og bemanding af (cyber) risikofunktion, herunder uafhængighed af kontrolfunktioner (3 lines of defense). Eksempel indsat nedenfor.

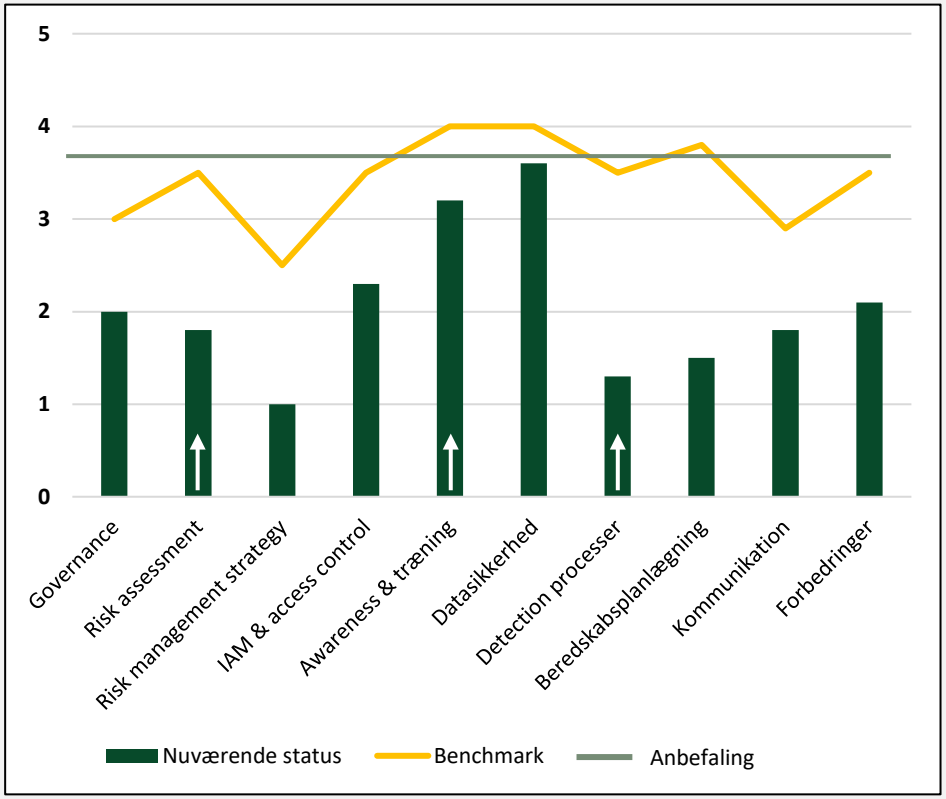


10. Status på sikkerheds-kategorier generelt (NIST)

Kort beskrivelse af virksomhedens modenhedsniveau i forhold til det ønskede modenhedsniveau ud fra NIST-modellens 5 funktioner: Identificer, beskyt, opdag, håndter og genopret. Eksempler indsat nedenfor og til højre.

Område	Sårbarhed/ svaghed	Aktiviteter	Status
Identificér	Overskrift eller kort beskrivelse af sårbar-/svaghed	Afsluttede, igangsatte og fremtidige generelle aktiviteter kort beskrevet	Rapportejerens vurdering af den generelle status for området
Beskyt	Overskrift eller kort beskrivelse af sårbar-/svaghed	Afsluttede, igangsatte og fremtidige generelle aktiviteter kort beskrevet	Rapportejerens vurdering af den generelle status for området
Opdag	Overskrift eller kort beskrivelse af sårbar-/svaghed	Afsluttede, igangsatte og fremtidige generelle aktiviteter kort beskrevet	Rapportejerens vurdering af den generelle status for området
Håndtér	Overskrift eller kort beskrivelse af sårbar-/svaghed	Afsluttede, igangsatte og fremtidige generelle aktiviteter kort beskrevet	Rapportejerens vurdering af den generelle status for området
Genopret	Overskrift eller kort beskrivelse af sårbar-/svaghed	Afsluttede, igangsatte og fremtidige generelle aktiviteter kort beskrevet	Rapportejerens vurdering af den generelle status for området

Eksempel på modenhedsoverblik
(illustrativt)



11. Krisehåndtering - ansvar og bemyndigelse

Skematisk beskrivelse af krisestaben (incident response team) med kontaktdetaljer og bemyndigelser i en krisesituation. Det vil ofte være vigtigt, at der er identificeret stedfortrædere for alle roller. En oversigt over et incident response team er forventelig ganske statisk og kan medtages i rapporteringen for at sikre, at risikorapporteringens modtagere derigennem vænnes til at se denne information, der er vigtig at have tilgængelig i en krisesituation.

12. Begrænsninger og udeladelser

Beskrivelse af eventuelle begrænsninger i rapporten, herunder områder der ikke er medtaget på grund af eksempelvis manglende datagrundlag eller dokumentation. For hver undladelse bør der kommenteres på, om den har væsentlig betydning for indholdet og validiteten af rapporten.

Appendiks 5

Cyberforsikringer

Indledning

Cyberforsikringer
Cyberforsikringer er et relevant redskab at overveje til risikoafdækning, men er i dag stadig et nicheprodukt med ganske stor variation i vilkår og præmier hos de (relativt) få forsikringsselskaber, som tilbyder dem.

Det forventes, at brugen af cyberforsikringer vil stige i de kommende år, herunder at det på nogle markeder og indenfor bestemte sektorer er eller vil blive et krav at tegne cyberforsikring, og at forsikringsmarkedet dermed kan være med til at drive sikkerhedsniveauet op. Denne udvikling forudsætter dog, at der sker en højere grad af standardisering på markedet, end det er tilfældet nu (ultimo 2022).

Det er pt. ikke politisk vilje til at gøre cyberforsikringer til et krav i Danmark.

Forsikringsmarkedet
Cyberforsikringer er i disse år i et såkaldt "hard market" med stigende præmier, flere dækningsbegrænsninger og højere underwriting standarder (pga. risiko for større tab).

Samtidig er der (relativt) få selskaber, der tilbyder en bredere portefølje af cyberforsikringer. Både forsikringsbrokere og -selskaber synes at have en vis tilbageholdenhed med at (ny)tegne IT- og cyber-relaterede risici. Det skyldes bl.a. det øgede trusselsbillede og det stigende antal ransomware-angreb mod danske virksomheder, der har medført, eller kan medføre, større tab end forventet.

