Cybersikkerhed for bestyrelse og direktion

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

Bestyrelsesforeningens Center for Cyberkompetencer

KROMANN REUMERT

Dubex:

INDUSTRIENS FOND

CENTER FOR CYBERSIKKERHED

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 informations-sikkerhed (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 persondataområdet har cybersikkerhed været sparsomt reguleret indtil nu. NIS1 og dets tilhørende sektorvise danske regler er rettet mod nationale myndigheder og kritisk infrastruktur. Den finansielle sektor er endvidere 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.

I december 2022 blev et nyt NIS-direktiv (**NIS2**) vedtaget i EU. NIS2 træder i kraft i dansk ret den 18. oktober 2024. En lang række virksomheder indenfor ca. 18 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 kommende regulering (udover NIS2) bl.a.:

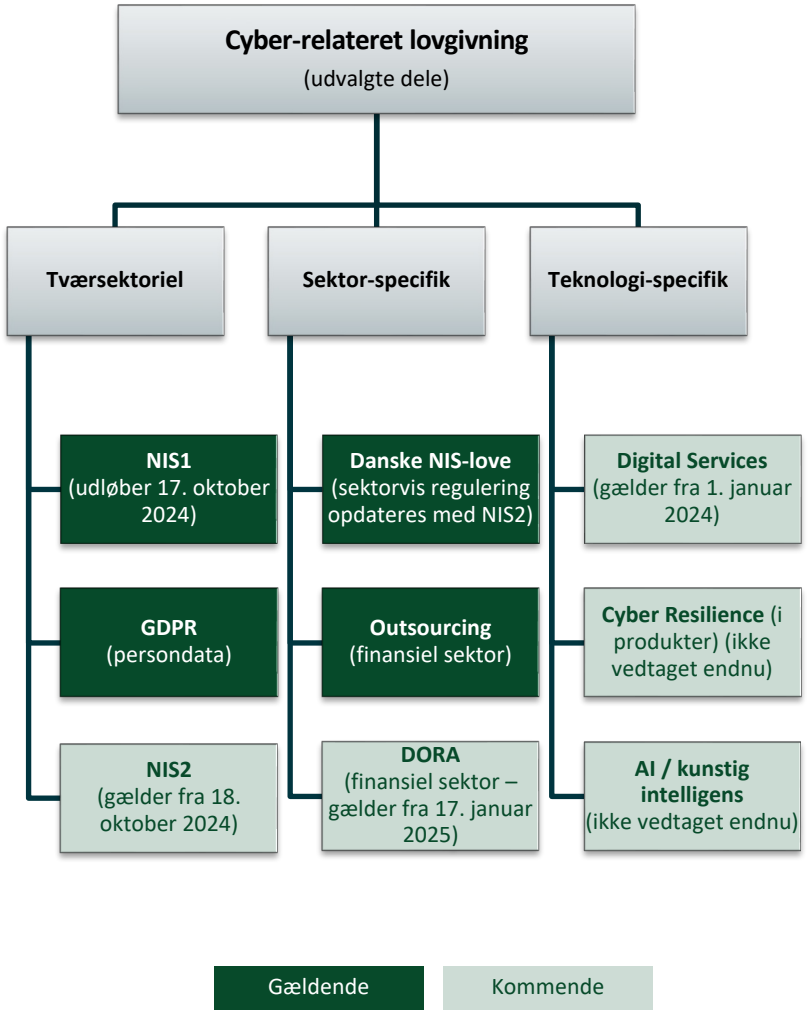
- **DORA-forordningen** om digital operationel modstandsdygtighed i den finansielle sektor.

Indenfor konkrete digitale teknologier omfatter kommende regulering bl.a.:

- **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 cybersikkerhed først og fremmest baseret på et civilretligt ansvar, hvorefter en direktør eller et bestyrelsesmedlem kan ifalde erstatningsansvar, hvis personen har handlet uagtsomt, f.eks. et bestyrelsesmedlems 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, selvom beslutningen senere viser sig at være forkert eller ugunstig, medmindre der er tale om et alvorligt fejlskøn.

