December 2020

CYBERSIKKERHED FOR BESTYRELSER

Anbefalinger til Styrkelse af Cyberkompetencer

BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance
Bestyrelsesforeningens Center for Cyberkompetencer

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

INDHOLD

KONTAKT

Bestyrelsesforeningens Center for Cyberkompetencer

Tom Jacobsgaard
Direktør
Mail: tj@bestyrelsesforeningen.dk

Marianne Philip
Bestyrelsesformand
Mail: mp@kromannreumert.com

Jørgen Bardenfleth
Formand for Advisory Board
Mail: joergen@bardenfleth.dk

Kirsten Hede
Projektdirektør
Mail: khe@bestyrelsesforeningen.dk

1. Indledning

Disse anbefalinger er udarbejdet som led i projektet "*Styrkelse af strategiske cyberkompetencer i danske virksomheder*", der har til formål at øge opmærksomheden over for cyberrisici og at styrke kompetencerne inden for cybersikkerhed i danske bestyrelser og direktioner, herunder bestyrelser og direktioner i små- og mellemstore virksomheder.

Projektet er støttet af Industriens Fond, og er en del af Industriens Fonds indsats indenfor cybersikkerhed.

Projektet udføres af Bestyrelsesforeningens Center for Cyberkompetencer i samarbejde med en partnerkreds bestående af CBS, AAU, CBS-Bestyrelsesuddannelserne, CFCS, World Economic Forum, Beierholm, BDO, EY, KPMG, PwC, Danish Cyber Defence, Dubex, Improsec, IBM, Jyske Bank, Nordea og Kromann Reumert.

Det er Bestyrelsesforeningens mål, at partnerkredsen løbende opdateres og kommer til at omfatte alle væsentlige rådgivere til bestyrelser, herunder bestyrelser i små- og mellemstore virksomheder.

Denne vejledning blev første gang udgivet i december 2019, og er senest opdateret i november 2020.

2. Cyberkompetencer i danske bestyrelser

I kernen af enhver forretningsmæssig beslutning er styring og afvejning af risici. Jo mere digitale virksomheders produkter og infrastruktur er, jo mere sårbare er de over for cyberangreb. Cyberangreb er blandt de største forretningsrisici, virksomheder står overfor, og koster danske virksomheder på bundlinje, kundeforhold og renommé. Det er derfor vigtigt at stille skarpt på cyber- og informationssikkerhed i bestyrelseslokalet.

Bestyrelser har brug for kompetencer indenfor cyber- og informationssikkerhed. Ikke kun for at håndtere risici men også for at gøre sikkerhed til en konkurrencefordel og en facilitator for virksomhedens produktudvikling og forretningsmodel.

Det er bestyrelsens opgave og ansvar at føre effektiv kontrol med virksomhedens risici – blandt andet for at beskytte og skabe afkast af den forretning, som bestyrelsen er sat til at varetage på vegne af ejerne.

Mange bestyrelser mangler dog tilstrækkelig viden og kompetencer til at kunne adressere virksomhedens risici på cyberområdet.

Risikostyring går ud på at forstå, identificere, analysere, prioritere og håndtere risiko. Alle risici kan ikke fjernes helt. Men ved at anvende en systematisk tilgang kan bestyrelsen og ledelsen tage de rigtige risici på et oplyst grundlag.

Formålet med disse anbefalinger er at klæde bestyrelsesmedlemmer på til arbejdet med en cyberstrategi og at give dem værktøjer til at sparre med og udfordre direktionen om virksomhedens cyber- og informationssikkerhed.

For at leve op til sit ansvar og træffe beslutninger på et oplyst grundlag bør det enkelte bestyrelsesmedlem derfor stille sig selv det grundlæggende spørgsmål: *"**Forstår jeg virksomhedens cyberrisici, og har vi en cyberstrategi?**"*

3. Kort om metoder, sårbarheder og risiko

Cyberangreb er drevet af forskellige motiver og metoder. Nogle har til formål at stjæle data, andre skal afpresse penge. Nogle angreb er simple, andre er avancerede. Angreb kan komme fra f.eks. kriminelle, stater, insidere og konkurrenter, og de kan være målrettede eller tilfældige. Den enkelte virksomheds risiko afhænger af en konkret vurdering.

Cyberangreb dækker over, at en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Angreb kan være målrettede eller tilfældige.

Angrebsaktører er f.eks. cyberkriminelle, stater, insidere og konkurrenter. Deres motiver varierer bl.a. fra økonomisk vinding til spionage og ødelæggelse af forretning.

Metoder omfatter forskellige værktøjer og teknikker, der udnytter sårbarheder (fejl/svagheder) i computersystemer, særligt software (engelsk: *vulnerabilities*).

Nogle almindelige angrebsmetoder er beskrevet til højre (*malware*, *phishing* og *DoS/DDoS*).

Truslen opstår ved, at en aktør har en relevant metode, der kan udnytte en sårbarhed (dansk: en *udnyttelig sårbarhed* / engelsk: *exploitable vulnerability*). Dette kaldes også en trussel.

Når en trussel udnytter en sårbarhed, medfører det en **hændelse** (engelsk: *incident*). En hændelse kan skyldes simple menneskelige fejl, og kan have mere eller mindre kritiske konsekvenser alt efter, hvor alvorlig den er.

Risikoen er udtryk for *usikkerheden* for og *konsekvenserne* ved en hændelse set i forhold til *sandsynligheden* for, at hændelsen indtræffer.

Risikovurderingen er den systematiske proces, hvor virksomheden identificerer sine *aktiver*, og vurderer den konkrete *risiko* i forhold til dem.