Gode råd

Det er en forretningsmæssig vigtig beslutning, i hvilket omfang virksomheden ønsker at tegne en cyberforsikring. Gode råd til overvejelser er:

- Gør det til et bevidst til- eller fravalg af cyberforsikringer baseret på en afvejning mellem risikovurdering og risikoappetit på den ene side og værdien af en forsikring (i præmie og dækning) på den anden side;
- Vær opmærksom på hvilke dækninger, der fås – og om forsikringen dækker de sandsynligt største tab (se eksempler på dækningselementer til højre); og
- Hav fokus på krav og undtagelser: Hvilke krav stiller forsikringsselskabet til sikkerhedsniveau og dokumentation, og hvor konkrete eller brede er undtagelserne til dækningen? (imødegå manglende transparens).

Eksempler på forskellige dækningselementer i cyberforsikringer

Vilkår afhænger bl.a. af, hvilken dækning der ønskes og med hvilke beløb

Egne tab og omkostninger

- Incident / Beredskab (egne)
- Retablering af data (egne)
- Driftsforstyrrelser / driftstab (egne / afledt)
- Løsepenge (egne)
- Bøder, sanktioner, advokat mv. (egne)
- Økonomisk kriminalitet (egne)
- Omdømmetab (egen)
- Identitetstyveri (egen)

Tredjeparts tab og omkostninger

- Erhvervsansvarsforsikring (tredjeparts)
- Datasikkerhed (privacy) (tredjeparts)
- Bøder, sanktioner, advokat mv. (tredjeparts)
- IPR krav (tredjeparts)
- Netværksbrud / datatab (tredjeparts)

Appendiks 6

Emner til bestyrelsens årshjul

Emner til bestyrelsens årshjul

- i forhold til cybersikkerhedsstrategien samt implementering og opfølgning på denne

Møde	Tema	Primære emner på agenda	Eksempler på fokusområder
Juni	**Strategi** (Tema 1-6)	• Cybersikkerhedsstrategi • Statusrapport[1]	• Trusselsbilledet • Risikovurderinger – LtO-aktiver[2] og aktiviteter • Risikoappetit og evt. investeringer • Forankring i organisationen • Fastlæggelse af rapportering og opfølgning
August	**Politikker, processer og beredskab** (Tema 3)	• Politikker • Forretningsgange • Instrukser • Statusrapport[1]	• Lovgivning • Opdateringer af diverse politikker, forretningsgange, instrukser, planer m.v. samt sikring af samkøring med aktuel cybersikkerhedsstrategi • Brug af rammeværker (fx D-mærket, ISO 27001, jf. Appendiks 2)
Oktober	**Politikker, processer og beredskab** (Tema 3)	• Operationalisering • Statusrapport[1]	• Forsyningskæder • Leverandørsikkerhed • Kontrakter • Krise-, kommunikations- og beredskabsplaner • Samarbejdsaftaler
December	**Kultur** (Tema 5) **Governance** (Tema 6)	• Kultur • Træning • Organisation • Cyberkompetencer • Governance • Statusrapport[1]	• Forankring af politikker og forretningsgange • Træningsprogrammer og sikring af læring (inkl. fra nærved-hændelser) • Organisering – herunder god rapportering • Hvem kontrollerer hvem (og om succeskriterier er forenelige med cybersikkerhedsstrategiens målsætninger)
Jan/februar	**Risikoappetit** (Tema 2)	• Risikoafvejning • Risikoappetit • Statusrapport[1]	• Risikohåndtering (forebyggelse og/eller genopretning) • Beredskabsplaner • Backup og andre genopretningsløsninger • Forsikringer
Marts/april	**Rapportering** (Tema 4) (regnskab)	• Kontrolmiljø • Rapporteringer • Statusrapport[1]	• Vurdering og kvantificering af risici • Evaluering af løbende rapportering • Input fra rådgivere, advokat, revisor m.v. • Kvalitetssikring

[1] Statusrapport = operationel statusrapport for drift, trusler, hændelser m.v.

[2] LtO aktiver = LtO = License to Operate. I denne sammenhæng de aktiver og/eller aktiviteter, som er afgørende for virksomhedens værdiskabelse og drift m.v.

Appendiks 7

Leverandørsikkerhed

Referencer:

- *Sikkerdigital.dk (https://www.digitalsikkerhed.dk/holdningspapir-om-styring-af-leverandoersikkerhed/)*
- *Center for Cybersikkerhed: (https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/Vejledning-cybersikkerhed-i-leverandorforhold_cfsc_digst-2022.pdf)*

Indledning

Alle virksomheder er afhængige af en lang række forskellige leverandører til deres it-systemer. Det omfatter bl.a.:

- **IT-udstyr**: F.eks. servere, PC'ere, telefoner, tablets, datalager og netværksudstyr;
- **Tjenester**: F.eks. databehandling, datafeeds og cloudservices (IaaS, PaaS og SaaS);
- **Software**: F.eks. standard kontorsoftware (Commercial-off-the-shelf/COTS) og specialudviklet software (bespoke); og
- **Forbindelser og kommunikation**: F.eks. internet, trådløst netværk og mobilnet (4G / 5G).

Sikkerhedsproblemer hos leverandørerne eller i leverandørernes produkter og services kan kompromittere dels virksomhedens egen cybersikkerhed, dels data opbevaret hos leverandøren eller virksomhedens adgang til services. Det skyldes bl.a. følgende forhold:

- IT-leverandører har ofte mange kunder, og er derfor selv et attraktivt mål for både cyberkriminelle og spioner;
- IT-leverandører kan blive kompromitteret af kriminelle, der skaffer sig adgang til den enkelte virksomhed eller mange virksomheder på en gang;
- IT-leverandørers hardware- og softwareprodukter kan indeholde sårbarheder eller udstyres med bagdøre; og
- Nogle gange har IT-leverandører ikke ordentligt styr på deres egen cybersikkerhed,

hvilket hver for sig og tilsammen kan ramme leverancerne af IT-leverandørernes services til kunder, eller de data der opbevares og behandles for kunder.

At have styr på virksomhedens IT-leverandører er derfor et væsentligt element i arbejdet med virksomhedens cybersikkerhed og forebyggelse af såkaldte "supply chain-angreb".