Business judgment rule
eksempler indenfor cybersikkerhed

Det er overordnet bestyrelsens ansvar at sikre, at der er etableret fornødne procedurer for risikostyring og interne kontroller (selskabslovens § 115), og det er overordnet direktionens ansvar at varetage den daglige ledelse og følge de retningslinjer og anvisninger, som bestyrelsen har givet (selskabsloven § 117).

Det er som minimum en ledelsesopgave:

- at direktionen udarbejder en **strategi** for cybersikkerhed, som bestyrelsen forholder sig til og godkender;
- at direktionen udarbejder en **risikovurdering,** der tager højde for bl.a. eksponering, størrelse, sandsynlighed og konsekvens, som bestyrelsen forholder sig til;
- at bestyrelsen fastlægger **risikoappetitten** indenfor cybersikkerhed baseret på den valgte strategi og konkrete risikovurdering (evt. ud fra et oplæg fra direktionen);
- at direktion og bestyrelse godkender **sikkerhedsforanstaltningerne** (organisatoriske, tekniske, operationelle mv.) i lyset af den konkrete risikovurdering. Bestyrelsen bør i hvert fald forholde sig til de væsentlige/best practices foranstaltninger;
- at sikre, at foranstaltningerne opfylder minimumskrav i **lovgivning**, som virksomheden er omfattet af;
- at direktion og bestyrelse sikrer sig en tilstrækkelig **rapportering** fra hhv. organisation og direktion; og
- at direktion og bestyrelse løbende fører **tilsyn** med strategiens gennemførelse.

Det er derimod et vidt forretningsmæssigt skøn:

- *hvordan* strategien nærmere skal se ud (se Appendiks 3 til inspiration);
- *hvor omfattende* risikovurderingen skal være (se Tema 1 til inspiration);
- *hvor meget* risiko virksomheden er villig til at tage (se Tema 2 til inspiration);
- *hvilke* sikkerhedsforanstaltninger der konkret skal anvendes (når lovens minimumskrav er opfyldt) (se Tema 3 og Appendiks 8 til inspiration);
- *hvordan* risikostyringsarbejdet skal tilrettelægges (se Tema 6 til inspiration); og
- *hvilke* kontroller der skal måles på (se Tema 4 til inspiration),

– 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.

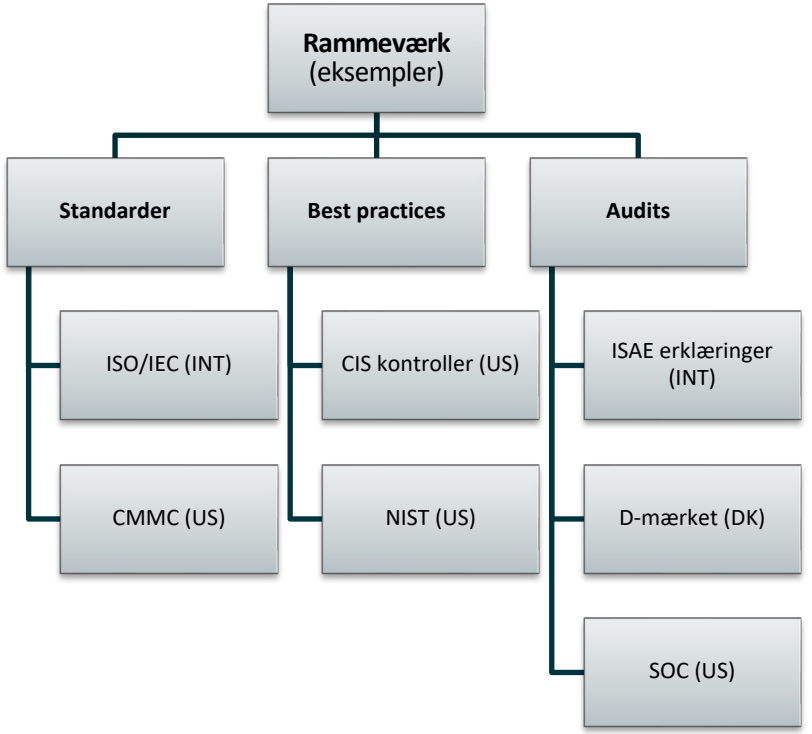
Der findes efterhånden en del rammeværk inden for cybersikkerhed. Formålet med dette appendiks er at give et overblik over nogle af de mest udbredte og anerkendte rammeværk i Danmark og internationalt.