Almindelige angrebsmetoder

Malware

Malware står for *malicious software* og er en betegnelse for ondsindet programkode, der gør skadelige eller uønskede ting, f.eks. stjæle adgangskoder eller inficere et computernetværk. De fleste cyberangreb involverer én eller anden form for malware. Malware-former tager typisk navn efter det, de er programmeret til, f.eks. *virus*, *orme*, *ransomware*, *spyware*, *keyloggere og trojanske heste*.

Phishing

Phishing er en metode, hvor hackeren forsøger at ”fiske” oplysninger ved at snyde modtageren af en e-mail til at indtaste brugernavn og kodeord, trykke på et link eller downloade en fil, der indeholder skadelig kode (malware). Phishing-mails sendes ofte bredt ud til mange modtagere i håbet om, at én eller flere ”hopper på krogen”. Lignende angrebsformer er bl.a. spear phishing (målrettet enkeltpersoner), CEO fraud (bl.a. målrettet bestyrelsesmedlemmer) og smishing (phishing via sms).

DoS og DDoS

Et Denial of Service (DoS)-angreb er et angreb, der gør en service utilgængelig ved f.eks. at “oversvømme” en hjemmeside eller et netværk med trafik, så den/det bryder sammen, og er utilgængeligt, mens angrebet står på. Ved et Distributed Denial of Service (DDoS)-angreb kommer trafikken fra flere kilder, typisk kompromitterede maskiner spredt på internettet (kaldet *botnets*), hvilket gør angrebet vanskeligt at blokere.

4. Temaer i en cyberstrategi

Virksomheders arbejde med cyber- og informationssikkerhed handler om mere end IT. Det handler i høj grad også om governance, ledelse, processer og mennesker. Sikkerhed er i sidste ende bestyrelsens ansvar, og bør være et vigtigt emne på bestyrelsens dagsorden. Cybertruslen er reel, og virksomheder er nødt til at have en strategi for at håndtere den.

Det overordnede formål med en cyberstrategi er at Forebygge, Beskytte, Opdage og Håndtere cyberhændelser samt Genoprette systemer, data mv. efter en hændelse (engelsk: *Prepare*, *Protect*, *Detect*, *Respond*, *Recover*). Disse kernefunktioner er ligeledes indbygget i anerkendte rammeværker for håndtering af cybersikkerhed, f.eks. NIST-standarden.

Som grundprincip for sikkerhedsniveauet skal bestyrelsen arbejde ud fra, at virksomheden skal træffe *"passende og forholdsmæssige tekniske og organisatoriske foranstaltninger"* baseret på en konkret risikovurdering. Dette krav findes i nogenlunde enslydende bestemmelser i gældende regulering på sikkerhedsområdet, og anses for best practice.

Gældende regulering er sparsom med eksempler på, hvad der udgør "*passende og forholdsmæssige tekniske og organisatoriske foranstaltninger*". Det er derfor i høj grad op til den enkelte bestyrelse og virksomhed at finde den rette balance mellem risikoappetit og sikkerhedsniveau samt at fastlægge en strategi for styring af cyberrisici.

En cyberstrategi er ikke en snæver IT-faglig opgave, men er en tværgående operationel risikostyringsopgave, der kræver samarbejde på tværs af traditionelle faglige skel. I arbejdet med en cyberstrategi kan bestyrelsen orientere sig indenfor de 6 temaer vist til højre.

5 overordnede formål med en cyberstrategi

1. **Forebygge** at et cyberangreb kan lykkes.
2. **Beskytte** virksomheden mod et cyberangreb.
3. **Opdage** hvis/når et angreb sker.
4. **Håndtere** et angreb hvis/når det sker.
5. **Genoprette** evt. ramte systemer og data.

Generelt krav til sikkerhedsniveauet

Virksomheden skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger, der sikrer et sikkerhedsniveau, der passer til risikoen.

6 temaer i en cyberstrategi

1. Risikovurdering og sårbarheder
2. Risikoappetit og strategi
3. Planer, processer og beredskab
4. Rapportering og kontrol
5. Kultur og mennesker
6. Kompetencer og organisering

5. Opbygning af anbefalingerne

Disse anbefalinger er bygget op om 6 temaer til en cyberstrategi, og består af tre dele: (1) Overordnede anbefalinger, (2) Kort checkliste, og (3) Uddybende værktøjskasse. De tre dele supplerer hinanden, og kan anvendes både sammen og hver for sig.

Anbefalingerne er udarbejdet med udgangspunkt i, at bestyrelsen bør følge anbefalingerne. Det væsentligste formål med anbefalingerne er at sikre, at bestyrelsen implementerer cyber- og informationssikkerhed som en integreret del af sit arbejde.

(afsnit 6 – side 8)

Checklisten er udarbejdet som en kort og overskuelig liste med nogle af de mest relevante spørgsmål, bestyrelsen kan stille sig selv og direktionen til brug for en systematisk og risikobaseret tilgang til cyber- og informationssikkerhed. Checklisten er vejledende.

(afsnit 7 – side 9)

Værktøjskassen er udarbejdet som en uddybende liste af spørgsmål og overvejelser i et bestyrelseslokale, som kan bruges til inspiration og understøttelse af en hensigtsmæssig risikohåndtering af cybertrusler. Der er en særskilt "værktøjskasse" for hvert af de 6 temaer. Værktøjskassen er vejledende og ikke-udrømmende.

(afsnit 8 – side 10 til 15)

6. Anbefalinger til bestyrelsen

Strategi

Udførelse

Mennesker

1. Risikovurdering og sårbarheder

Det anbefales, at
- bestyrelsen mindst to gange om året modtager og forholder sig til en opdateret risikovurdering på cyberområdet baseret på virksomhedens vigtigste værdier, teknologilandskab, primære sårbarheder, sandsynlige trusler, mulige tab ved angreb og anbefaling til (yderligere) investering.

2. Risikoappetit og strategi

Det anbefales, at
- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter virksomhedens risikoappetit indenfor cyber- og informationssikkerhed baseret på en afvejning af virksomhedens forretningsmål og digitaliseringsstrategi, risikoprofil, eksisterende sikkerhedsbudget og investeringsvilje.