Vigtige IT-leverandører

Langt de fleste virksomheder anvender én eller flere af følgende typer vigtige IT-leverandører, som de sikkerhedsmæssigt (og regulatorisk) skal forholde sig til:

Outsourcing leverandører

Outsourcing betyder, at en virksomhed lader en ekstern IT-leverandør overtage it-opgaver (udvikling, vedligehold, support, drift, hosting m.v.), som virksomheden enten tidligere har stået for eller alternativt selv skulle stå for. Det er vigtigt at sikre, at outsourcingleverandørens håndtering (leverance) af sikkerhed lever op til virksomhedens krav. Indenfor den finansielle sektor er kravene til outsourcingleverandører lovfæstet.

Cloud leverandører

Udbyderne af cloudtjenester har etableret store driftscentre (datacentre), hvorfra de effektivt kan levere IT-kapacitet afregnet efter forbrug. I praksis handler sådanne cloudservices om, at kunder køber IT-kapacitet hos en udbyder - det kaldes også Infrastructure-as-a-Service (IaaS). Blandt de største og mest kendte leverandører af cloudservices er Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) og IBM Cloud. De store cloudleverandører har som udgangspunkt et højt sikkerhedsniveau, men ansvaret er typisk delt, så man som kunde er ansvarlig for (dele) af ens egen sikkerhed samt overholdelse af databeskyttelsesreglerne. Når man anvender cloudservices, er det vigtigt at forstå denne model og dermed virksomhedens eget ansvar. Indenfor den finansielle sektor er kravene til cloudleverandører lovfæstet. Overførsel af (person)data til cloududbydere har desuden selvstændige problemstillinger i relation til tredjelandsoverførsler, som virksomheden skal være opmærksom på .

Software-as-a-Service leverandører

Software-as-a-Service (SaaS) er, når en leverandør stiller en applikation (software) til rådighed som en service, mens data i applikationen opbevares eksternt som led i servicen. Typiske eksempler er Microsoft Office 365, Google Workplace eller målrettede systemer som SalesForce eller ServiceNow. Mange Software-as-a-Service leverandører er dermed også cloudleverandører og leverer driftsopgaver og udfører databehandling. Her er det ligeledes vigtigt at være opmærksom på, hvordan ansvaret er delt mellem leverandøren og virksomheden.

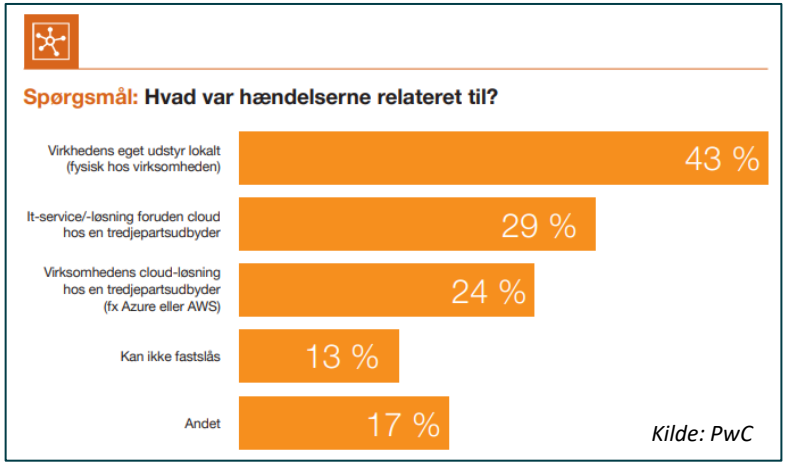
Bestyrelsens rolle

Bestyrelsen har det overordnede ansvar for sikkerheden i de IT-løsninger og IT-services, virksomheden anvender. Bestyrelsen skal være bevidst om, at sikkerhedshændelser hos virksomhedens leverandører kan have alvorlige konsekvenser for virksomheden selv, da virksomheden f.eks. selv kan kompromitteres, få driftsforstyrrelser og miste data, hvis en IT-leverandør udsættes for et cyberangreb.

Bestyrelsen bør derfor bl.a. tilse, at ***1)*** virksomhedens risikovurderinger også omfatter dens IT-leverandører, og ***2)*** der er truffet passende organisatoriske og tekniske foranstaltninger i relation til disse leverandører, herunder at virksomheden har en plan i tilfælde af nedbrud eller bortfald af en væsentlig IT-leverandør.

God sikkerhed hos IT-leverandøren stiller krav til virksomheden. Sikkerhedsansvaret ligger hos virksomheden. Det betyder bl.a., at selvom virksomheden har outsourcet driften af it-system til en leverandør, kan virksomheden reelt ikke outsource ansvaret herfor – hverken i relation til ledelsesansvar, regulatorisk ansvar, erstatningsansvar overfor kunder eller - i de fleste tilfælde – kommercielt (medmindre en økonomisk risikofordeling kan forhandles kontraktuelt på det private marked eller håndteres via forsikring).

Ifølge PwC Cybercrime Survey 2022 svarede hhv. 24 og 29 % af dem, der vidste, de havde været ramt af en sikkerhedshændelse, at den var relateret til en tredjepartsudbyder.



Ansvarsfordeling

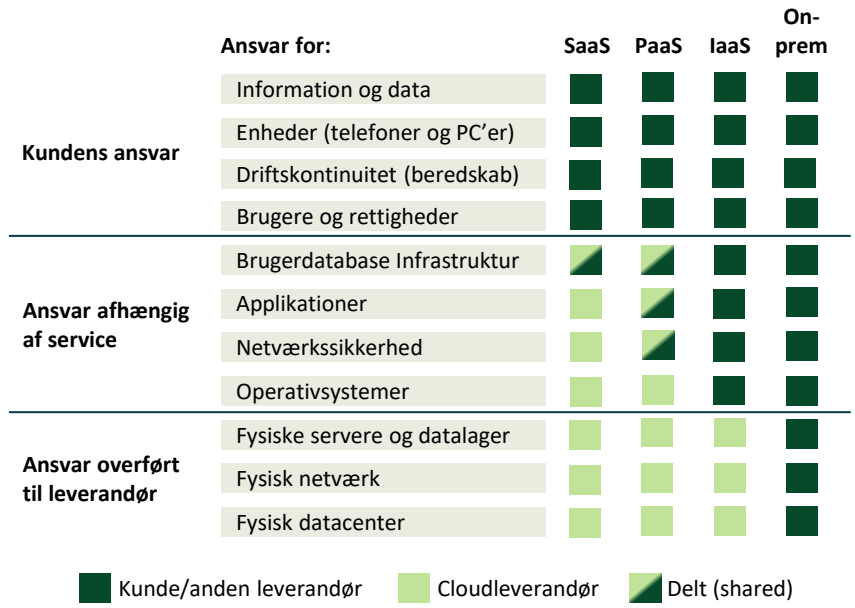
med fokus på cloud-løsninger

Uanset hvilken type it-leverandør eller -service, virksomheden benytter, skal den vide, hvordan ansvaret er delt mellem leverandøren og virksomheden.