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 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 vælge, 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 oprindelig 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 (CSF), ofte blot betegnet NIST CSF, 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 har ansvaret for den overordnede forretningsstrategi, herunder hvordan denne realiseres gennem en digital strategi. Formålet med en cybersikkerhedsstrategi er både at beskytte forretningen og at understøtte den digitale strategi, der skal bruges til at realisere forretningsstrategien.

Som beskrevet i vejledningen (side 16-19), 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 direktionens 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 direktionens 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 bruger? 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 til bestyrelsen. 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 eller 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 (Note 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.

(Note 1) Den "acceptable risiko" omtales også ofte som "risikoappetitten". Den udtrykker den risiko, 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 = bestyrelse, direktion, forretning og kontrolfunktioner.
- Skal sammenholdes med virksomhedens strategi 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 afhængig 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, forretningsmodel, samlede risikoprofil og risikoappetit.

8. Investeringsbehov

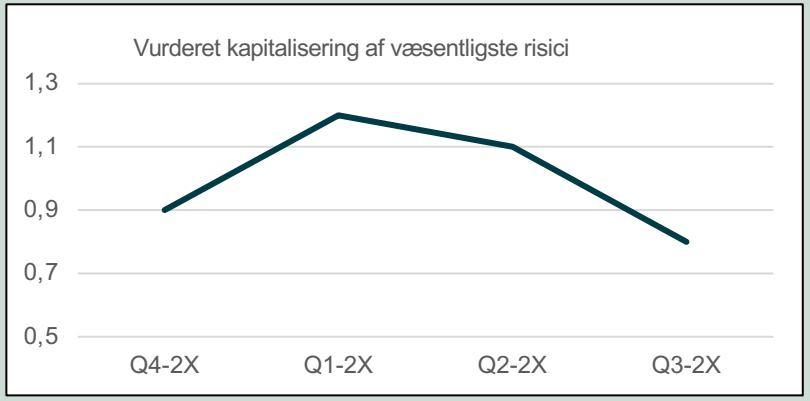
- Anbefalingen af den tilhørende investeringsramme med henblik på at opnå en tilfredsstillende ramme for risikoappetitten/accepten.

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.

Bilag 1: "Siden sidst"

DRAFT

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*
…			

Bestyrelsesforeningens Center for Cyberkompetencer

* Farven angives af den risiko, der har det højest vurderet restrisikoniveau, og er derfor ikke en gennemsnitsvurdering af alle angivne risici

INDUSTRIENS FOND

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.

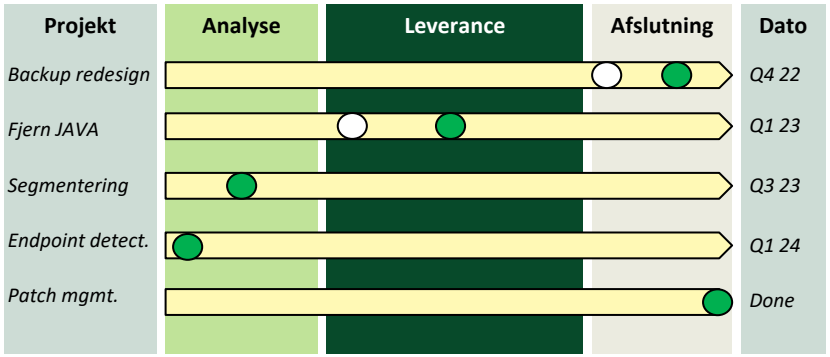
Rapporten vil kunne afsløre en eventuel stigende eksponering samlet set og – væsentligt - skærpe underleverandører og outsourcingpartneres fokus på deres cybersikkerhed. Det er naturligvis afhængigt af relationens størrelse og kritikalitet samt eventuelle lovgivningskrav (f.eks. indenfor den finansielle 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