3. Planer, processer og beredskab

Det anbefales, at
- bestyrelsen fører kontrol med, at cyber- og informationssikkerhedsrisici er fastlagt i politikker og håndteret i processer for it/fysisk sikkerhed og digital adfærd.
- bestyrelsen fører kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering i tilfælde af alt fra hackerangreb til strømnedbrud.

4. Rapportering og kontrol

Det anbefales, at
- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul, og har cybersikkerhed på agendaen på hvert bestyrelsesmøde.
- bestyrelsen modtager relevant rapportering forud for hvert bestyrelsesmøde med bl.a. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest og awareness aktiviteter, resultater fra revisionsgennemgange, evt. forslag til supplerende tiltag ift. forsikringsdækning og investeringer.

5. Kultur og mennesker

Det anbefales, at
- virksomheden har et træningsprogram for bestyrelse, direktion og medarbejdere i relation til cyber- og informationssikkerhed.
- bestyrelsen går forrest i at understøtte en stærk og bevidst cyber- og informationssikkerhedskultur i virksomheden.

6. Kompetencer og organisering

Det anbefales, at
- mindst ét medlem af bestyrelsen har viden om eller erfaring med cyber- og informationssikkerhed og tilegner sig indsigt i virksomhedens tekniske og sikkerhedsmæssige fundament.
- virksomhedens sikkerhedsorganisation er direkte forankret på et direktionsniveau, der rapporterer direkte til bestyrelsen.

7. Kort checkliste med relevante spørgsmål til bestyrelse og ledelse

1. Risikovurdering og sårbarheder

- ❑ Hvad betyder det for forretningen, hvis vigtige værdier ændres, stjæles, lækkes eller hvis kritiske systemer eller andre it-services er utilgængelige i kortere eller længere tid?
- ❑ Hvem er de sandsynlige angribere, hvad er deres mål, og hvilke redskaber/teknikker bruger de til at opnå disse mål?
- ❑ På hvilke områder er virksomheden mest sårbar overfor angreb (teknologi, personale, processer), og hvor sandsynligt er angreb indenfor disse områder?
- ❑ Hvad er virksomhedens plan for risikohåndtering, inkl. investeringer?

2. Risikoappetit og strategi

- ❑ Hvor stort er budgettet for cyber- og informationssikkerhed?
- ❑ Hvor ligger virksomhedens sikkerhedsniveau- og budget sammenlignet med andre forretningsområder? Med andre virksomheder?
- ❑ Hvad er de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet?
- ❑ Baseret herpå, hvad er virksomhedens tolerance for at påtage sig cyberrisici?

3. Planer, processer og beredskab

- ❑ Har virksomheden nedskrevne it-sikkerhedspolitikker, som direktionen aktivt støtter, og som medarbejderne er trænet i?
- ❑ Foreligger der beredskabs- og kommunikationsplaner – både elektronisk og på papir – til at håndtere sikkerhedshændelser?
- ❑ Beskriver planerne hvordan forretningen kan fortsætte i tilfælde af manglende adgang til de vigtigste it-systemer og it-services, hvem der skal involveres i en krisesituation, og hvordan der sker reetablering af it-systemer og it-services?
- ❑ Angiver planerne en handlingsplan for de første 24 timer efter en sikkerhedshændelse, herunder hvem der har ansvaret for at føre minutrapport?
- ❑ Bliver planerne øvet og testet regelmæssigt?
- ❑ Hvad er resultatet af seneste test, og har det ført til ændringer?
- ❑ Bliver planerne justeret i lyset af angreb, der har ramt andre virksomheder?
- ❑ Er der indgået aftale med eksterne, som kan tilkaldes for at støtte interne teams?

4. Rapportering og kontrol

- ❑ Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed (risici, status, investeringer, anbefalinger mv.) fra direktionen?
- ❑ Er cyber- og informationssikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?

5. Kultur og mennesker

- ❑ 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?
- ❑ 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?
- ❑ Går bestyrelsen forrest i at understøtte en stærk og bevidst cybersikkerhedskultur, f.eks. ved selv at anvende VPN, password managers og flerfaktor godkendelse?

6. Kompetencer og organisering

- ❑ Har mindst ét bestyrelsesmedlem kompetencer og erfaring indenfor cyber- og informationssikkerhed? Hvis ikke, får bestyrelsen intern eller ekstern rådgivning og/eller sparring på området? F.eks. fra rådgivere eller en komité?
- ❑ Deltager bestyrelsen aktivt i diskussioner om cyber- og informationssikkerhed?
- ❑ Er bestyrelsen opmærksom på, at dens medlemmer selv kan være et oplagt mål for cyberangreb?
- ❑ Hvor i organisationen (person/funktion) ligger ansvaret for cyber- og informationssikkerhed?
- ❑ Rapporterer denne sikkerhedsfunktion direkte til de rigtige på ledelsesniveau?
- ❑ Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- ❑ Har virksomheden de rette tekniske kompetencer inhouse, eller er der behov for ekstern hjælp?

8. Værktøjskasse

Tema 1 – Risikovurdering og sårbarheder

Til brug for styring af cyberrisici og fastlæggelse af en overordnet cyberstrategi er bestyrelsen nødt til at have tilstrækkelig indsigt i virksomhedens overordnede teknologilandskab, vigtigste værdier, primære sårbarheder samt de mest sandsynlige trusler og konsekvenser af et cyberangreb.

Selvom bestyrelser er vant til at arbejde med risiko, sandsynlighed og konsekvens, er de færreste hjemmevante i cyber- og informationsrisici.

Indenfor cyber- og informationssikkerhed er risikovurderingen (også) omdrejningspunktet i risikostyringen, hvor risici identificeres, analyseres og evalueres.

Til at kontrollere, at bestyrelsen modtager tilstrækkelig information, kan listen til højre være til inspiration.

Bestyrelsen bør mindst to gange om året modtage en opdateret risikovurdering fra direktionen, der bl.a. beskriver:

1) Vigtigste værdier og systemer
2) Konsekvenser ved læk eller nedbrud
3) Primære sårbarheder
4) Trusler (prioriteret) og sandsynlighed
5) Plan for risikohåndtering og investeringer

CFCS vurderer, at op mod 80 procent af de e-mails en organisation modtager udefra kan være uønskede eller direkte skadelige, og at større organisationer dagligt modtager phishing-mails. (Kilde: CFCS – Cybertruslen fra phishing-mails)

Centrale overvejelser i et bestyrelseslokale

Værdier og systemlandskab
- Hvad er virksomhedens vigtigste værdier? Det kan være materielle aktiver (f.eks. systemer), immaterielle aktiver (f.eks. data og IP) og renommé.
- Hvor opbevares virksomhedens vigtigste data og informationer (f.eks. i cloud, hos ekstern leverandør, indenfor eller udenfor Danmark?)
- Hvilke it systemer og –services er de mest kritiske?
- Hvem er virksomhedens vigtigste leverandører og samarbejdspartnere?
- Hvilke kontrol- og sikkerhedssystemer har virksomheden implementeret (f.eks. overvågning, AI på adgangskontroller, multi faktorautentificering)?
- Bliver disse oversigter løbende vedligeholdt – og af hvem?

Konsekvenser ved en sikkerhedshændelse
- Hvad betyder det for forretningen, hvis vigtige værdier ændres, stjæles, lækkes eller hvis kritiske systemer eller andre it-services er utilgængelige i kortere eller længere tid?

Sårbarheder
- Hvor er virksomheden mest udsat for sikkerhedsbrud? (Sårbarheder kan ligge i systemer og programmer som f.eks. Active Directory, processer der mangler eller ikke følges, manglende awareness hos medarbejdere og lign.)
- Er adgang til data og netværk begrænset til det nødvendige? (risikoen er større jo flere mennesker, der har adgang)
- Bliver sikkerhedsniveauet jævnligt testet, f.eks. gennem ”red team”-angreb, firewall audits, sårbarhedsskanninger, penetrationstest, GAP analyser og lign?

Trusselsbillede og sandsynlighed
- Hvem er de sandsynlige angribere?
- Hvad er deres mål (f.eks. stjæle penge, IP, informationer, digital identitet)?
- Hvilke redskaber/teknikker bruger de til at opnå ovenstående mål (f.eks. phishing, drive-by exploits, social engineering, DDoS, malware mv.)
- Hvor sandsynlige er disse trusler overfor virksomhedens sårbarheder?

Plan for risikohåndtering og investeringer
- Hvad er virksomhedens plan for risikohåndtering, inklusive investeringer?

8. Værktøjskasse

Tema 2 – Risikoappetit og strategi

Som led i cyberstrategien bør bestyrelsen mindst én gang årligt fastlægge virksomhedens risikoappetit på cyber- og informationssikkerhedsområdet, forstået som den risiko, bestyrelsen er villig til at acceptere for at opnå virksomhedens strategiske målsætninger.

Risikoappetitten er redskabet til at koble de strategiske målsætninger sammen med den operationelle drift.

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

Risikoappetitten kan udtrykkes som en overordnet målsætning (f.eks. at der skal være en "lav risiko" for, at virksomheden kan blive misbrugt til datalæk, eller at sikkerhedsniveauet som minimum skal opretholdes ved outsourcing).

Risikoappetitten kan også være målbar (f.eks. en minimum tilgængelighed på kritiske systemer eller forbud mod at opbevare følsom data udenfor Danmark).

Bestyrelsesmedlemmer skal være påpasselige med at undervurdere risikoen og anvende gennemsnits-betragtninger og middelværdier, da det kan give et skævt billede af den reelle risikoeksponering – eks. kan man jo ikke vide, om man selv er gennemsnittet.

Til at fastsætte risikoappetitten og føre tilsyn med virksomhedens eksponering kan bestyrelsen bruge listen til højre til inspiration.

Ifølge PwC 2021 Digital Trust Insights Survey svarede 50% af respondenterne, at de tænker cybersikkerhed og privacy ind i enhver forretningsmæssig beslutning. 55% svarede, at de øger cyber budgettet i 2021.

Centrale overvejelser i et bestyrelseslokale

Strategi

- 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.

Risikobillede

- Hvad er det centrale i risikovurderingen fra direktionen *(se 'Risikovurdering og sårbarheder' i Tema 1)*, herunder på hvilke områder er virksomheden mest sårbar overfor angreb, hvor sandsynligt er angreb på virksomheden indenfor disse områder, og hvad er de potentielle konsekvenser ved et angreb, f.eks. økonomisk, samfundsmæssigt og for renomméet?
- Har virksomheden kritisk infrastruktur eller er den i øvrigt underlagt regulatoriske krav, der påvirker risikoappetitten?
- Er virksomheden på vej til at investere i ny teknologi og services (f.eks. mere IoT og cloud), der ændrer risikobilledet og kræver ny investering i sikkerhed?
- Har virksomheden legacy-systemer (dvs. ældre systemer der skal udskiftes)? Hvis ja, er der en plan for udfasning eller isolering af programmer og operativsystemer, der ikke længere supporteres eller opdateres?

Omkostninger

- Hvor stort er budgettet for cyber- og informationssikkerhed?
- Hvor ligger virksomhedens sikkerhedsniveau- og budget sammenlignet med andre virksomheder?
- Hvad er de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet?
- Hvad er de rigtige investeringer for os? Skal vi forsikre os ud af det, eller indgå samarbejdsaftaler?

Risikoappetit

- 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.?

8. Værktøjskasse

Tema 3 – Planer, processer og beredskab

Det ikke er et spørgsmål om, hvorvidt virksomheden bliver ramt, men et spørgsmål om hvornår. Alle virksomheder bør derfor have et velafprøvet beredskab. Det er vigtigt, at bestyrelsen spørger ind til, og om der foreligger velafprøvede planer og processer til at håndtere cyber- og informationssikkerhedshændelser.

Selvom virksomheden allerede har sikkerhedspolitikker og beredskabsplaner, er det ikke sikkert, at de tager højde for, hvordan virksomheden forebygger, beskytter, opdager og håndterer en sikkerhedshændelse og genopretter systemer efter et angreb.

Sikkerhedshændelser kan have store omkostninger til udredning, genopretning, driftstab, kompensation til kunder mv. Det er derfor vigtigt, at have dokumenterede og testede politikker, processer og beredskabsplaner, som medarbejderne er trænet i, for at kunne forebygge og håndtere et angreb effektivt.

Hvis virksomheden ikke følger en standard eller et rammeværk for styring af informationssikkerhed, kan det overvejes at læne sig op ad 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).

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 til inspiration.

Ifølge PwC 2019 Annual Corporate Directors Survey svarede 53 % af respondenterne, at bestyrelsen var tryg ved virksomhedens plan for håndtering af sikkerhedshændelser.

Centrale overvejelser i et bestyrelseslokale

Udmøntning

- Er risikoappetitten *(se 'Risikovurdering og sårbarheder' i Tema 1)* udmøntet som rammer i virksomhedens interne politikker, f.eks. for operationel risici, compliance risici, markedsrisici, likviditetsrisici, forsikringsrisici, outsourcing mv. ?

Processer og politikker

- Har virksomheden nedskrevne it-sikkerhedspolitikker, som direktionen aktivt støtter, og som medarbejderne er trænet i? F.eks. politikker for, hvor ofte it-sikkerhedsniveauet skal testes/opgraderes (såsom at firewall audits skal udføres månedligt eller at nye applikationer skal gennemgå code review, før de udrulles), politikker for opførsel for medarbejdere, leverandører og kunder mv.
- Har virksomheden en politik om, at backup skal kunne genskabe 100% - og hvis ikke Hvor meget data kan genskabes og hvor langt tilbage?
- Er sikkerhed tænkt ind i virksomhedens forretningsprocesser?

Beredskabsplaner Er der planer for reetablering af systemer og data (Disaster Recovery Plans og Technical Recovery Plans)?

- Er der planer for, hvordan forretningen kan fortsætte i tilfælde af manglende adgang til systemer, programmer og data (Business Continuity Plans og IT Service Continuity Plans)?
- Beskriver planerne, hvem der skal involveres i en krisesituation, f.eks. kommunikation, økonomi, ledelse, jura, responsteamet og it-specialister?
- Beskriver planerne hvordan forretningen kan fortsætte i en krisesituation? Er der indgået aftale med eksterne ressourcer og specialister, som kan tilkaldes for at støtte interne teams?
- Har planerne procedurer for indsamling af dokumentation og orientering, f.eks. hvornår bestyrelsen skal orienteres og hvem der fører minutlog efter et angreb?
- Hvad er procedurerne for at kommunikere med myndighederne, f.eks. politi, tilsyn, Erhvervsstyrelsen (virk.dk)?
- Hvornår og hvordan vil man orientere andre interessenter – f.eks. leverandører eller individer, hvis personoplysninger er kompromitteret?
- Bliver planerne øvet og testet regelmæssigt?
- Hvad er resultatet af seneste test, og har det ført til forbedringer?
- Bliver planerne justeret i lyset af angreb, der har ramt andre virksomheder?

8. Værktøjskasse

Tema 4 – Rapportering og kontrol

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 2.

Den specifikke rapportering, bestyrelsen bør modtage, og hvor ofte, er delvist afhængig af den enkelte virksomhed.

Der findes ikke en standard for rapportering på cyber- og informations-sikkerhedsområdet, og rapporteringen kan nemt blive subjektiv.

Det er derfor vigtigt, at bestyrelsen beder om en konsistent rapportering, og at bestyrelsen får information nok til at forstå, hvad der ligger bag det, der rapporteres, og hvordan det stemmer med den overordnede cyberstrategi.

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

Ifølge PwC 2019 Annual Corporate Directors Survey svarede 66 % af respondenterne, at bestyrelsen modtager meningsfuld rapportering på cyberområdet.

Centrale overvejelser i et bestyrelseslokale

Rapportering
Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed fra direktionen, f.eks. om:

- Top 5-10 væsentligste cyberrisici samt udvikling/trends siden sidst
- Resultater fra test af beredskabsplaner og kritiske systemer
- Sikkerhedshændelser og konsekvenser heraf
- Status på implementering af sikkerhedstiltag
- Eventuelle fravigelser fra de af bestyrelsen fastsatte risikotolerancer
- Resultater fra interne og eksterne audits
- Sikkerhedsbudget og sammenligning med markedet
- Forsikringer og hvilke udgifter/tab de dækker ved et cyberangreb
- Anbefalinger til forbedringer og investeringer forbundet hermed

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 2.

Audit 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 findings fra disse audits, 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?

8. Værktøjskasse

Tema 5 – Kultur og mennesker

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 et højt sikkerhedsniveau, da der ikke skal mere end én uopmærksom medarbejder til at trykke på et forkert link.

Der er et behov for træning og awareness programmer for medarbejderne i danske virksomheder, både i forhold til at dele viden, øge viden og ændre adfærd.

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".

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.

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

Ifølge PwC 2019 Cybercrime Survey udgør ansattes/insideres ubevidste handlinger fortsat den største cybertrussel. 54% af respondenterne angav, at virksomheden rent faktisk testede sine medarbejdere i awarenesstræning mv.

Centrale overvejelser i et bestyrelseslokale

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 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?

8. Værktøjskasse

Tema 6 – Kompetencer og organisering

Bestyrelsesmedlemmer forventes i dag at være i stand til at forholde sig til væsentlige forhold i relation til virksomhedens sikkerhed, og at kunne medvirke til at stille spørgsmål til direktionen og forholde sig til svarene.

Bestyrelsen behøver ikke kende cyber- og informationssikkerhed i detaljer, men mindst ét medlem bør have indsigt i virksomhedens tekniske og sikkerheds-mæssige fundament og være i stand til at sparre på lige fod med direktionen.

Cyber- og informationssikkerhed er for vigtigt og komplekst til, at forståelsen ligger hos 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 sikkerheds-hændelse. 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.

Indtil de rette kompetencer er til stede, må bestyrelsen sikre sig, at både bestyrelsen, ledelsen og organisationen faktisk har eller har adgang til de nødvendige kompetencer og ressourcer på cyberområdet – om nødvendigt gennem aftaler med eksterne samarbejdspartner og specialister.

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

Ifølge PwC 2019 Annual Corporate Directors Survey svarede 36 % af respondenterne, at bestyrelsen havde tilstrækkelige kompetencer på cyberområdet. Ifølge PwC 2021 Digital Trust Insights Survey svarede 51% af respondenterne, at de planlægger at øge cybersikkerheds bemandingen de kommende 12 måneder

Centrale overvejelser i et bestyrelseslokale

Bestyrelsen

- Har mindst ét bestyrelsesmedlem kompetencer og erfaring med cyber- og informationssikkerhed, f.eks. cybersikkerheds- og risikovurderingsprocesser, leverandørstyring, sikkerhedskrav og lignende?
- Er cybersikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- Holder bestyrelsen sig løbende orienteret om de cybertrusler og aktører, der truer virksomheden, deres metoder og motivation?
- Deltager bestyrelsen aktivt i diskussioner om cybersikkerhed?
- Modtager bestyrelsen løbende træning og uddannelse i cybersikkerhed?
- Er bestyrelsen opmærksom på, at den selv kan være et oplagt mål for cyberangreb (f.eks. CEO fraud)?

Direktionen

- Har virksomheden en sikkerhedsorganisation forankret på direktionsniveau, f.eks. CEO, CFO eller CIO?
- Rapporterer denne funktion direkte til bestyrelsen eller gennem en anden rapporteringsproces?

Organisationen

- Hvor i organisationen (person/funktion) ligger ansvaret i øvrigt for cyber- og informationssikkerhed?
- Bør andre forretningsområder involveres i arbejdet med cybersikkerhed, f.eks. ledere af afdelinger, der udvikler vores produkter og services?
- Rapporterer denne sikkerhedsfunktion til de rigtige på ledelsesniveau?
- Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?

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 trends og best practices for at give cybersikkerhed et ekstra perspektiv?

APPENDIKS

Appendiks 1. Ordliste – eksempler på udvalgte ord og begreber inden for cybersikkerhed

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.

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.

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.

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.

Der findes forskellige definitioner af centrale begreber inden for cyber- og informationssikkerhed. Udvalgte begreber fremgår i dette appendiks. Mere information kan bl.a. findes i CFCS's dynamiske ordliste her: https://cfcs.dk/da/cybertruslen/ordforklaringer/

Appendiks 2. Årshjul – eksempel på cyber-delen

1. kvartal

- Organisation, herunder cyberkompetencer og organisering
- Cybersikkerhed awareness
- Status på drift og sikkerhedshændelser

Se vejledning

5 – Kultur og mennesker

6 – Kompetencer og organisering

2. Kvartal

- Rammer og strategi for styring af cyberrisici
- Fastlæggelse af risikoappetit
- Status på drift og sikkerhedshændelser

Se vejledning

1 – Risikovurdering og sårbarheder

2 – Risikoappetit og strategi

3. Kvartal

- Politikker og planer for risikohåndtering og beredskab
- Forsikringsdækning for cyberangreb
- Status på drift og sikkerhedshændelser

Se vejledning

3 – Planer, processer og beredskab

4. Kvartal

- Årsbudget, herunder budget for IT-sikkerhed og investeringer i forbedringer
- Status på drift og sikkerhedshændelser

Se vejledning

4 – Rapportering og kontrol

Appendiks 3. Akut checkliste ved cyberhændelser

Tabellen til højre viser et eksempel på en akut checkliste ved en cyberhændelse.

Checklisten er illustrativ:

- ✓ Alle sikkerhedshændelser er forskellige
- ✓ Der findes ikke én tjekliste, der dækker alle situationer
- ✓ Det er vigtigt at kunne være fleksibel i reaktionen

Det vigtigste arbejde sker *før,* virksomheden bliver ramt, bl.a. ved etablering af en *incident response* plan, sikring af backup og evt. indgåelse af aftale med en ekstern sikkerhedspartner, der kan hjælpe.

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.

På bl.a. https://sikkerdigital.dk/virksomhed/naar-skaden-er-sket findes overordnet hjælp til nogle af de mest almindelige typer hændelser.

#	Akut checkliste	Eksempler
1	**Undgå panik og bevar roen**	› Betal ikke de kriminelle
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 password › Kontakt banken (ved økonomisk svindel)
4	**Brug Incident Response planen**	› Processen for hændelseshåndtering ligger typisk hos systemejerne
5	**Få kvalificeret ekstern hjælp**	› Fra bl.a. 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**	› Politianmeldelse › Anmeldelse til Datatilsynet (ved tab af persondata) › Anmeldelse til andre myndigheder (særlig i kritiske sektorer)
9	**Husk dokumentation af forløbet**	› Minutlog og revisionsspor mm.
10	**Sørg for bevissikring**	› Få kvalificeret ekstern hjælp til bevissikring › 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

Appendiks 4. Personlig cybersikkerhed for bestyrelsesmedlemmer – 20 konkrete råd

#	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?
4	Brug en dedikeret e-mailkonti til virksomhedskommunikation	› Hvis du bruger din egen, så benyt en anerkendt udbyder med spamfiltre og to-faktor login.
5	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 to-faktorautentificering	› Slå altid 2-faktor-autentificering 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.
11	Lås altid dine enheder	› Indstil dine enheder til automatisk skærmlås.
12	Krypter dit indhold	› Du bør også gøre fjernsletning af data muligt.

#	Beskytte	
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 som du kan, f.eks. gennem 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 5. Sikker kommunikation i bestyrelsen

Som led i at styrke de strategiske cyberkompetencer i danske virksomheder, er en sikker kommunikation i bestyrelseslokalet en vigtig forudsætning for at modvirke eventuelle sårbarheder, som kan skade virksomheden, dens kunder og/eller ansatte.

En velovervejet og gensidig forståelse for sikker kommunikation i bestyrelsen, er en forudsætning for en fortrolig kommunikation i bestyrelseslokalet og ikke mindst for virksomheden generelt.

I takt med udviklingen på digitaliseringsområdet og større digital kompleksitet er der en række områder, som de cyberkriminelle er særlig interesseret i.

I bestyrelseslokalet handler det bl.a. om at beskytte:

► *Data*

► *Omdømme*

► *Immaterielle rettigheder*

► *Strukturelle ændringer som f.eks. ejerskifte, generationsskifte, fusioner*

► *Sensitiv information, f.eks. om virksomhedens risikolandskab, medarbejdere og kunder*

► *Produktnyheder, f.eks. produkter, services og ydelser, som virksomheden ønsker at lancere*

Generelle anbefalinger til sikker kommunikation i bestyrelsen:

1. Mobile elektroniske enheder i lokalet

› Bestyrelsen bør overveje at begrænse mobile elektroniske enheder, når bestyrelsesmøder afholdes. Dette for at begrænse, at digitale medier, via applikationer, smartwatch eller andre elektroniske enheder, kan kompromitteres før-under-efter mødet.

2. Elektronisk kommunikation

› Bestyrelsen bør overveje at undgå brugen af e-mails til at udveksle sensitiv information samt anvende bitlockere, som krypterer og kræver kode for at få adgang til filer. Bestyrelsen kan f.eks. udveksle information og opbevare filer på en board management platform. Eksempel på overblik over forskellige board management software muligheder: https://www.capterra.com/board-management-software/

3. Overvågning i bestyrelseslokalet

› Bestyrelsen bør overveje at begrænse møder i lokaler med lyd- eller videoovervågning i rummet, idet dette begrænser risikoen for at sensitive information lækkes.

4. Tredjeparter i bestyrelsen

› Tredjeparter, som deltager i bestyrelsesmøder eller som modtager sensitive informationer, bør screenes inden deltagelse i bestyrelsesmøder, herunder i forhold til sociale platforme m.v. Dette samme gælder for nye bestyrelsesmedlemmer.

5. Fysisk placering af bestyrelsesmøder

› Bestyrelsen kan overveje at skifte mødelokale fra gang til gang og at booke lokale under et anonymiseret navn for at begrænse mønsteret i bestyrelsens mødeårshjul. Dette gælder særligt, hvis bestyrelsen skal drøfte sensitive emner.

6. Sikker destruktion af sensitive materialer

› Bestyrelsen bør begrænse medbragte sensitive informationer i papirformat og destruere sensitivt materiale efterfølgende, f.eks. efter anvisninger i en arkiverings- og sletningspolitik.

Appendiks 6. Cyber respons under COVID-19

COVID-19 har påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger. Særlige cybertrusler, risici og angreb relateret til COVID-19 er bl.a.:

Phishingangreb, ondsindede internetsider og angreb på organisationens e-mailsystemer.

- Cyber-kriminelle anvender i høj grad den stigende interesse i den globale epidemi til at sprede spam kampagner relateret til COVID-19.

Ransomware, afpresning, IP rettigheder og skade på virksomhedens omdømme.

- Cyber-kriminelle målretter angreb mod de organisationer, som anses at være under pres fra COVID-19.
- Handlinger eller udtalelser anset som upassende fra organisationen kan være årsag til hacktivisme.

Operationelle forstyrrelser fra cyberangreb

- Organisationer bliver i højere grad udsat for et COVID-19 tematiseret angreb, såsom falske donationslinks, hvilket leder til et ransomware angreb, hvor cyber-kriminelle krypterer kritiske IT aktiver og kræver en betaling for dekrypteringen af disse.

Virtualisering af tidligere fysiske aktiviteter og **decentralisering** af processer

- Ændring i netværks-baseline:

1. Fjernadgang til høj-risiko handlinger giver alarmer
2. Al trafik vil være udsvingsgivende indtil en ny baseline kan etableres
3. Pres på helpdesk

Center for Cybersikkerhed har specifikt set på cybertruslen mod Danmark under COVID-19: https://cfcs.dk/da/temasider/covid-19/cybertruslen-mod-danmark-under-covid-19/

Følgende handlinger kan mitigere disse trusler og beskytte organisationen imod særlige indenfor cyber relateret til COVID-19:

- **MFA**. Implementering af multifaktor-autentifikation (MFA) på samtlige VPN forbindelser til at øge den generelle sikkerhed. Hvis MFA ikke kan anvendes, kan der bruges længere og mere komplekse adgangskoder.
- **Opdatering**. Opdatering af VPN, netværksinfrastrukturenheder og enheder for at opnå fjernadgang til organisationens miljø med de seneste softwareopdateringer og sikkerhedskonfigurationer.
- **Adgange**. Monitering af privilegerede adgange ved optimering af adfærdsanalytiske værktøjer for at identificere mistænksomme aktiviteter.
- **Filtrering**. Web og e-mailbeskyttelse ved implementering af web-filtrering. Således blokeres ondsindede hjemmesider. E-mailfiltreringen kan implementeres og anvendes til at blokere spam og phishing e-mails.
- **Overvågning**. Øge monitoreringskapaciteten og identificeringen af potentielle malware eller kampagner, som anvender de nuværende COVID-19 scenarier, f.eks. via blacklisting eller markering af udefrakommende e-mails. Øge organisationens end point-monitorering.
- **Falske hjemmesider og e-mails**. Minimere indvirkningen af forsøg på besvigelser i kritiske betalingssystemer relateret til COVID-19. En række COVID-19 relaterede websider og e-mails anvendes til phishingkampagner med henblik på at stjæle adgange og sprede malware.
- **Værktøjer**. Support for anvendelsen af samarbejdsværktøjer, såsom Microsoft Teams, Skype eller Cisco Webex.
- **Ressourcer og back-up**. Forøge kapaciteten til krisehåndtering ved at øge allokeringen af ressourcer. Evaluering af backupsystemer og failover kapaciteter. Helpdesk skal forberedes til at håndtere et øget antal af events.
- **Forberedelse**. Forbered værste scenarier, evaluering af krisehåndtering og interne eventresponskapaciteter. Ligeledes bør tilgængeligheden af tredjeparter evalueres.
- **SOC/SIEM**. Forstærkning af sikkerhedsinformation- og eventhåndteringssystemer (SIEM) samt sikkerhedsoperationscentre (SOC) og monitoreringsteams til at kunne håndtere en øget mængde sikkerhedsalarmer. Alarmer sorteres efter risici og procedurer for at skelne falske-positive fra reelle mistænksomme events.

Appendiks 7. Sikkert fjernarbejde under COVID-19

COVID-19 betyder, at mange nu arbejder hjemme – og mange vil formentlig fortsat gøre det fremadrettet.
Gode råd til en sikker arbejdsplads uden for kontoret:

Hold systemerne opdateret: prioriter at holde systemer, operativsystemer og applikationer opdateret.

Oprethold stærke adgangskoder, herunder lange og komplekse adgangskoder, multifaktor autentifikation og password managers.
Skift jævnligt adgangskode.

Anvend et sikret netværk, anvend lange og komplekse adgangskoder til dit trådløse netværk baseret på anerkendte standarder som WPA2.
Skift jævnligt adgangskode til dit netværk.

Begræns gæsteadgangen til dit hjemmenetværk, som anvendes til fjernarbejde.
Segmenter eventuelt dit netværk så din arbejdscomputer ikke anvender samme adgangspunkt som private enheder.

Anvend en krypteret forbindelse, f. eks. en VPN tunnel.

Vær skeptisk over for ukendte e-mails, bekræft mistænksomme e-mails, verificer f. eks. afsenderen med et opkald.

Hold dig opdateret med organisationens sikkerhedsteam for en bedre forståelse af de seneste risici på området.

Rapporter straks potentielle sikkerhedsbrud eller mistænksomme aktiviteter til rette personale i virksomheden.

Se også Center for Cybersikkerheds gode råd til hjemmearbejde her: https://cfcs.dk/da/temasider/covid-19/hjemmearbejde/

Appendiks 8. Referencer og baggrundsmateriale

Center for Cybersikkerhed	> Cyberforsvar der virker: (https://sikkerdigital.dk/media/10150/cyberforsvar-der-virker.pdf) > CFCS: Ordforklaringer: (https://cfcs.dk/da/cybertruslen/ordforklaringer/) > CFCS: Cybertruslen mod Danmark: (https://cfcs.dk/da/cybertruslen/)
Deloitte	> Cyber Risk Landscape Report 2019: (https://cyber.deloitte.dk/artikler/artikler-it-sikkerhed/cyber-risk-landscape-report-2019/)
Digitaliseringsstyrelsen	> Sikkerdigital.dk (https://sikkerdigital.dk/virksomhed/) > Vejledning i it-risikostyring og vurdering: (https://sikkerdigital.dk/media/10382/vejledning-it-risikostyring-og-vurdering.pdf)
Erhvervsstyrelsen	> Styrket digital sikkerhed i virksomhederne: (https://erhvervsstyrelsen.dk/styrket-it-sikkerhed-i-virksomhederne)
IBM	> IBM X-Force Threat Intelligence Index 2019 (https://www.ibm.com/security/data-breach/threat-intelligence)
Industriens Fond	> Projekt for Styrkelse af Strategiske Cyberkompetencer: (https://www.industriensfond.dk/Styrkelse-af-Strategiske-Cyberkompetencer)
National Cyber Security Centre (UK)	> Board Toolkit (https://s3.eu-west-1.amazonaws.com/ncsc-content/files/board_toolkit_final.pdf)
PwC	> Hvordan kan din bestyrelse være effektiv i håndteringen af cyberrisici? (https://www.pwc.dk/da/nyt/publikationer/bestyrelseshaandbogen-2019/bestyrelse-haandteringen-af-cyberrisici.html) > 2021 Global Digital Trust Insights: (https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html) > 2019 Annual Corporate Directors Survey: (https://www.pwc.com/us/en/services/governance-insights-center/assets/pwc-2019-annual-corporate-directors-survey-full-report-v2.pdf.pdf) > 2019 Cybercrime Survey: https://www.pwc.dk/da/publikationer/2019/11/cybercrime-survey-2019.html
World Economic Forum	> Advancing Cyber Resilience Principles and Tools for Boards: (http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf) > Ten Ways the C-Suite Can Protect their Company against Cyberattack: (https://www.weforum.org/press/2019/10/ten-ways-the-c-suite-can-protect-their-company-against-cyberattack/)