I et (traditionelt) datacenter placeret fysisk hos virksomheden (kaldet "on-premise") har virksomheden ansvaret for alt fra den fysiske sikkerhed, som sikring mod indbrud og brand, til den fysiske/digitale sikring af stabil strømstrømforsyning, netværk, servere, operativsystemer, applikationer, brugerstyring m.v.

Særligt cloudleverandører arbejder med en model for delt ansvar (Shared Responsibility), hvilket betyder, at virksomheden selv har et ansvar for visse dele af sikkerheden uanset outsourcingen til cloud. Det er vigtigt, at disse grænser er kendte og veldefinerede, så der ikke er dele af sikkerheden, der ikke bliver taget ansvar for. Ansvarsfordelingen ændrer sig afhængigt af leverandør- og service set-up.

Nedenstående figur viser den generelle ansvarsfordeling ved forskellige typer af cloudløsninger. Det er vigtigt at bemærke, at virksomheden (ved brug af cloud-services) selv har ansvar for de brugere, der er oprettet, den data, der er placeret i løsningen, og sin egen driftskontinuitet (business continuity), medmindre andet er aftalt med enten cloudleverandøren eller en anden tredjepartsleverandør.



Due diligence

Forud for en beslutning om at indgå aftale med en IT-leverandør – det kan f.eks. være om køb af vigtige softwarelicenser, udvikling og vedligehold af væsentlige systemer, outsourcing af drift af forretningskritiske services, infrastruktur, hosting m.v. , bør virksomheden altid foretage en forudgående undersøgelse (due diligence) af leverandøren.

Dybden af undersøgelsespligten afhænger selvsagt af kompleksiteten og kritikaliteten af ydelsen. Sikkerhed og krav til sikkerhed bør dog altid være en del af den tekniske, operationelle, juridiske og kommercielle dialog og forhandling allerede ved anskaffelsen og aftaleindgåelsen. Ikke kun ud fra et ansvarsmæssigt perspektiv, men også fordi det ofte er dyrt og besværligt på bagkant at stille sikkerhedskrav, der ikke er en del af leverandørens standardydelse.

Sikkerhedskravene skal afspejle, hvor kritiske systemerne er for virksomheden (altså en risikovurdering). Ansvaret for sikkerheden kan ikke delegeres, og derfor bør virksomheden som led i sin due diligence som minimum stille følgende basisspørgsmål til sine IT-leverandører:

1. Hvad gør IT-leverandøren for at beskytte mod uønsket adgang?
2. Hvad gør IT-leverandøren for at sikre tilgængelighed og høj oppetid?
3. Hvad gør IT-leverandøren for at dokumentere egen sikkerhed?
4. Hvad gør IT-leverandøren for at passe på persondata (GDPR)?
5. Hvordan aftales den konkrete ansvarsfordeling mellem virksomheden og leverandøren?

Det er i praksis særdeles svært for især mindre virksomheder at få en reel dialog med de store, internationale IT- og cloudleverandører om sikkerheden i deres løsninger. Ofte er virksomheden derfor nødt til at forlade sig på en egen vurdering af sikkerheden og de certificeringer, som leverandøren standardmæssigt udleverer. Særligt de store cloudleverandører bruger dog betydelige ressourcer på sikkerhed, så i praksis burde sikkerhedsniveauet for cloudydelser fra større IT/cloudleverandører være ganske høj, således at sikkerhedsproblemerne typisk opstår på de områder, hvor virksomheden selv har ansvaret.

På sikkerdigital.dk findes et spørgeskema og en vejledning (kaldet ”Leverandørpakken”), der kan hjælpe de IT-, indkøbs- og kontraktansvarlige med at stille de vigtigste spørgsmål til IT-leverandører og gå i dialog med dem.

Generelle emner

som bestyrelsen bør føre kontrol med i relation til leverandørsikkerhed

1. **Overblik over it-aktiver og leverandører**: At virksomheden har et overblik over alle sine IT-leverandører og de løsninger og services, de hver især leverer til virksomheden. Overblikket bør dække data og forretningsprocesser håndteret af de enkelte leverandører (se også vejledningens Tema 1 (Risikovurdering). Uden dette er det svært at stille de relevante sikkerhedskrav.

2. **Drøftelse af konsekvenser ved hændelser**: At virksomheden har lavet en business impact analyse, BIA, der kortlægger, hvor afhængig kerneforretningen er af de forskellige IT-leverandører, og at sikkerhedskravene er tilsvarende høje, hvis konsekvenserne ved nedbrud / utilgængelighed som følge af et angreb er store.

3. **Ressourceforbrug og kompetencer**: At virksomheden forstår, hvilke krav sikker anvendelse af de leverede it-løsninger stiller til virksomheden. IT-løsninger, der installeres lokalt i virksomheden (on-premise løsninger) kan stille større krav til virksomhedens egen IT-sikkerhed og øvrige håndtering.

4. **Kontrakter og forpligtelser**: At virksomheden i aftaler med IT-leverandører har ***1)*** fastlagt en klar ansvars- og risikofordeling i forhold til de services og den tilgængelighed, leverandørerne er ansvarlige for at levere, ***2)*** fastlagt rapporteringskrav ved sårbarheder og evt. cyberangreb, og ***3)*** sikret opfyldelse af lovkrav (GPDR/tredjelandsoverførsler, outsourcingkrav for den finansielle sektor, NIS/NIS2-krav for omfattede sektorer m.v.).

5. **Certificeringer**: Om virksomheden stiller krav til, at dens IT-leverandører følger, eller er certificeret efter, en eller flere standarder eller rammeværk indenfor IT-sikkerhed (f.eks. ISO27001, ISAE3402 eller D-mærket), og om virksomheden bruger disse til kontrollere, at IT-leverandøren lever op til aftalte krav. Hvad er konsekvensen hvis leverandøren ikke lever op til kravene eller mister certificeringen?