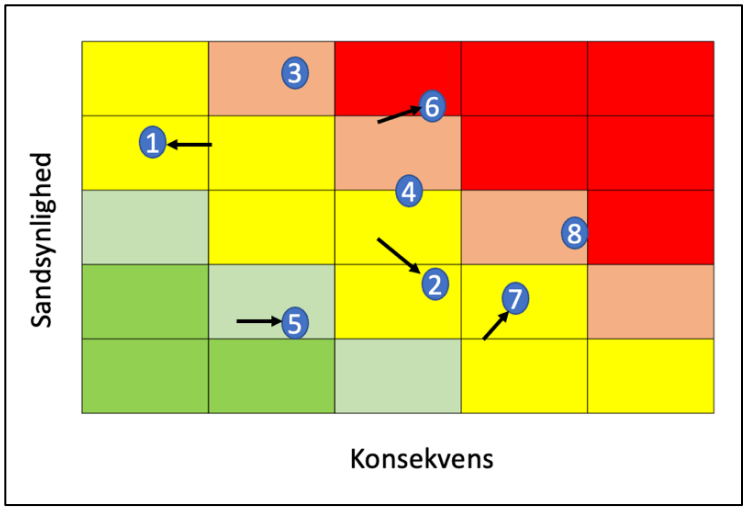
Risici mappes til forretningssystemer, og forretningssystemernes "helbredstilstand" kan måles ud fra CIS-kontrollerne, således at svagheder kan prioriteres efter hvor kritisk systemet er for virksomheden og hvilke risici, det er relateret til.

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

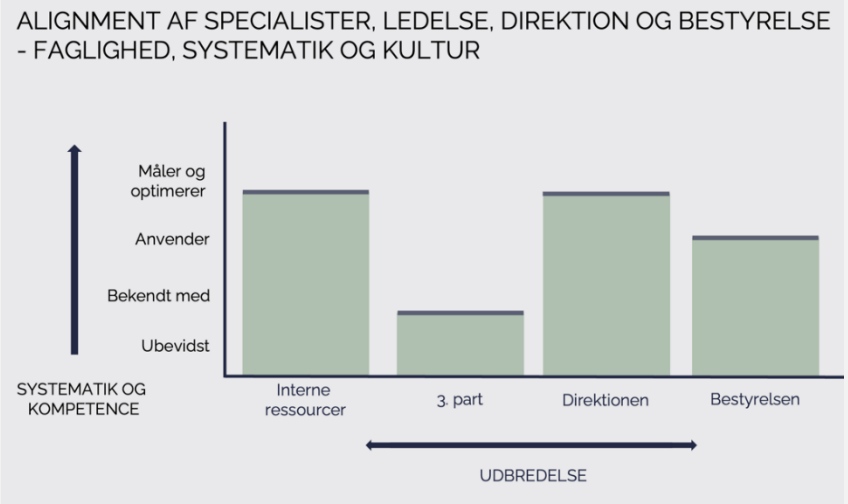
Arbejdet med cybersikkerheds problemstillinger bør inkludere identifikation af de væsentligste virksomhedsrelevante risici og deres potentielle konsekvenser samt en vurdering af sandsynligheden for, at disse risici materialiserer sig.

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.