6. **Samarbejde**: At virksomheden og leverandøren har aftalt rammerne for samarbejde, f.eks. omfang og frekvens for afholdelse af møder og hvilke ressourcer der er tilknyttet samarbejdet, samt har aftalt, hvordan ændringer i trusselsbilledet kommunikeres og behandles.

7. **Opfølgning**: At virksomheden minimum én gang om året følger op på, at IT-leverandørerne opfylder de aftalte sikkerhedskrav, og at disse krav er passende i forhold til en aktuel og opdateret risikovurdering.

8. **Overvågning**: At virksomheden overvåger sine IT-leverandører (i det omfang det er muligt), især i tilfælde hvor IT-leverandøren har adgang til virksomhedens øvrige IT-systemer.

Appendiks 8

Basal cyberhygiejne

(best practices IT-sikkerhed)

Indledning

Mange cyberangreb kan undgås – eller konsekvenserne af dem væsentlig mindskes - ved at gennemføre, implementere og vedligeholde en række relativt simple tekniske sikkerhedstiltag. Dette betegnes ofte som opretholdelse af en basal god cyberhygiejne.

Oversigten på de følgende sider i dette appendiks indeholder 12 sådanne "basal cyberhygiejne" sikkerhedstiltag, der anses for (en del af) best practices IT-sikkerhed.

Fælles for de oplistede tiltag er, at ***1)*** én eller flere af dem ofte ikke er på plads, når en organisation rammes af et succesfuldt cyberangeb, og 2) hvis de havde været på plads, kunne angrebet have været afværget eller skaden ved det være mindsket.

Listen er ikke en udtømmende liste over alle de (tekniske) sikkerhedstiltag, en virksomhed kan og bør gennemføre. Men virksomheden er kommet godt i gang, hvis tiltagene er eller bliver gennemført.

Basal cyberhygiejne

1	**Multi-faktor bruger-validering**	Anvend som minimum to-faktor brugervalidering på alle former for fjernadgang (VPN-løsninger, fjernskrivebord, Citrix m.v.) og på alle (væsentlige) cloud services, f.eks. Microsoft Office 365, Google Gmail m.v. Særlig fokus skal være på brugere med *administrative adgange* da disse adgange kan gøre stor skade, samt konsulenter og andre *eksterne brugere*, der også måtte have adgang og ofte glemmes ved implementering af to-faktor brugervalidering.
2	**Overblik over virksomheden "set udefra"**	Udarbejd og vedligehold et overblik over virksomheden IT-systemer, herunder hvordan virksomhedens IT-infrastruktur ser ud udefra (eksterne angrebsoverflade). Det kan eksempelvis gøres ved at få lavet en sårbarhedsscanning, så man får indblik i, hvad angribere "ser" udefra, når de scanner virksomheden. Overblikket er med til at forebygge risikoen for, at der ved en fejl er systemer eksponeret og tilgængelige, som virksomheden ikke kender til, har glemt eller overset (som f.eks. "Hafnium" og "Log4J" sårbarhederne viste). For alle systemer, der tilgængelige udefra, er det særligt vigtigt at holde dem opdateret samt holde øje med, hvad der sker på dem.
3	**Opdater programmer** *– fjern sårbarheder*	Opdater systemer og programmer hurtigst muligt, når der kommer opdateringer, så eventuelle sårbarheder fjernes, før de misbruges. Hav især fokus på systemer, som kan tilgås udefra (jf. også ovenfor #1 og #2) samt bl.a. webbrowsere, operativsystemer, firewalls og netværksudstyr.
4	**Opdateret og aktivt antimalware software**	Installer en moderne sikkerhedsløsning samt overvågning på alle systemer, enheder og online indgange, så der er en effektiv beskyttelse mod angreb. De fleste moderne operativsystemer har en glimrende antimalware løsning indbygget, som man skal sørge for er aktiv og opdateret.

Basal cyberhygiejne

5	**Backup**	Sørg for at have backup af alle virksomhedens forretningskritiske systemer og data, inklusive en offline kopi. Svigter al anden sikkerhed, er backup den sidste redning. Dette ved angriberne, og de går derfor målrettet efter at ødelægge backuppen. Derfor skal backuppen være offline og/eller særligt beskyttet. Husk test af backuppen, så man ved den virker, og hvor lang tid en genetablering tager. En backup, der ikke er testet, er ikke en backup. Gennemgå herudover beredskabsplanen og sørg for, at den fungerer efter hensigten, herunder indeholder en prioritering af indsatsen.
6	**Overvågning og alarmering**	For at opdage en hændelse eller kompromittering skal der kikkes efter den, og det kræver overvågning af systemer og netværk. Der bør derfor foretages systematisk opsamling og analyse af alle relevante sikkerhedsdata (logdata) fra infrastrukturen og systemer. Overvågningen kan bruges dels til at opdage hændelser i (nær) realtid, dels som et værktøj til at se, hvad der er sket, og dermed hurtigere komme tilbage i (normal) drift.
7	**Begræns og beskyt administrative adgang**	Mange angreb sker via udnyttelse af administrative adgange. Begræns derfor antallet af konti med administrative adgangen mest muligt, og beskyt de nødvendige administrative adgange med to-faktor validering (jf. #1), og/eller med særligt stærke passwords.
8	**Beskyt Windows Active Directory**	Windows Active Directory er en slags digitalt nøgleskab, og indeholder bl.a. information om alle brugere, passwords, systemer og adgange. Angriberne går målrettet efter kompromittering af Active Directory, da det giver dem fuld adgang til systemerne. Derfor er det vigtigt, at Active Directory er særligt beskyttet og overvåget.

Basal cyberhygiejne

9	**Segmenter netværket**	Segmentering af netværket sikrer, at en angriber ikke frit kan hoppe rundt mellem systemer på netværket. Samtidig giver segmentering bedre mulighed for at opdage et angreb, og hjælper med at inddæmme et eventuelt angreb.
10	**Beskyt produktions-miljøet**	Har virksomheden produktion eller teknisk udstyr koblet på netværket, er dette ofte mere sårbart end almindeligt it-udstyr, da det mangler sikkerhedskontroller, og ofte kun opdateres langsomt og besværligt. Derfor bør der etableres særlige sikkerhedsforanstaltninger til produktionsmiljøet f.eks. overvågning (jf. #6) og segmentering (jf. #9).
11	**Sikring af fjernarbejde og hjemmearbejde**	Når virksomhedens medarbejdere arbejder udenfor kontoret, bør det ske fra en enhed udleveret fra virksomheden under anvendelse af en krypteret forbindelse (f.eks. VPN) samt multi-faktor brugervalidering (jf. #1). Enheder der tages med udenfor kontoret skal desuden være krypteret således, at data er beskyttet såfremt enheden stjæles.
12	**Awareness træning**	Gennem oplysning om og uddannelse i basal cybersikkerhed spiller medarbejderne en afgørende rolle i et tilstrækkeligt sikkerhedsniveau. Awareness træning handler bl.a. om at informere medarbejderne om, hvad basal it-sikkerhed er, hvad de skal gøre ved tvivlsomme mails, samt give dem forståelse for og kendskab til, hvordan de skal forholde sig over for potentielle risici og hvis der sker et angreb.

Appendiks 9

Personlig cybersikkerhed for bestyrelsesmedlemmer

FOREBYGGE

1. **Kend og overhold virksomhedens it-sikkerhedspolitik**
   - IT-sikkerhedspolitikken kan f.eks. indeholde om, hvilke fildelingstjenester du kan bruge m.v.

2. **Skab overblik over data og systemadgange**
   - Hvordan opbevares dine og virksomhedens data?
   - Hvad er risikoen, hvis de mistes?

3. **Brug en dedikeret e-mailkonti til virksomhedskommunikation**
   - Hvis du bruger din egen, så benyt en anerkendt udbyder med spamfiltre og to-faktor login.

4. **Arbejd ikke som lokal administrator på din computer**
   - Hvis kun én bruger har administratorrollen på din private pc, bør du oprette en ny administrator-bruger, og ændre din nuværende til standardbruger.

5. **Brug stærke adgangskoder og genbrug ikke**
   - Brug mindst 12 tegn og kun ét sted. Brug gerne en veletableret og gennemprøvet passwordmanager. Hør evt. om virksomheden har en løsning.

6. **Benyt multi-faktor brugervalidering**
   - Slå altid multi-faktor-validering til. Se vejledning på www.sikkerdigtial.dk.

7. **Kontroller om du har været med i et læk af adgangskoder**
   - Tjek dette på f.eks. https://haveibeenpwned.com/ og https://haveibeenpwned.com/Passwords

8. **Tænk over hvad du deler på sociale medier**
   - Minimér privat information og tænk over om det, du deler, kan misbruges.

9. **Brug ikke fremmede USB-enheder eller opladere**
   - Brug kun dine egne USB-sticks og opladere - ellers anvend et kabel eller en 'USB Charge-Only Adapter'.

BESKYTTE

10. **Benyt et privacy-filter til din computer og tablet**
    - Gør det sværere for folk at se, hvad du har på din skærm, og du kan arbejde sikkert i offentligheden.

10. **Lås altid dine enheder**
    - Indstil dine enheder til automatisk skærmlås.

11. **Krypter dit indhold**
    - Du bør også gøre fjernsletning af data muligt.

13. **Benyt sikkerhedsprodukter med antivirus og firewall**
    - Din computer skal være sikret mod cyberangreb, f.eks. med en firewall og antivirus. Der findes også firewall og antivirus til telefoner og tablets. Læs mere: https://sikkerdigital.dk/borger/gode-raad/beskyt-dine-enheder-mod-virus/

14. **Opdater dit operativsystem og programmer regelmæssigt**
    - Opdater dine enheder efter, du har fået notifikation om, at de er tilgængelige.
    - Slet programmer, du ikke bruger.
    - Læs mere: https://sikkerdigital.dk/borger/gode-raad/opdater-dine-programmer/

15. **Beskyt dig med VPN på usikre netværk**
    - Hvis du ikke bruger VPN, skal du sikre, at følsom kommunikation er beskyttet med kryptering.

OPDAGE

16. **Sund skepsis og opmærksomhed**
    - Vær opmærksom på mistænkelige henvendelser.

17. **Vær opmærksom på atypiske hændelser på din computer eller mobiltelefon**
    - Ignorer ikke hvis f.eks. programmer åbner og lukker tilfældigt, din mus bevæger sig af sig selv mv. Reager straks. afbryd forbindelsen til internettet og kontakt en it-ekspert. Sluk ikke computeren.

18. **Underret virksomhedens it-afdeling hurtigst muligt**
    - Gem klokkeslæt og beskriv fejlen, så godt du kan, f.eks. Ved billeder af skærmen.

HÅNDTERE

19. **Hav en plan klar til når uheldet er ude**
    - Hav altid en plan klar for, hvem du skal kontakte, f.eks. en aftale med virksomhedens it-afdeling.

GENOPRETTE

20. **Tag sikkerhedskopier – både online og offline**
    - Husk sikkerhedskopier (backup) af dine data, f.eks. gennem en cloud-tjeneste eller eksternt harddisk.

Appendiks 10

Akut checkliste ved cyberhændelser

Indledning

Tabellen til højre viser et eksempel på en basis checkliste ved en cyberhændelse. Listen kan også bruges til gennemgang af virksomhedens krise- og kommunikations-plan i tilfælde af, at virksomheden rammes af en større cyberhændelse.

Det vigtigste arbejde sker ***før***, virksomheden bliver ramt, bl.a. ved etablering af en incident response plan (hændelseshåndtering), business continuity plan (driftskontinuitet), disaster recovery plan (genoprettelse) samt en krise- og kommunikationsplan, herunder sikring af backup og evt. indgåelse af aftaler med eksterne rådgivere, der kan yde professionel bistand i krisesituationer.