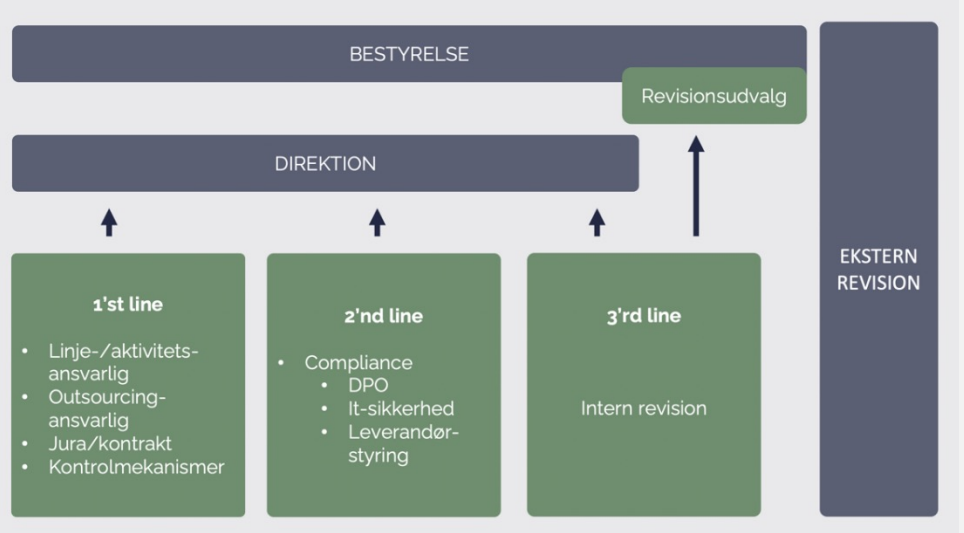


9. Status personale, medarbejdere og organisering

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.

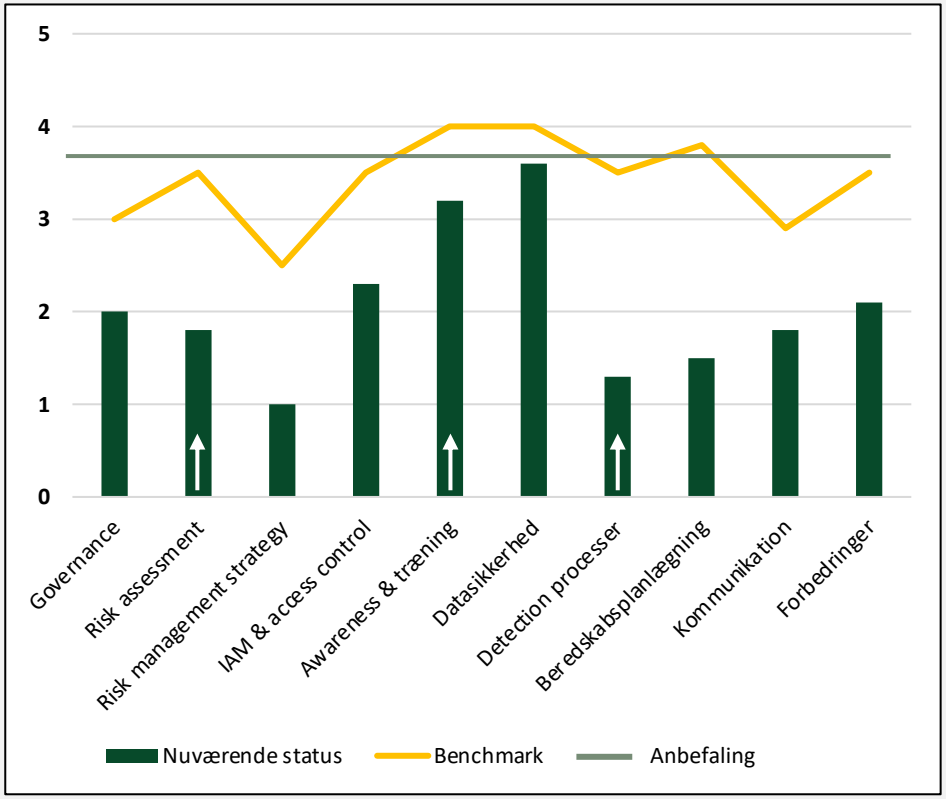


10. Status på sikkerheds-kategorier generelt (NIST)

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).

Der er pt. ikke politisk vilje til at stille krav om cyberforsikringer 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 forretningsmæssigt 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	Tredjeparts tab og omkostninger
Incident / Beredskab (egne)	Erhvervsansvarsforsikring (tredjeparts)
Retablering af data (egne)	Datasikkerhed (privacy) (tredjeparts)
Driftsforstyrrelser / driftstab (egne / afledt)	Bøder, sanktioner, advokat mv. (tredjeparts)
Løsepenge (egne)	IPR krav (tredjeparts)
Bøder, sanktioner, advokat mv. (egne)	Netværksbrud / datatab (tredjeparts)
Økonomisk kriminalitet (egne)	
Omdømmetab (eget)	
Identitetstyveri (eget)	

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.

Disse sikkerhedsproblemer kan hver for sig og tilsammen 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 indebærer 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.