Er man blevet ramt af f.eks. et ransomwareangreb, og ønsker dialog med gerningsmændene, bør professionel hjælp til kommunikation overvejes. En sådan kommunikation er i langt de fleste tilfælde forsvarlig og fornuftig, da den tjener flere formål:

- ***dels*** at købe vigtig tid til de tekniske undersøgelser (omfang af skaden, hvordan bruddet opstod, identifikation af sårbarheder og ramte systemer, "oprensning" af de ramte områder, undersøgelser om backup virker (fuldt ud) identifikation af områder der skal styrkes sikkerhedsmæssigt m.v.);

- ***dels*** at (forsøge at) opnå vigtig information fra gerningsmændene, f.eks. om hvordan bruddet blev opdaget/udnyttet og – i det omfang gerningsmændene truer med at lække data (hvad ofte er tilfældet) – at trække tiden mest muligt med henblik på at undgå datalæk (så længe der "forhandles", reduceres risikoen for offentliggørelse) og samtidig prøve at finde ud af, hvor meget og hvilke typer data, gerningsmændene er i besiddelse af; og

- ***dels*** at forhandle kravet om løsesum ned således, at beløbet er lavest muligt i det tilfælde, at betaling af løsesum måtte blive et nødvendigt scenarie.

Betaling af løsesum bør være sidste udvej, hvis data ikke kan reetableres på anden måde og/eller hvis hensynet til at undgå datalæk vejer tungere end løsesumsbetaling. Vær opmærksom på, at reetableringsarbejdet generelt er det samme, uanset om data frigives via betaling af løsesum eller ved genetablering fra backup.

Efter en kritisk hændelse kommer ofte en lang proces med at sikre, at angrebet er ordentlig elimineret, systemer er genetableret (ofte fra backup), og alle sårbarheder er udbedret. For mange virksomheder går der flere måneder, inden de er tilbage i normal drift.

Akut checkliste
ved cyberhændelser

1. **Undgå panik og bevar roen.**
   - ❑ Betal ikke de kriminelle i panik.

2. **Få overblik over problemet.**
   - ❑ Bed om en root cause analyse.

3. **Begræns den akutte skade.**
   - ❑ Isoler hændelsen hvis muligt.
   - ❑ Afbryd forbindelsen til internettet.
   - ❑ Afbryd forbindelsen til netværket.
   - ❑ Sluk ikke for computerne.
   - ❑ Skift passwords.
   - ❑ Kontakt bank og advokat (ved økonomisk svindel).

4. **Brug Incident Response- og kriseplanen.**
   - ❑ Processen for hændelseshåndtering ligger typisk hos systemejerne.

5. **Få kvalificeret ekstern hjælp.**
   - ❑ Fra bl.a. krise-, kommunikations- og sikkerhedseksperter, jurister og leverandører.

6. **Prioritér indsatsen.**
   - ❑ Hvad er der sket og hvad er ramt?
   - ❑ Hvad er konsekvensen for forretningen?
   - ❑ Implementer en plan for forretnings kontinuitet
   - ❑ Er der kompromitteret persondata?
   - ❑ Fokus: Er der (stadig) en backup, der virker?

7. **Kommunikér klart og løbende**
   - ❑ Intern underretning til ledelse og medarbejdere.
   - ❑ Ekstern kommunikation til samarbejdspartnere og presse.

8. **Foretag nødvendige anmeldelser**
   - ❑ Anmeldelse til Datatilsynet indenfor 72 timer (persondata)
   - ❑ Anmeldelse til relevante tilsynsmyndigheder (særlig i kritiske sektorer)
   - ❑ Notifikation til evt. forsikringsselskab
   - ❑ Politianmeldelse

9. **Husk dokumentation af forløbet**
   - ❑ Hændelseslog til dokumentation af forløb og beslutningsgrundlag (skal ofte også bruges overfor datatilsyn, andre tilsynsmyndigheder, forsikringsselskab, kunder m.v.)

10. **Sørg for bevissikring**
    - ❑ Få kvalificeret ekstern hjælp til bevissikring (ofte teknisk).
    - ❑ Pas på ikke at ødelægge beviser.
    - ❑ Kopi af inficerede maskiner til efterforskning.
    - ❑ Sikring af logfiler.

11. **Følg op på udbedringsplan**
    - ❑ Etablering af overvågning og evt. sikkerhedskontroller, så yderligere forsøg på kompromittering opdages og undgås fremadrettet.

Appendiks 11

Geopolitiske overvejelser

Indledning

Sikkerhedspolitik, og hvordan virksomheder skal håndtere en ny geopolitisk virkelighed, er rykket højt på agenden efter Corona-pandemien og ikke mindst Ruslands angrebskrig mod Ukraine.

Det internationale system, der har eksisteret siden afslutningen af den kolde krig, er i opbrud, og fremtiden byder på en mere fragmenteret verdensorden præget af stormagtsrivalisering med en militær og civil konkurrence på områder som økonomi, energi, teknologi og innovation. Dette medfører bl.a. en revurdering af komplekse forsyningskæder, teknologioverførsel og globalisering.

Mange af fremtidens konflikter vil formentlig ikke være i form af trusler mod Vesten om direkte åben militær konfrontation men foregå i en gråzone med anvendelse af hybride trusler, som dækker over meget varierede ikke-militære sikkerhedspolitiske virkemidler som f.eks. irregulære militære styrker (”små grønne mænd”), desinformation via sociale medier, manipulation af den demokratiske samtale, påvirkning af valghandlinger, reel sabotage, økonomiske foranstaltninger f.eks. bestikkelse og cyberangreb.

Samtidig må det forventes at stater i stigende omfang anvender spionage rettet mod både myndigheder og virksomheder bl.a. for at imødegå konsekvenserne af sanktioner på teknologioverførsler

Særlige opmærksomhedspunkter

I Danmark har Maersk allerede oplevet, hvor fatale konsekvenserne af denne udvikling kan være, da de i 2017 blev ramt af et destruktivt russisk cyberangreb (NotPetya), der lammede alle deres it-systemer i flere uger og medførte omkostninger på DKK 1,5 mia. Cyberangrebet var egentlig rettet mod Ukraine, men spredte sig også i it-systemerne hos Maersk da deres lokale kontor i Ukraine blev ramt.

Nogle af de områder man som virksomhed er nødt til at være opmærksom på, omfatter bl.a.:

- Risikoen for **spionage** fra fremmede stater, f.eks. i forhold til teknologi, forretning eller medarbejdere;
- Udvidet råderum for **cyberkriminelle** der i praksis kan operere uhindret og ofte kan være i ledtog med myndigheder og efterretningstjenester f.eks. i Rusland;
- Risikoen for kompromittering af virksomhedens **supply chain** såfremt der anvendes produkter eller løsninger fra fjendtligt indstillede lande, eller hvis nogen af virksomhedens leverandører kompromitteres af et angreb;
- Risikoen for **destruktive angreb** mod virksomheden – enten direkte eller som ”følgeskade” ved angreb på f.eks. virksomhedens samarbejdspartnere; og
- Risikoen for **påvirkningsangreb** f.eks. via sociale medier. Sådanne angreb er ofte samfundsrettede, men ofte sker der inddragelse af virksomheder eller virksomheders ”brand” i sådanne kampagner.