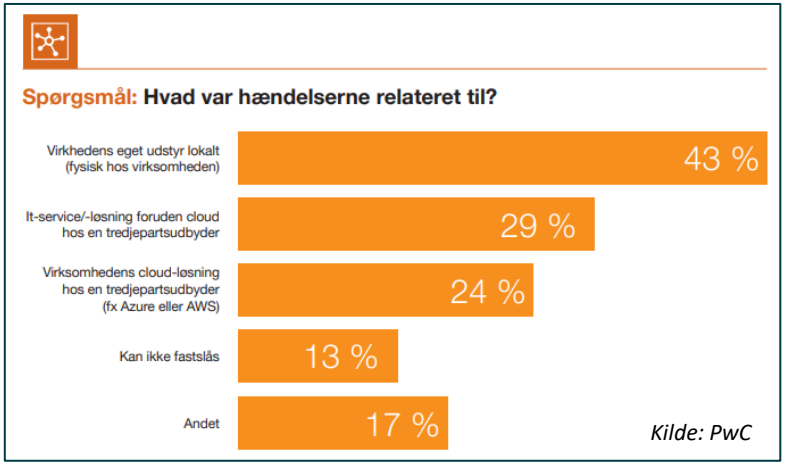
Bestyrelsens rolle

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. sikre, at ***1)*** virksomhedens risikovurderinger også omfatter dens IT-leverandører, og at ***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 eller kommerciel risiko (medmindre en økonomisk risikoallokering kan forhandles kontraktuelt 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

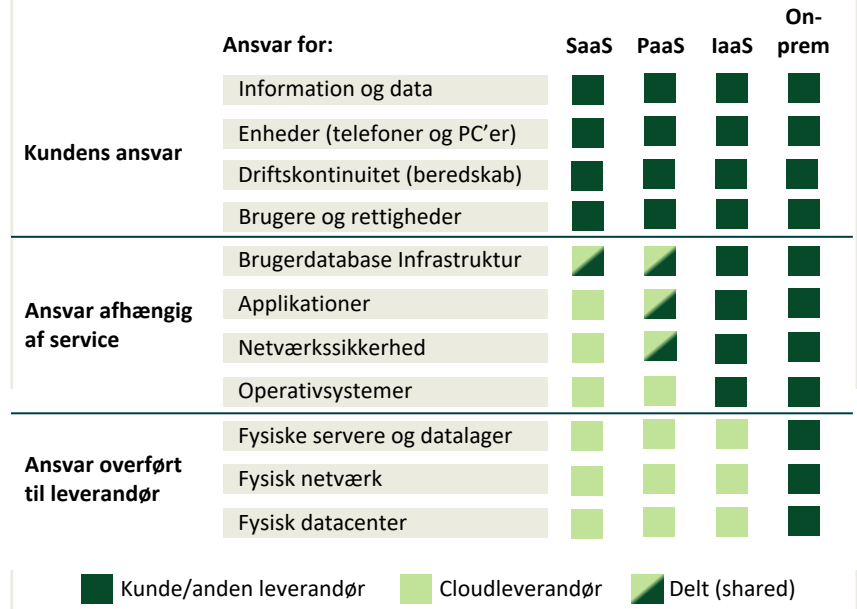
med fokus på cloud-løsninger

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-premises") har virksomheden ansvaret for alt fra den fysiske sikkerhed, som sikring mod indbrud og brand, til den fysiske/digitale sikring af stabil strømforsyning, 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 afhængig 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 højt, 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 at 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 mindskes væsentligt - 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 cyberangreb, 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 virksomhedens 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, der er eksponeret og tilgængelige, som virksomheden ikke kender til, har glemt eller overset (som f.eks. "Hafnium" og "Log4J" sårbarhederne viste). For alle systemer, der er tilgængelige udefra, er det særlig 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 adgange**	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 information 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, så 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 cybersikkerheds-hændelse. Listen kan også bruges til gennemgang af virksomhedens krise- og kommunikations-plan i tilfælde af, at virksomheden rammes af en større hændelse.

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 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, advokater 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 (teknisk og juridisk).
    - ❑ 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 normalt 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 sit spor.

Log-management system: En centraliseret teknisk løsning som opsamler og sikrer 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, overbevisende 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 ansvarlige 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 phishing-mails. 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 ransomware angreb 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