For virksomheder betyder denne udvikling, at de er nødt til at inddrage disse mulige direkte og indirekte trusler relateret til den geopolitiske situation i virksomhedens risikovurderinger og beredskab.

Appendiks 12

Ordliste
(udvalgte begreber)

Eksempler på udvalgte ord og begreber inden for cybersikkerhed

Active Directory (AD): Er den centrale bruger- og rettighedsdatabase i et Windows netværk der bl.a. indeholder informationer om computere, ressourcer, brugere og password og godkender login til systemerne. Ved et angreb vil hackerne gå målrettet efter at få administrator rettigheder til Active Directory (AD). Derfor er det vigtigt at overvåge.

Botnet: Et botnet er et netværk af kompromitterede computere, der styres af en tredjepart. Et botnet bliver skabt ved, at computere med internetadgang bliver inficeret med malware, hvorefter den, der kontrollerer botnettet, kan anvende det til f.eks. at udføre DDoS-angreb, phishing-angreb (spam), distribuere malware, mine bitcoins osv.

CEO fraud: "Direktørbedrageri" der går ud på at franarre en virksomhed oplysninger eller udbetale penge ved at udgive sig som direktør af virksomheden. Anvender ofte (spear)phishing-teknikker (f.eks. e-mail) og social engineering.

DDoS-angreb: Står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere (et botnet) til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

Drive-by exploits: Et udtryk for, at den ramte virksomhed ikke var målet for kampagnen, men blot blev ramt ved et hændeligt uheld.

Logs: De informationer som IT-systemer kan konfigureres til at opsamle om forskellige former for aktiviteter, herunder sikkerhedshændelser. Som udgangspunkt gemmes logs lokalt på systemet, hvilket er problematisk da en angriber som det første vil søge at slette loggen for at skjule deres spor.

Log-management system: En centraliseret teknisk løsning som opsamler og sikre logs fra mange forskellige IT-systemer. Virksomheden kan enten selv have et log-management system eller købe det som en service der leveres via Internettet.

Malware: Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting der, hvor de er installeret. Begrebet dækker over alle kategorier af skadelige programmer herunder virus og orme som f.eks. spyware, ransomware, botnets og trojanske heste. Antivirusprogrammer bekæmper som oftest ikke kun vira, men flere forskellige typer malware.

Man-in-the-middle: Angreb, hvor en skadelig enhed eller person placerer sig mellem to enheder, eksempelvis mellem brugeren og routeren. Dermed får mellemmanden adgang til al data, brugeren afsender.

Mass interception: Massiv overvågning af tele- og internetaktivitet, eksempelvis gennem logning af internetsessioner. Udføres af stater, men kan også ved hjælp af en ekstensive netværk af overvågningsprogrammer bruges af it-kriminelle til at indhente enorme mængder data om adfærd.

MSSP: En forkortelse for en Managed Security Service Provider, der er er en leverandør af sikkerhedsservices, typisk leveret over Internettet. I forbindelse med logning og overvågning vil en MSSP kunne levere en Managed SIEM og SOC-løsning, samt hjælpe med at reagere på hændelser.

Phishing/spear phishing: Phishing er forsøg på via social engineering at manipulere en person til i god tro at videregive personlige oplysninger eller klikke på inficerede filer eller links til falske hjemmesider. Phishing-mails sendes ofte bredt ud til mange modtagere. Spear phishing adskiller sig særligt ved at være målrettet den enkelte modtager og anvende teknikker fra social engineering. E-mails er typisk udformet, så de virker særligt relevante, overbeisende og troværdige for modtageren ved f.eks. at anvende navn, personspecifikke informationer eller relevante filer, der er opdaget ved forudgående rekognoscering.

Ransomware: Ved et ransomware-angreb bliver data og systemer på offerets computer holdt som gidsel, da de krypteres og derved bliver utilgængelige. Den ansvarelige bag angrebet kræver en løsesum typisk i form af kryptovaluta (f.eks. Bitcoin), for at give adgang til data igen. Som regel vil den ansvarlige bag angrebet installere malware ved hjælp af phishingmails. De fleste ransomware-angreb lykkes, fordi brugeren snydes til at klikke på et link eller en vedhæftet fil i en e-mail, men ransomware-angreb kan også ske via sms eller et reklamebanner på en hjemmeside. Der findes mange varianter af ransomware. Målrettede ransomwareangreb forsøger at ramme f.eks. administrative netværk i specifikke virksomheder og myndigheder.

SIEM: En forkortelse for et "Security Information and Event Management" system, der er en teknisk løsning, som udover opsamling af logs også sammenholder og analyserer logdata og sende alarmer ved mistænkelige aktiviteter. Virksomheden kan enten selv have en SIEM løsning eller købe det som en service der leveres via Internettet. Når et SIEM-system finder mistænkelige aktiviteter i logdata, bliver der genereret en alarm som derefter skal kvalificeres og analyseres dvs. det skal undersøges hvorvidt der er tale om en sikkerhedshændelse eller en falsk alarm.

SOC: En forkortelse for "Security Operation Center", der er en centraliseret funktion eller organisation der ved hjælp af mennesker, processer og teknologi overvåger og reagerer på sikkerhedshændelser. Dette kan bl.a. ske ved at overvåge og analyserer alarmer fra et SIEM systemer. Denne funktion kendes også under navne som Security Analytics Center (SAC) og Cyber Defense Center (CDC).

Social engineering: Et udtryk for, at man udnytter sociale interaktioner og psykiske kneb til at narre en person eller en virksomhed til at udlevere informationer, give adgang til systemer eller overføre penge til dem.

SQL injection: Angreb rettet mod databaselaget i software, som udnytter en sårbarhed i håndtering af input og databasekald. Databasekaldet manipuleres gennem inputtet (typisk ved brug af specialtegn) til at opnå en anden effekt end den tilsigtede - for eksempel at afsløre, hvem der har administratorrettigheder.

Se flere ordforklaringer på CFCS' hjemmeside: Ordforklaringer af begreber i cybersikkerhed (cfcs.dk)

BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance