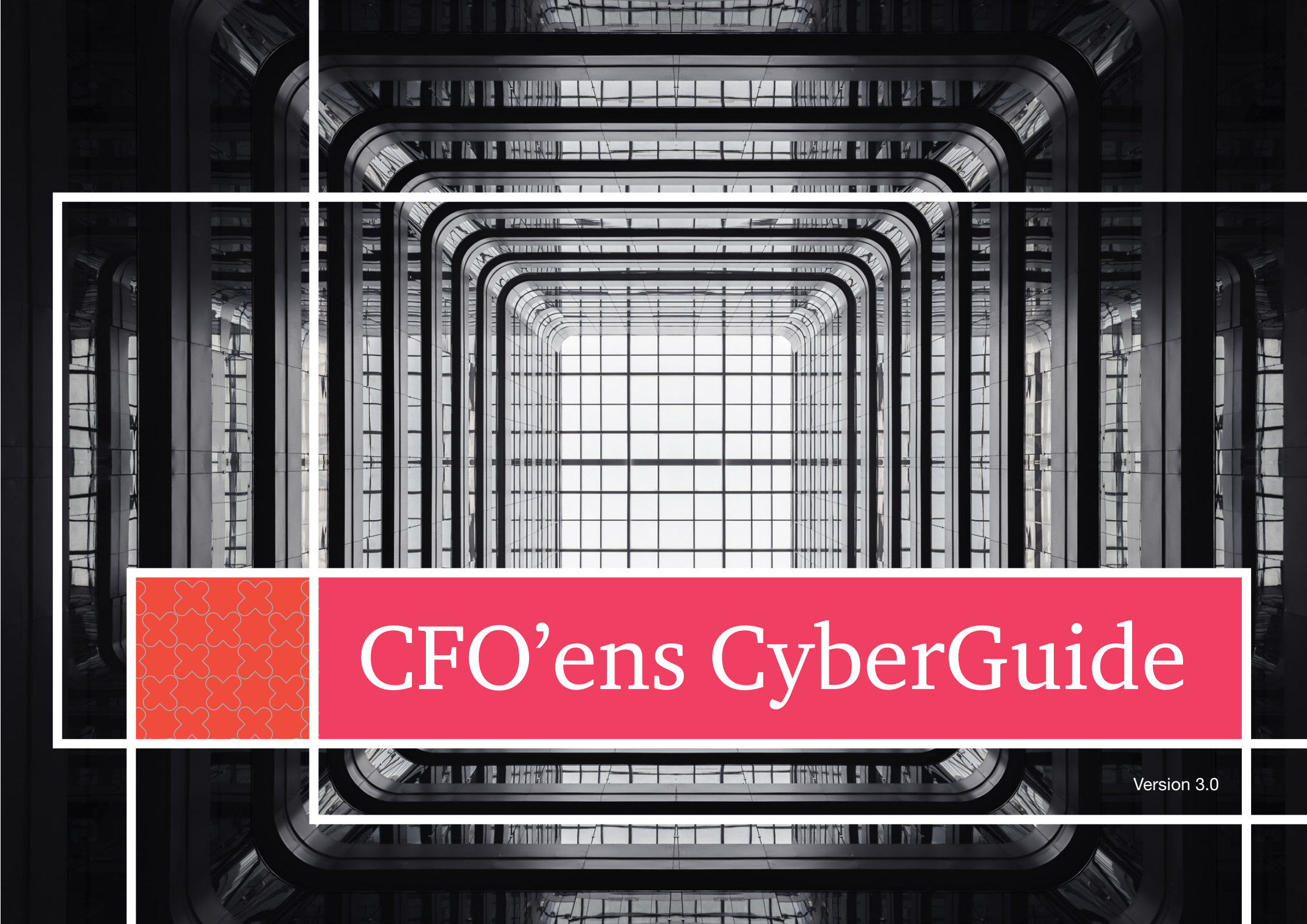


CFO'ens CyberGuide

Version 3.0

Indhold

Som CFO eller ledelse af en virksomhed har man en forpligtelse over for alle sine interessenter – medarbejdere, kunder, leverandører og samarbejdspartnere – om at sikre virksomheden mod digitale trusler. Truslerne er både interne og eksterne, og det handler derfor både om at sikre egen forretning og eksistens som virksomhed, men i ligeså høj grad om at forstå den risiko, der er ved at indgå i netværk med andre virksomheder.

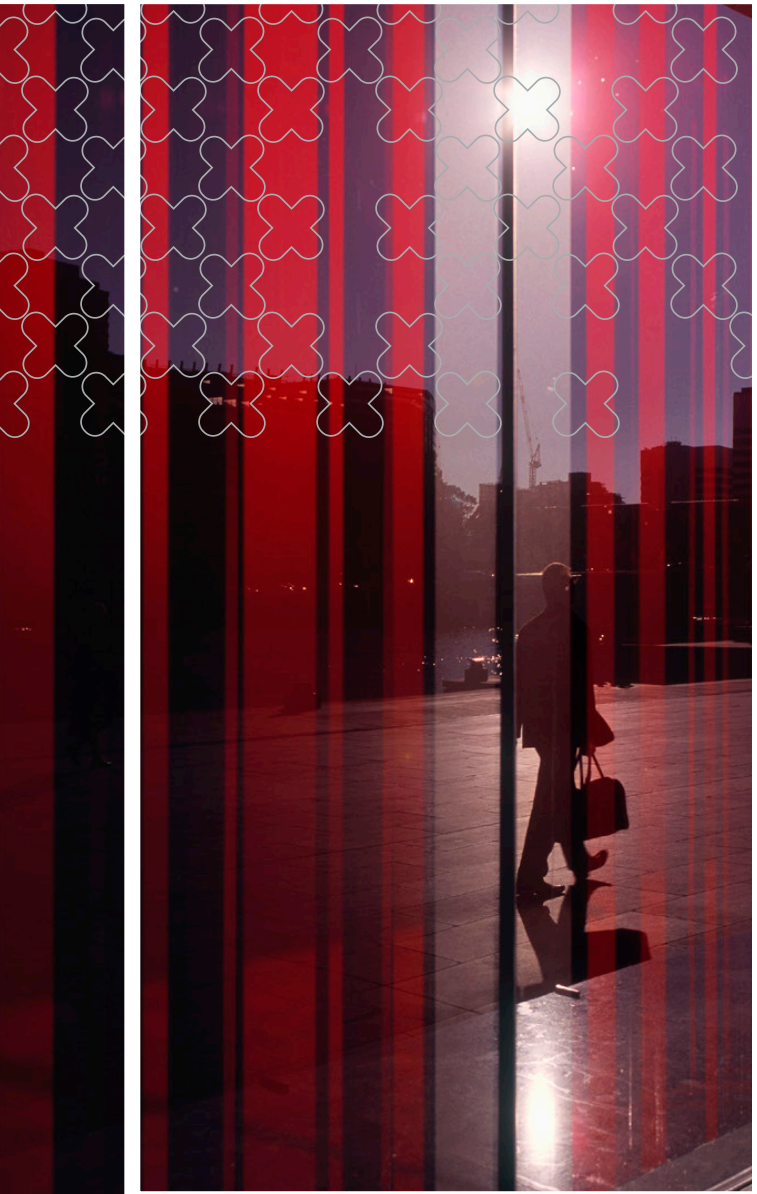
For at komme godt i gang med at styrke cybersikkerheden er du som CFO nødt til at gå grundigt til værks. Vi har i PwC skabt denne guide for at forberede dig både på de kerneudfordringer, som digitaliseringen skaber for din virksomhed, og samtidig for at tage dig igennem de trin, der ligger i at opbygge et cyberstrategisk fundament.

Guiden er bygget op i følgende seks indbyrdes forbundne afsnit:

Selvom denne guide er bygget kronologisk op, kan den også læses ved at springe mellem de enkelte afsnit. Hvert afsnit er bygget op med en indledning, der beskriver det primære fokus for afsnittet. Samtidig afsluttes hvert afsnit med en opsummering, der beskriver de vigtigste observationer, samt praktiske forslag til, hvordan du kommer videre med processen.

Guiden har til formål at klæde dig og direktionen på til at oversætte cybertruslen til et relevant risikobillede for jeres forretning. Med praktisk viden og indsigt fra konkrete cases fra virkeligheden kan guiden hjælpe jer godt i gang med at opbygge en forstærket cybersikkerhed og dermed dermed sikre, at I er bedre rustet mod cybertruslen.

Introduktion til den digitale udfordring for CFO'en



Digitaliseringen og de muligheder, der følger i kølvandet, har gennem de senere år bevæget sig højt op på topledelsens agenda. I forlængelse heraf er mange virksomheder blevet bedre til at udnytte de digitale muligheder i alle led i forretningen. I takt med at digitaliseringen tager fart, er cybersikkerhed mere end nogensinde også blevet et vigtigt tema. For digitaliseringen skaber ikke kun nye muligheder, men byder også på nye trusler.

PwC's Cybercrime Survey 2021 viser, at organiserede kriminelle nu udgør den største trussel i relation til cyber- og informationssikkerhed. Hele 78 % af de adspurgte anser således organiserede kriminelle for at være blandt de største cybertrusler, hvilket er den højeste andel i Cybercrime Surveyens historie. Heldigvis har mange virksomheder forbedret deres cyber- og informationssikkerhed. Vi ser dog også, at mange virksomheder fortsat har et stort potentiale i at styrke sig på netop disse områder. Samtidig ser vi, at der er behov for nye metoder, hvorpå cybersikkerhed kan integreres på tværs af forretningens områder som del af en robust cybersikkerhedsmodel, der skal sikre virksomhedens "kronjuveler".

Det er vigtigt, at indsigten i det aktuelle trusselsbillede samt det rigtige niveau for risikovillighed bliver drøftet i virksomhedens ledelse. Til gengæld skal virksomhederne passe på med at gå for detaljeret til værks i risikostyringen. Fokus bør være på de overordnede forretningsprocesser og ikke de enkelte it-systemer.

PwC's Cybercrime Survey 2021 viser, at 80 % af de adspurgte vurderer, at direktionen/ledelsen fokuserer på at opnå den rette balance mellem cybertrusler og investeringer i cybersikkerhed. De virksomheder, der har oplevet, hvor store omkostninger, der kan være forbundet med en cyberhændelse, anerkender, at sikkerhed bør prioriteres højere. Det kan derfor være relevant at diskutere omkostninger op mod den værdi, der skal beskyttes.

Det er vores erfaring, at de virksomheder, som er påbegyndt sikkerhedsrejsen, er druknet i et for stort detaljeringsarbejde. Her kan man med fordel skabe et hurtigt overblik ved at se på de større trusler først. For at hjælpe virksomhederne godt på vej i arbejdet med at øge cybersikkerheden, har vi i PwC samlet en række gode råd i denne guide. Guiden er målrettet direktionen og ledelsen særligt med udgangspunkt i CFO'en, da det i mange tilfælde er helt naturligt, at ansvaret for cybersikkerhed og den centrale rolle i relation til risici ofte placeres her. I mange virksomheder er der dog en anden organisering af ledelsen, og derfor er det vigtigt at understrege, at guiden er målrettet den samlede ledelse.

Guiden tager fat på de væsentligste udfordringer i relation til cybersikkerhed og -trusler. Den giver samtidig nogle konkrete bud på, hvordan CFO'en løser udfordringerne og løfter virksomhedens cybersikkerhed i samarbejde med både interne og eksterne interessenter. Cybersikkerhed er et vigtigt element i at drive ansvarlig virksomhed. Det er ledelsens rolle at løfte dialogen om cybersikkerhed og ansvarlighed ikke bare i virksomhedens eget risikoperspektiv, men også forhold til etiske forpligtelser. I år fokuserer Cybercrime Surveyen 2021 bl.a. på, at organiserede kriminelle udfører mere avancerede cyberangreb og hvordan vi gennem en vedvarende sikkerhedsindsats skaber og opretholder tilliden i virksomheder.

God fornøjelse.

Mads Nørgaard Madsen
Partner og leder af
Technology & Security

Trusselsbilledet i Danmark

62%

forventer en stigning i deres cyber- og informationssikkerhedsbudget inden for de næste 12 måneder.

78%

angiver, at organiserede kriminelle udgør den største trussel i relation til cyber- og informationssikkerhed.

Nøgletal fra PwC Cybercrime Survey 2021

pwc.dk/cyber21

81%

af CXO'erne er bekymrede for, at kritiske systemer bliver utilgængelige i længere tid, hvilket er rekordhøjt.

Det digitale trusselsbillede

I dette afsnit får du indblik i det digitale trusselsbillede, som både danske og globale virksomheder står overfor. Du får en indsigt i, hvordan den digitale udvikling skaber en række muligheder og trusler, og hvem de cyberkriminelle er, hvad de går efter og hvordan.

Digitalisering i form af fx IoT, Industri 4.0, hjemmearbejde og den voldsomme vækst i antallet af forbundne enheder i samfundet øger væksten og innovationen, men øger også risikoen for, at virksomheder udsættes for angreb fra cyberkriminelle. Og sårbarheden understreges yderligere af, at hver enkelt virksomhed også er en del af et stort økosystem af digitale værdikæder. Det er derfor afgørende, at man som direktion og ledelse forstår ikke blot de digitale muligheder, men også de trusler, disse skaber for virksomheden.

Digitaliseringen tager fart i disse år. Flere og flere virksomheder bliver mere digitaliserede i deres forretning, og digitale løsninger understøtter i stigende grad forretningskritiske funktioner. En udvikling, der kun er styrket i kølvandet på situationen med COVID-19. Det gælder funktioner i både administration, økonomi, kommunikation, produktion og ikke mindst i de virksomheder, hvor produktet er digitalt. Det gælder også dér, hvor hele eller dele af virksomhedens it er outsourcet til en underleverandør.

Hver enkelt virksomhed er direkte forbundet til måske hundredvis af andre virksomheder i et erhvervsmæssigt økosystem, der rækker langt ud over matriklen, hvor data og informationer udveksles mellem parterne.

Dette økosystem medfører enorme vækstmuligheder, men betyder også, at virksomhederne er mere sårbare overfor cyberangreb end nogensinde før.

Hvor sikkerhed tidligere handlede om at sikre virksomheden fysisk, så har digitaliseringen betydet, at sikring er en langt mere kompleks størrelse. De cyberkriminelle kan sidde hvorsomhelst på kloden og begå alvorlig kriminalitet mod snart sagt enhver virksomhed.

Man er som virksomhedsledelse nødt til at sikre sin egen virksomhed og også stille sikkerhedsmæssige krav til de virksomheder, der indgår i virksomhedens økosystem.

Cyberangreb: Ikke et spørgsmål om hvis, men hvornår det sker

Som det fremgår af tallene fra PwC's Cybercrime Survey 2021 på foregående side, så er det ikke længere et spørgsmål om, hvorvidt der sker et cyberangreb mod virksomheden, men hvornår det sker.

Det er en illusion at tro, at man helt kan undgå cyberangreb, men med den rette viden, de rette teknologiske valg og en god sikkerhedskultur kan man minimere risikoen for at blive ramt af et cyberangreb. Og man kan desuden forberede organisationen på, hvordan man håndterer en hændelse og derved reducerer konsekvenserne af angrebet.

Hvem er de cyberkriminelle?

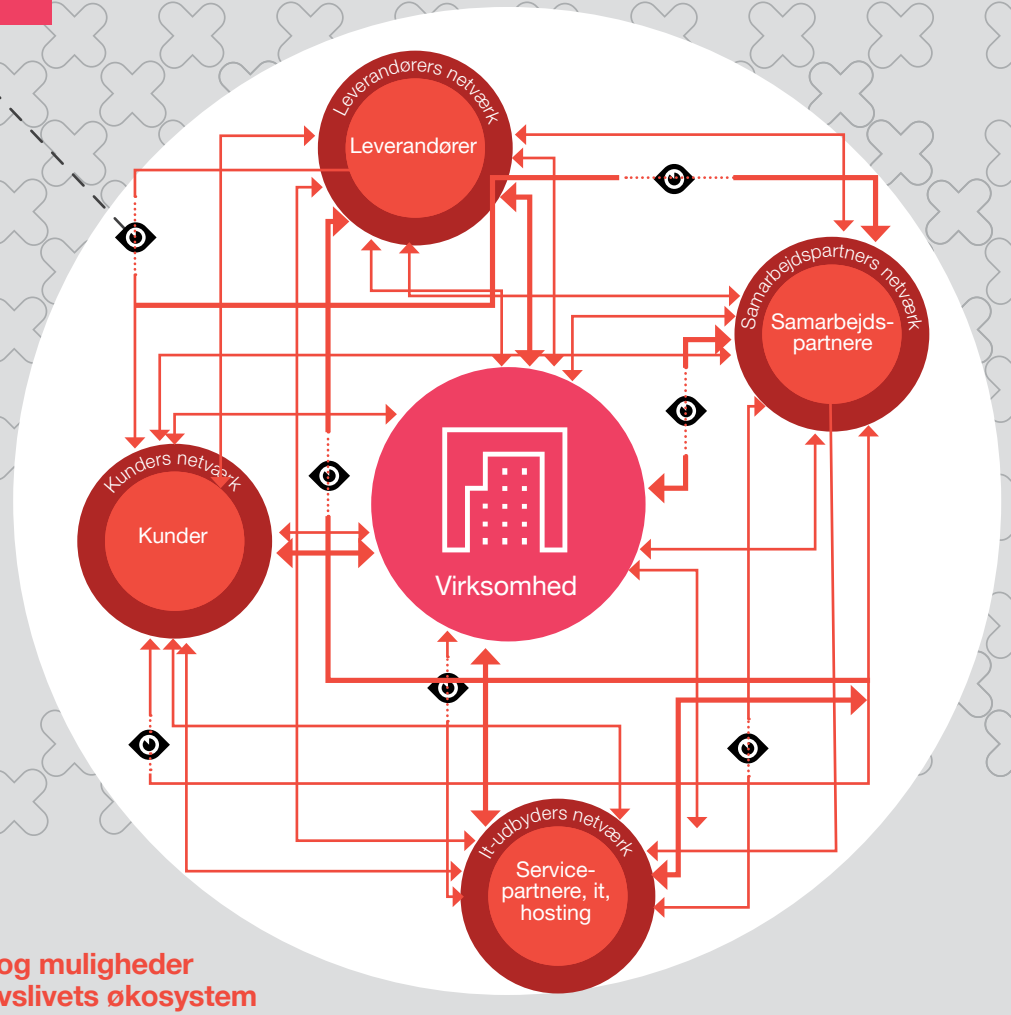
Angriberne er oftest organiserede kriminelle, der har økonomiske motiver. Der er dog også andre cyberkriminelle med andre motiver.

Såkaldte hacktivister opererer af idealistiske hensyn og forsøger fx at skabe en politisk eller adfærdsmæssig forandring i samfundet. Derudover kan nationalstater stå bag angreb mod danske virksomheder. Disse investerer store midler i bl.a. at stjæle viden og information, der kan styrke den pågældende nations konkurrenceevne.

Erhvervslivets økosystem

Organiserede kriminelle

De fleste angreb bliver udført af organiserede kriminelle. De er specialiserede i at udnytte svagheder i virksomheders digitale netværk, stjæle informationer eller gennemføre ransomware-angreb med økonomisk vinding som resultat.



Trusler og muligheder i erhvervslivets økosystem

Den øgede digitalisering medvirker til, at virksomheder i stigende grad indgår i digitale økosystemer, der kan skabe vækst og nye muligheder. Virksomheder udveksler data og har digitale integrationer, der gør det muligt at kommunikere, sælge og levere ydelser effektivt i økosystemet. Det samme digitale netværk gør dog i en vis udstrækning også livet lettere for kriminelle og skaber øget sårbarhed.

Cyberkriminelle udnytter de svageste led i det digitale netværk, og det kan koste dyrt for både den enkelte virksomhed, der bliver ramt, men i høj grad også de virksomheder, der er i netværk med den pågældende virksomhed. Derfor er det vigtigt, at virksomheden kender sit økosystem og sikrer, at kritiske data er beskyttet tilstrækkeligt, uanset hvor i økosystemet de behandles.

Top 5: **De største trusler**[1]

Phishing (78 %)

Hændelser forårsaget af leverandørfejl (35 %)

Malware (vira, orme eller anden ondsindt kode) introduceret i virksomheden (32 %)

Finansiel svindel (CEO-svindel, kreditkortsvindel, ulovlige banktransaktioner mv.) rettet mod netop din virksomhed (28 %)

Social engineering (27 %)

Kilde: PwC's Cybercrime Survey 2021

1 "Hvilke hændelser har din virksomhed oplevet i de seneste 12 måneder som resultat af cyberkriminalitet eller informationssikkerhedshændelser?"

Den menneskelige faktor spiller en stor rolle

De cyberkriminelle arbejder med metoder, der er designet til at udnytte virksomhedernes sårbarheder på alle måder. Det gælder særligt at finde svagheder i de teknologiske systemer, men de ved også af erfaring, at menneskets fejlbarlighed er en væsentlig sårbarhed i alle virksomheder. Medarbejdere på alle niveauer er derfor i stigende grad mål for cyberkriminelle, der kun bliver dygtigere til at udnytte den menneskelige svaghed bl.a. ved brug af phishingmails, der kan lokke medarbejderen til at åbne en bagdør, der gør det muligt for angriberen at infiltrere virksomhedens systemer eller sprede ondsindet kode.

I PwC's Cybercrime Survey 2021 svarer mere end hver anden, at deres virksomhed har været udsat for mindst én sikkerhedshændelse inden for den seneste regnskabsperiode. Undersøgelsen viser desuden, at virksomhederne er fortsat bekymrede for cybertruslen, og mere end halvdelen (54 %) svarer i 2021, at de er mere bekymrede for cybertruslen i dag, end de var for 12 måneder siden.

Typiske hændelser

Hvad er phishing?

Cyberkriminelle kompromitterer virksomheder ved at sende mails og lokke modtagerne til at klikke på et "ondsindet link". Dette link kan enten "fiske" efter at brugeren udleverer sensitive data, fx brugernavn og password eller kan downloade ondsindet kode, fx ransomware.

Hvad er CEO fraud?

Cyberkriminelle forsøger gennem falske mails at narre medarbejdere til fx at betale falske fakturaer eller overføre et beløb til en specifik konto. De cyberkriminelle udgiver sig for at være en ledende medarbejder, CEO eller CFO, og sender mails, der kommer fra dennes emailkonto. Avancerede angreb kopierer lederens mail-vaner og sprogbrug samt opsnapper eventuelle spørgsmål og svarer på vegne af lederen.

Hvad er ransomware?

Ransomware består af ondsindet kode, der krypterer virksomhedens data. De cyberkriminelle afpresser efterfølgende virksomheden til at betale en løsesum, oftest i Bitcoins, til at få adgang til egne data igen.

Trusselsaktør:
Organiserede cyberkriminelle

Motiv

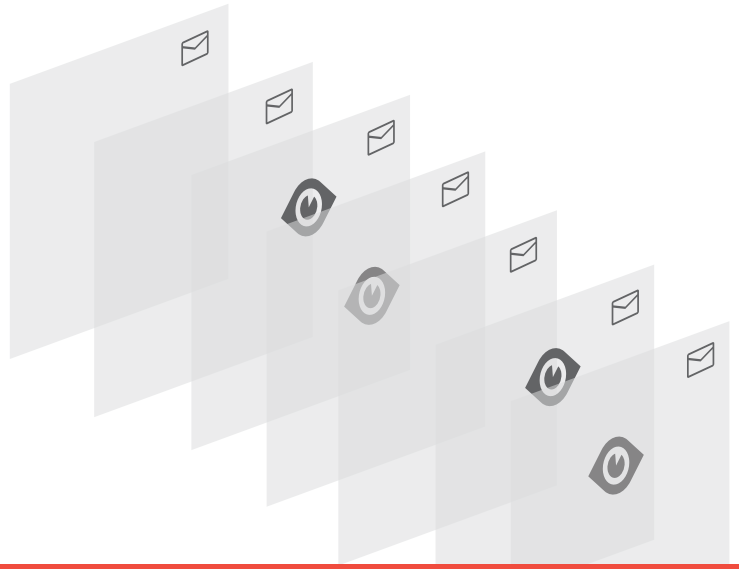
+ Søger typisk kortsigtet økonomisk gevinst.
+ Indsamling af information til fremtidige økonomiske gevinster.

Konsekvens

+ Kompromittering af virksomheden og dens netværk.
+ Akut nedlukning af drift.
+ Direkte tab af omsætning.
+ Tab af penge.
+ Tab af tillid og risiko for yderligere tab af omsætning.
+ Mulig tab af konkurrenceevne.

Medarbejdere:
Den menneskelige faktor

+ Menneskelige fejl er ganske ofte årsag til, at cyberkriminelle får held med et hackerangreb. Cyberkriminelle er eksperter i at lokke medarbejdere til at begå fejl, som kan kompromittere virksomheden og det netværk, den indgår i.
+ Løbende træning og uddannelse af medarbejderne kan medvirke til at opbygge en sikkerhedskultur og dermed reducere sårbarheden.



Case: **Cyberangreb har store omkostninger**

En mellemstor dansk produktionsvirksomhed med en stor kundegruppe i sit digitale netværk oplevede for nylig at være den direkte årsag til, at flere kunder blev kompromitteret med phishingmails på grund af virksomhedens manglende sikkerhed.

En hacker har skaffet sig adgang til virksomhedens mailsystem og har i længere tid monitoreret mailboksen. Hackeren begynder at sende ransomware med virksomheden som afsender ud til kunder og kontakter, der ser ud til at indeholde relevant og væsentlig information. Nogle af kunderne undrer sig og spørger, om det kan være rigtigt, at de mails kommer fra den pågældende virksomhed. Hackeren opsnapper disse mails og bekræfter på vegne af virksomheden, at den er fra dem. Flere af virksomhedens kunder og kontakter klikker på linket med det resultat, at de får krypteret og låst deres systemer. Efterfølgende kan de være nødt til at betale løsesum, eller bruge tid og penge på at genetablere systemer og data (back-up). Uanset hvad så lider de et tab.

Den direkte konsekvens er, at denne virksomhed – pga. manglende sikkerhedsforanstaltninger – er årsag til, at vigtige kunder og kontakter lider tab. Den afledte konsekvens er det tillidsbrud, der sker fra de pågældende kunder og kontakter i relation til produktionsvirksomheden.

Erfaringer fra PwC Danmarks Incident Response Team

Opsummering: **Det digitale trusselsbillede**

- Den øgede digitalisering skaber nye muligheder, men også øget sårbarhed.
- Det er ikke et spørgsmål om hvis, men hvornår virksomheden rammes af cyberangreb.
- Cyberkriminelle er eksperter i at få medarbejderne til at begå fejl, der lukker den kriminelle ind i virksomheden.
- Teknologiske valg er afgørende for cybersikkerheden.
- Cyberkriminelle er ofte organiserede kriminelle, der motiveres af økonomi. De er professionelle, og de benytter avancerede metoder til at udnytte kendte svagheder.

Forslag: **Sådan kommer du videre**

- Få et overblik over virksomhedens økosystem. Hvem samarbejder vi med, og hvilke data udveksler vi med hinanden og hvordan?
- Få en uvildig validering af organisationens faktiske sikkerhedsniveau, bl.a. gennem sikkerhedstest.
- Søg svar på, om I har det fornødne kendskab til de risici, der er ved et cyberangreb.

CFO’ens centrale rolle

I dette kapitel får du en forståelse for CFO’ens centrale rolle i arbejdet med cybersikkerhed. Du får indblik i, hvorfor CFO’en besidder denne afgørende rolle, samt hvorfor cybersikkerhed i dag er en essentiel del af virksomhedens samlede risikostyring.

Den stigende digitalisering betyder, at cybersikkerhed flytter højere op på agendaen i virksomhedens ledelse, da det i høj grad omfatter virksomhedens økonomi og forretningsgrundlag. Som ansvarlig for virksomhedens finansielle sikkerhed og risikostyring, er det naturligt CFO’ens opgave at spille en væsentlig rolle i at lægge virksomhedens cybersikkerhedsstrategi.

CFO’en har en helt unik position i forhold til at håndtere cyberrisici. Cybersikkerhed er meget mere end blot et spørgsmål om hardware og software. Cybersikkerhed medvirker til, at omverdenen kan have tillid til virksomheden, hvorfor det er et strategisk spørgsmål, der i stigende der i stigende grad bør varetages af virksomhedens øverste ledelse, og her er CFO’en den naturlige ansvarsperson. CFO’en kender således virksomhedens overordnede strategi, forretning, økonomi og aktiver.

CFO’en har desuden et generelt kendskab til regulatoriske krav og ikke mindst en fornemmelse for virksomhedens omdømme og troværdighed hos samarbejdspartnere. Og som ansvarlig for risikostyring i virksomheden er det også CFO’ens rolle at sikre, at virksomheden løbende har styr på konkrete risici og sammenholder dem med virksomhedens risikovillighed. Dette gælder også de risici, der er relateret til cybertruslen.

Det er CFO’ens rolle at sørge for, at der er etableret en handlingsplan for cybersikkerhed, og at der er etableret systemer for rapportering og håndtering af risici, samt et beredskab, der kan håndtere en cyber- eller it-relateret hændelse.

CFO’ens mange interessenter

CFO’en er ikke alene om at udarbejde virksomhedens cyberstrategi. Til at hjælpe med arbejdet har hun/han en række vigtige interessenter. Det gælder både internt og eksternt.

Interne interessenter

En af de væsentlige interne interessenter er bestyrelsen. CFO’ens opgave er at forsyne bestyrelsen med afgørende information, der kan danne grundlag for bestyrelsens og ledelsens prioritering af cybersikkerhed. Senere i denne guide (side 34) kommer vi nærmere ind på, hvordan CFO’en med fordel kan styrke samarbejdet med bestyrelsen gennem løbende dialog om virksomhedens arbejde med cybersikkerhed.

Det daglige arbejde med at udvikle og fastlægge en cybersikkerhedsstrategi sker i samarbejde med kollegerne i direktionen og forretningsledelsen, herunder afdelingschefer for de centrale funktioner som salg, marketing, indkøb, produktion, it, HR osv. CFO’ens rolle er at facilitere, at de rette interne såvel som eksterne kompetencer sættes i spil og bidrager, når virksomhedens cyberstrategi skal udarbejdes og løbende evalueres. Med sin indsigt i forretningens mange aspekter bliver CFO’en bindeleddet mellem forretningen, medarbejderkulturen og virksomhedens tekniske forsvarskapacitet på området.

CFO'ens rolle i forhold til cybersikkerhed

Bestyrelse

- Har vi styr på cybersikkerhed?
- Hvad vil der ske, hvis vi bliver ramt? Hvad vil konsekvenserne være?
- Har vi et tilstrækkeligt beredskab?
- Investerer vi nok?

Hvordan sikrer jeg, at vi leverer den fornødne dokumentation og rapportering?

Eksterne interessenter

Kunder, leverandører og samarbejdspartnere

- Beskytter I vores informationer tilstrækkeligt?
- Hvordan skaber vi den fornødne tillid?
- Hvordan viser vi, at vi er en ansvarlig virksomhed?
- Kan vi have tillid til at samarbejde med jer?

CFO'ens opgaver i forhold til cybersikkerhed

- + Ansvar for risikostyring, herunder sikre forretningen mod negative konsekvenser ved eventuelt cyberangreb.
- + Rapportering til bestyrelse/revisionskomité om udvikling og opfølgning på cyber-sikkerhedsstrategi og risiko.
- + Sikre etablering af et passende cyberprogram, der adresserer virksomhedens risici samt eksterne krav fra kunder eller myndigheder, fx GDPR.
- + Løbende overvåge effektiviteten af virksomhedens cyberprogram.

Interne interessenter

It-ansvarlig

- Vi har investeret i at opdatere vores it løbende
- Har vi et tilstrækkeligt sikkerhedsprogram?
- Er vi bekendt med den risiko, som vores leve-randører udgør?
- Vi har outsourcet vores it-drift til en anerkendt leverandør

Eksterne interessenter

Eftersom cybersikkerhedsniveauet både påvirker og påvirkes af virksomhedens omverden, er det vigtigt også at inddrage de eksterne interessenter i arbejdet med at forme virksomhedens cybersikkerhedstrategi. Det kan være kunder, underleverandører, myndigheder og andresamarbejdspartnere. CFO'en har gennem sit ansvar for risikostyring en naturlig dialog med kunder, leverandører og samarbejdspartnere, og derfor er det naturligt, at ansvaret for cybersikkerhed er placeret her.

+

Opsummering:
CFO'ens centrale rolle

+ Cybersikkerhed er et forretningsstrategisk vigtigt fokusområde, der bør prioriteres og placeres i ledelsen. CFO'en er det naturlige bindeled herfor.
+ En af de væsentlige interessenter er bestyrelsen som en vigtig sparringspartner på strategisk niveau. Andre interne interessenter inddrages tværorganisatorisk for at sikre en forretningsmæssig prioritering.
+ CFO'ens dialog med eksterne interessenter skal udvides til også at omfatte cybersikkerhed.
+ CFO'en bør forholde sig kritisk til, om den aktuelle indsats på cybersikkerhedsområdet er tilstrækkelig eller udelukkende har et teknisk fokus.

Forslag:
Sådan kommer du videre

+ Skab en systematisk og løbende rapportering i forhold til bestyrelsen omkring cyberrisikovurdering og fremdrift på planer for cybersikkerhed.
+ Inddrag bredt interne interessenter i forretningen/organisationen i arbejdet omkring udvikling og implementering af cyberstrategi og sikkerhedsprogram.
+ Inddrag eksterne interessenter, som kunder, leverandører og samarbejdspartnere , herunder også it-leverandører i udformningen og ikke mindst udmøntningen af cyberstrategien.

> Cyberkriminelle er eksperter i at lokke medarbejdere til at begå fejl, som kan føre til kompromitterering af virksomheden og de parter, der indgår i virksomhedens økosystem.

Det cyberstrategiske fundament

I dette afsnit får du en forståelse af, hvad det cyberstrategiske fundament indebærer. Her kommer vi tættere på, hvordan du sikrer virksomheden mod cyberhændelser. Vi giver dig et overblik over de væsentligste kompenenter på Sikkerhedsrejsen og de spørgsmål, du skal stille dig selv og din organisation på vej mod et bedre cyberforsvar og beredskab.

Den øgede trussel fra cyberkriminalitet betyder, at cyberstrategi er flyttet op på ledelsesagendaen. Samtidig betyder de mere og mere avancerede og intelligente metoder, der bliver taget i brug, at der er behov for en cyberstrategi, som omfatter og inddrager hele virksomheden. Det handler om at få styr på, hvad der skal beskyttes og hvordan.

En helt afgørende faktor for at opnå en stærk cybersikkerhed er erkendelsen af, at dette er en generel ledelsesopgave, som ikke bør isoleres til udelukkende at angå it-afdelingen.

I mange virksomheder begår man den fejl at tro, at cybersikkerhed udelukkende er et spørgsmål om it. Men cybersikkerhed handler om mange andre ting. Det handler om at forstå virksomhedens forretningsmæssige værdi og strategi. At forstå hvad der er afgørende for virksomhedens eksistens, samt hvordan man beskytter de aktiviteter og processer, der understøtter disse aktiver. Det er et stort – men værdiskabende – arbejde at få skabt et fundament for den cybersikkerhed, der vurderes nødvendig for virksomheden.

Denne guide fører dig igennem de fem indsatsområder, som understøtter et cyberstrategisk fundament i din virksomhed, som på den måde står bedre rustet mod de digitale trusler, I møder.

PAVA – et forståeligt sikkerhedskoncept

Vi introducerer PwC's PAVA-koncept på disse sider og refererer løbende til konceptet gennem denne guide.

PAVA-konceptet er et generisk kommunikations-, vurderings- og rapporteringskoncept, der illustrerer de indsatsområder, som er nødvendige for en holistisk tilgang til cyber- og informationssikkerhed. PAVA dækker over fem hovedområder – fra governance, risk og compliance til proces, adfærd, validering og arkitektur. Afhængig af den enkelte virksomheds risikoprofil og aktuelle modenhed, er der behov for en indsats inden for alle områder, for at opnå en langsigtet og robust cyber- og informationssikkerhed.

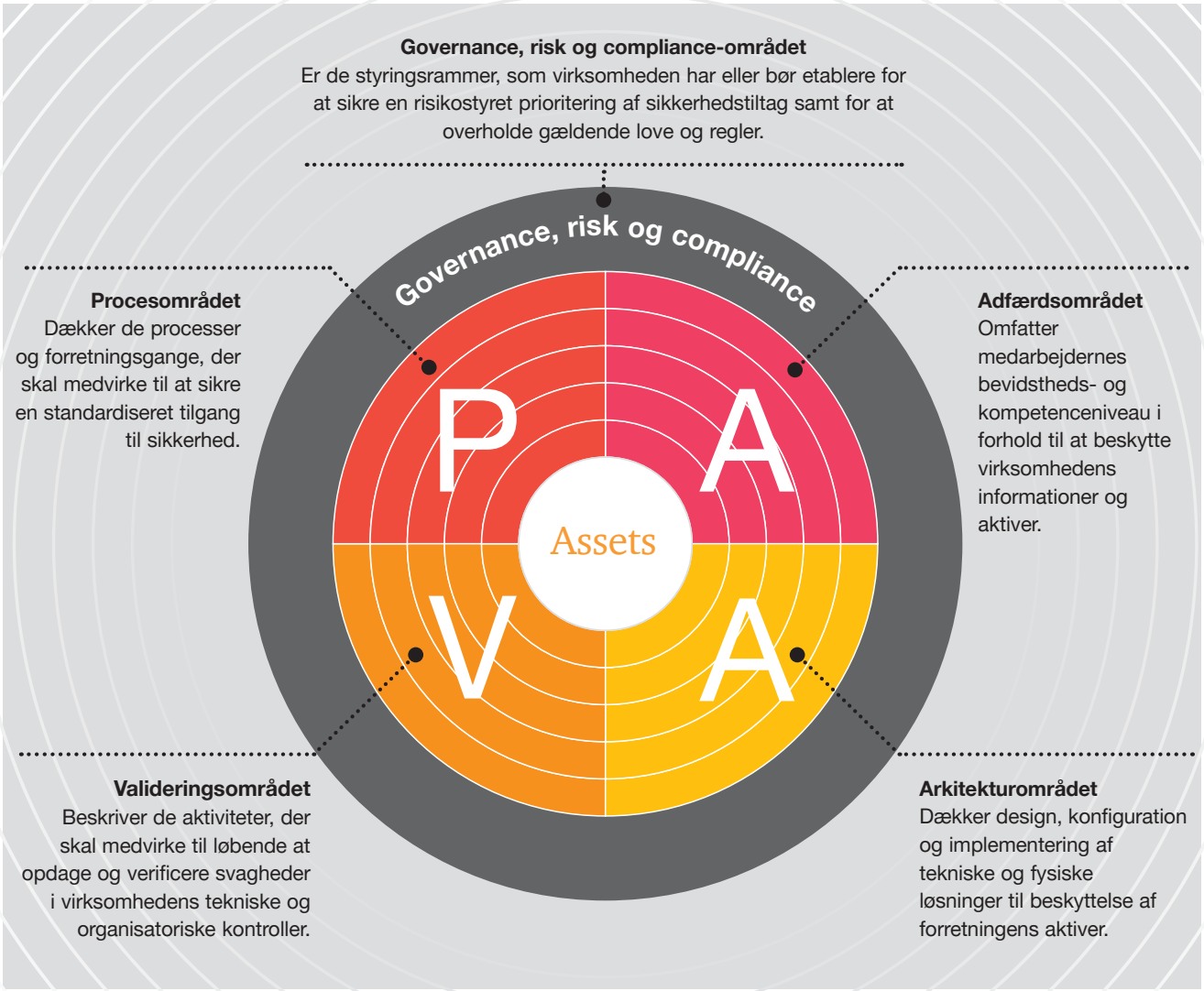
Vi vil i denne guide løbende referere de anbefalede indsatser til områderne i PAVA-modellen med henblik på at illustrere den nødvendige indsats, der kræves for at have en tilstrækkelig tilgang til cyber- og informationssikkerhed.

Sikkerhedsrejsen

Første skridt på din virksomheds sikkerhedsrejse er at få styr på, hvad der ud fra et forretningsmæssigt perspektiv er virksomhedens vigtigste aktiver, og hvad der er det væsentlige at beskytte. Cybersikkerhed handler desuden om at kende det digitale trusselsbillede og heraf kunne udlede de risici, virksomheden løber. Og når man kender disse risici, skal man holde disse op mod den risiko, man er villig til at løbe. Man skal naturligvis også kende virksomhedens aktuelle teknologiske modenhedsniveau, så man forstår sit udgangspunkt og kan tage stilling til, hvor man gerne vil hen.

En fundamental del af en stærk cyberstrategi handler om virksomhedens teknologiske valg. Her skaber CFO'en et overblik over det teknologiske set-up og diskuterer løsninger med virksomhedens teknologisk ansvarlige. Det kræver, at man har overblik over virksomhedens økosystem.

PAVA – et forståeligt sikkerhedskoncept



+

Husk at mobilisere ledelsen bredt:

Det er vigtigt at involvere og mobilisere bredt fra start. Skaf opbakning og input fra alle relevante afdelinger.

- + Produktion.
- + Indkøb og logistik.
- + Salg- og marketing.
- + HR.
- + Økonomi- og regnskab.
- + It-afdelingen.

Virksomheden skal lave et grundigt eftersyn på, hvad der er outsourcet, og hvad virksomheden selv driver. CFO'en er ansvarlig for at skabe overblik over, om teknologivalgene lever op til de nødvendige sikkerhedskrav.

I det store arbejde med at sikre virksomheden mod cyberangreb, ligger der desuden en opgave i at få overblik over de politikker og processer, der danner grundlag for, hvem der har adgang til hvilke data og it-systemer i virksomheden. Det er ikke ualmindeligt, at den såkaldte netværkssegmentering er mangelfuld eller ikke-eksisterende i mange virksomheder. Det vil sige, at hvis en cyberkriminel skulle få held til at hacke sig ind på blot en enkelt bruger i virksomheden, så har vedkommende adgang til alle systemer og al data i virksomheden.

Sikkerhedsrejsen

Her er du nu

Kend dine vigtigste aktiver

Hvad er virksomhedens vigtigste aktiver? Hvad er vigtigst at beskytte i tilfælde af et cyberangreb?

- Få styr på teknologien
- Håndtering af brugere og adgange
- Beredskabsplanlægning
- Skab en sikkerhedskultur

Jo flere, der har adgang til virksomhedens systemer, og jo mere de har adgang til, desto større er risikoen for kompromitterende hændelser.

Hvem har adgang til hvilke systemer og hvorfor?
Svarene på ovenstående findes i samarbejde med virksomhedens it-ansvarlige og evt. it-servicepartnere. I arbejdet får CFO'en overblik over virksomhedens politikker på området, om de bliver overholdt, og om de skal opdateres.

Virksomhedens evne til at klare sig igennem et cyberangreb og hurtigt rejse sig igen er afgørende. Ledelsen skal sikre, at man håndterer et cyberangreb effektivt, herunder genopretter virksomhedens systemer og data med mindst mulig negativ konsekvens for forretningen. En af de væsentligste forudsætninger for at kunne det er, at have styr på beredskab og krisestyring. Spørgsmål i den forbindelse er:

Har virksomheden beredskabsplaner; er der en klar ansvarsfordeling og opgavebeskrivelse; kender nøglemedarbejderne til planerne, og er der backupsystemer? CFO'en skal have et klart overblik over, hvad der skal ske inden for de første 24 timer – og derefter.

Cybersikkerhed handler også om evnen til på tværs af organisationen at skabe en medarbejderkultur, der forstår risikoen og problematikkerne, og agerer derefter. Dette vil samtidig danne grundlag for en kultur i organisationen båret af klarhed og åbenhed.

Mens medarbejdere er en af de største risikofaktorer, er de også det bedste våben mod de cyberkriminelle.

Jo mere opmærksomme og oplyste medarbejdere og ledelse er, des bedre er forsvaret mod cyberangreb. Fokus er på vidensniveau i organisationen og den adfærd, der er i virksomheden. Det drejer sig om at iværksætte planer for løbende kommunikation og om uddannelse, test og evaluering af medarbejdernes kapaciteter.

Mobilisering af ledelsen
Sikkerhedsrejsen starter bedst ved at mobilisere ledelsen, som i fællesskab identificerer virksomhedens vigtigste aktiver.

For at lykkes med at flytte virksomheden fra hvor man er i dag til, hvor man gerne vil være, kræver det, at processen er solidt forankret i ledelsen. Det er en opgave, der kræver involvering af de personer i virksomheden, der repræsenterer de væsentligste

Hvordan er det teknologiske forsvar? Passer det med de identificerede trusler og risici? Hvad er behovet for yderligere sikring?

Hvordan er processerne for, hvem der har adgang til hvad og hvorfor? Overholdes disse? Er der behov for opdatering?

Hvordan er processerne for hændelseshåndtering? Er der it-beredskab for genetablering efter kompromittering? Har vi planer for krisehåndtering og forretningsnødplaner?

Involvering af organisationer er afgørende. Strategien for cybersikkerhed skal kommunikeres ud til alle medarbejdere.

Sæt jer et mål for sikkerhedsrejsen

Handlingsplan

Vi vil have overblik over vores vigtigste aktiver, teknologivalg, håndtering af brugere og adgange, beredskabsplanlægning og sikkerhedskultur

afdelinger og funktioner. Jeres virksomheds specifikke forretningsledelse afgør selvfølgelig, hvem der er mest relevant at inddrage.

Den første opgave er at få overblik over den nuværende situation. Derefter drejer det sig om fremtidens ønskescenarie: Hvor vil vi hen, og hvor langt er der fra tilstanden, som den er, og til hvor den gerne skulle være? Det afstemmes i forhold til ledelsen, vision og budget. Ledelsen prioriterer herefter handlingspunkter og ambitionsniveau og søsætter en handlingsplan, der retter sig mod implementering af såvel teknologi, som etableringen af en sikkerhedskultur.

+

Opsummering:
Det cyberstrategiske fundament

Mange mener, at cybersikkerhed primært er it-afdelingens ansvar, men hovedbudskabet er, at cybersikkerhed er en central problemstilling for ledelsen. Det er forretningen, der bliver påvirket af et cyberangreb, og derfor er det et forretningsmæssigt ansvar at få styr på sikkerheden, baseret på en tværorganisatorisk indsats orkestreret af CFO'en.

Forslag: **Sådan kommer du videre**

+ Skab overblik ved at mobilisere forretningen og dens ledelse. Skab fælles forståelse for det digitale trusselsbillede og konsekvenserne for forretningen ved et cyberangreb.
+ Afstem et fælles billede af de vigtigste aktiver, der skal beskyttes (kronjuvelerne).
+ Identificér et fælles fremtidigt billede af, hvor I gerne vil stå sikkerhedsmæssigt og hvilket niveau af risici, I er villige til at acceptere.
+ Igangsæt og investér i et sikkerhedsprogram og en sikkerhedsrejse, der har fokus på de væsentligste bestanddele, såsom teknologivalg, brugerstyring, sikkerhedskultur mv.

Få styr på virksomhedens vigtigste aktiver

For at udarbejde sin cybersikkerheds-strategi må man nødvendigvis vide, hvad man skal beskytte. Når man tager kompleksiteten af virksomheden i betragtning og forstår virksomhedens økosystem, så er det ikke muligt at beskytte alle dele af forretningen på samme niveau. Vi giver nogle pejlemærker for, hvordan man bruger trusselsbilledet til at foretage en risikoanalyse og identificere de aktiver, der er mest kritiske for virksomheden. Formålet er at skabe en klar og fælles forståelse for, hvad der er det vigtigste at beskytte for senere at kunne prioritere indsatsen.

De vigtigste aktiver

Pas på kronjuvelerne

I en verden, hvor cyberkriminalitet i stigende grad er en del af risikobilledet, er det afgørende, at ledelsen har en fælles forståelse for, hvad der er så kritisk et aktiv for virksomheden, at en kompromittering vil udgøre en risiko for virksomhedens eksistens. For kun gennem den erkendelse kan man beskytte virksomheden optimalt mod cyberkriminalitet.

Når man skal beskytte virksomheden mod cyberangreb, så kan det være frugtbart allerførst at konstatere, at man ikke kan beskytte hele virksomheden lige godt. Deri ligger nemlig en vigtig erkendelse af, at der er noget, der er vigtigere at beskytte end andet.

Et andet afgørende element er at fokusere på den værdiskabelse, der ligger i forretningen – altså hvordan forretningen skaber værdi. Fra det udgangspunkt kan man afgøre, hvilke kritiske processer i virksomheden, der er nødvendige for at skabe værdi. Dernæst, hvilke data og it-systemer, der er nødvendige for at skabe den pågældende værdi. Og til sidst fokusere på den grundlæggende it-infrastruktur.

Et af de væsentlige spørgsmål, man kan stille sig selv, når det drejer sig om cybersikkerhed er: "Hvad er det allervigtigste for os at beskytte?" Hvad er virksomhedens mest værdiskabende aktiver? Det er afgørende for den fremtidige strategi for cybersikkerhed, at der er en fælles forståelse i virksomheden omkring disse spørgsmål. Kender man ikke de vigtigste aktiver, kan man ikke prioritere sikkerhedsindsatsen og virksomheden udsættes for en potentiel og unødig trussel mod virksomhedens eksistens, eller man investerer i sikkerhedsinitiativer, der ikke giver det ønskede udbytte.

Der er mange metoder til at skabe det nødvendige overblik over virksomhedens aktiver. En af de metoder, der kan bringes i spil, er at foretage en indledende workshop, hvor relevante ledende medarbejdere deltager (se foregående afsnit). Fordelen ved workshoppen er, at man kan samle de rigtige personer, og alle kan komme med input. Derudover, at man får et fælles udgangspunkt, der kan sætte den fremadrettede proces i gang.

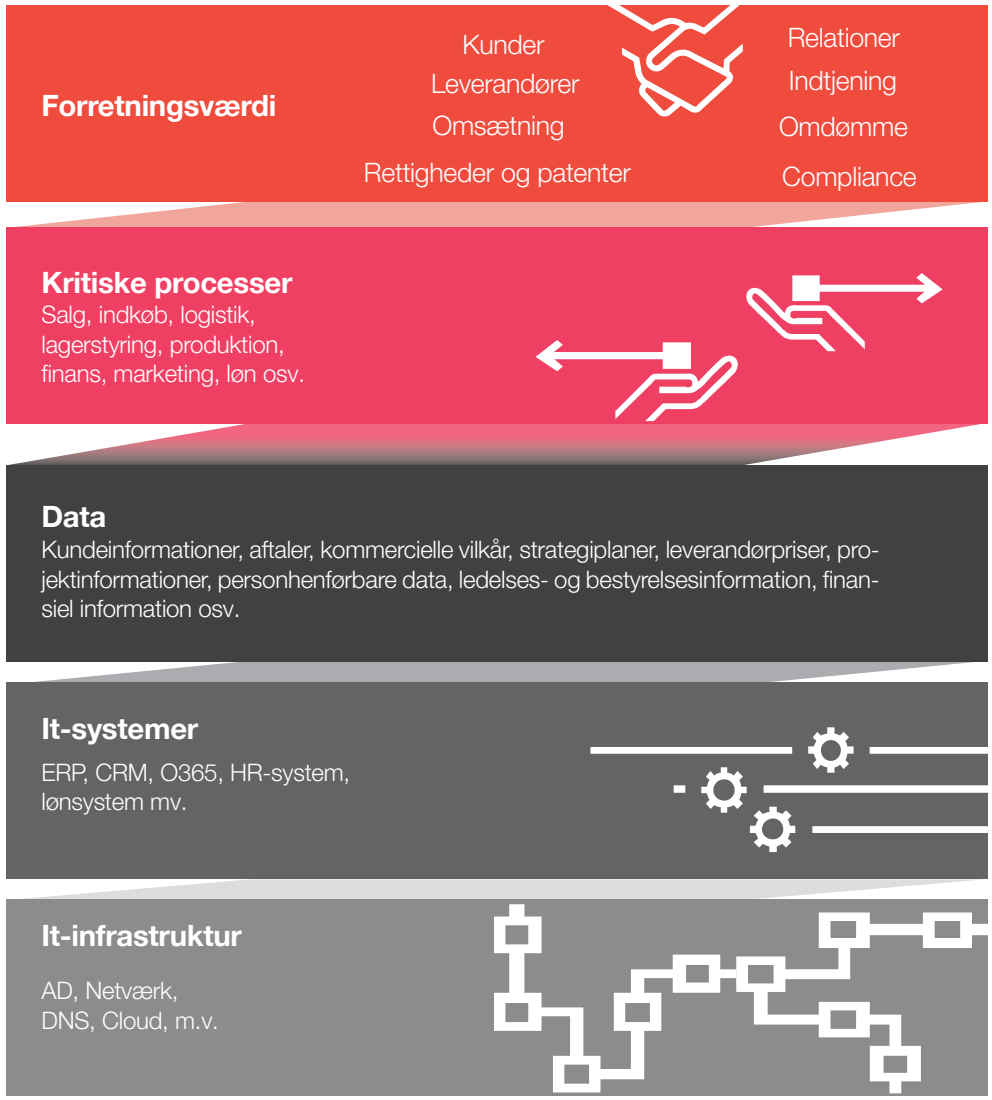
Assets
Identifikation og klassificering af virksomhedens kritiske aktiver (assets) er centralt for sikkerheds-arbejdet. Indsigten giver mulighed for at målrette sikkerhedsindsatsen på basis af forretningsrisikoen.

Governance, risk og compliance-området
Sikkerhed bør være en ledelses-prioritet, og involverer hele forretningen. PAVA's fokus på Governance, risk og compliance skal medvirke til, at roller og ansvar er etableret, så beslutninger kan foretages på basis af forretningskritikalitet såvel som overholdelse af lovgivning.

Workshoppen skal give en fælles forståelse for:

- De værste scenarier for virksomhedens eksistens.
- Virksomhedens 'økosystem'.
- Trusselsbilledet generelt.
- Virksomhedens sårbarhed og risikoprofil.
- Fælles viden om risikostyring og den tænkning, der skal føre til en ny sikkerhedskultur og en cyber-strategi i virksomheden.

Tilsammen udgør ovenstående elementer en risikoanalyse, der danner grundlaget for, hvad der er vigtigst at beskytte, og hvor indsatsen skal prioriteres.



Virksomhedens forretningsmæssige værdi ligger i det øverste lag. Det er de kritiske processer, der sikrer, at virksomheden kan skabe den fornødne forretningsmæssige værdi. Disse kritiske processer understøttes og sikres af data, it-systemer og it-infrastruktur.

Case: Værdi i servicevirksomhed

Service til forsyningssektoren

Servicevirksomheden leverer tekniske serviceydelser til forsyningssektoren. Kunderne er afhængige af virksomhedens service. Det er servicevirksomhedens forretningsværdi.

De kritiske processer er de processer, der understøtter forretningsværdien.

I forbindelse med virksomhedens gennemgang af cybersikkerhed og -beredskab skal sikkerhedsniveauet gennemgåes. Med henblik på at evaluere det nuværende sikkerhedsniveau foretager forretningsledelsen i virksomheden en trussels- og risikovurdering for at identificere de mest kritiske aktiver.

Ved at vurdere de enkelte forretningsområder, finder de, at løsningerne, der understøtter serviceforretningen, udgør den største risiko, set fra et cyber- og it-perspektiv. Virksomheden modtager realtids-data via en specialiseret løsning, der overvåger kundens it-miljø. Teknikkerne kan derved servicere kunden effektivt og registrere tid og materialeforbrug i samme løsning.

Ledelsen vurderer, at et brud på tilgængelighed eller tab af kunders data i denne løsning ikke blot vil have stor påvirkning af omsætningen på kort sigt, men potentielt også have negativ konsekvens for virksomhedens omdømme og tab af kunder på længere sigt.

Sammen med it-afdelingen og virksomhedens leverandører evalueres den nuværende infrastruktur, og der implementeres bl.a. en ny cloud-baseret løsning til at beskytte mod datatab og manglende tilgængelighed af systemet, og beskyttelsen af teknikernes bærbare computere øges.

Erfaringer fra PwC Danmarks Incident Response Team

Spørg jer selv "Hvad er det værste, der kan ske for virksomheden?". Det positive ved netop dette spørgsmål er, at alle bør kunne forholde sig til det. Der vil med sikkerhed komme mange forskellige svar, og her er det CFO'ens rolle at sikre, at gruppen diskuterer ud fra et forretningsmæssigt perspektiv. Og at man ud fra de 'worst case' scenarier, der kommer på banen, hele tiden fokuserer på, hvor kritisk en given hændelse vil være for virksomhedens eksistens.

Det kan være en hjælp at diskutere sandsynligheden og de potentielle konsekvenser for forretningen ved en hændelse. Inddrag især it-afdelingen i dialogen. I denne dialog er det afgørende at udfordre forestillingen om, at der er styr på situationen ved bl.a. at bede om dokumentation for "at der er styr på det".

+ Inspiration til spørgsmål til alle i ledelsen:

1. Forstår vi det digitale trusselsbillede – hvad kan der ske for os/imod os? Forstår vi, hvordan en ondsindet aktør vil kunne kompromittere vores forretning?
2. Forstår vi, hvad det er vigtigst for os at beskytte?
3. Forstår vi konsekvenserne ved en kompromittering – kender vi virksomhedens risikoprofil?

Benyt eventuelt disse underspørgsmål i processen:

+ Fortrolighed:
  - Hvad sker der, hvis vi får brud på fortrolighed – fx hvis information relateret til IP-rettigheder, bestyrelses- og ledelseskommunikation, eller andet kommer i de forkerte hænder?
+ Integritet:
  - Hvad sker der, hvis vi får brud på vores værdikæde – fx hvis kontooplysninger ændres på en faktura, og vi fejlagtigt betaler til kriminelle?
+ Tilgængelighed:
  - Hvad sker der, hvis vi ikke har adgang til kritiske systemer, data mv. i en kortere eller længere periode og dermed ikke kan producere eller opfylde kundeforpligtelser?
+ Non-compliance:
  - Hvad sker der, hvis vi ikke kan overholde gældende lovgivning og får bøde eller et forbud for at udføre vores forretning?

4. Hvad gør vi for at imødekomme disse risici?

+ Scenarier: **Det værste, der kan ske?**

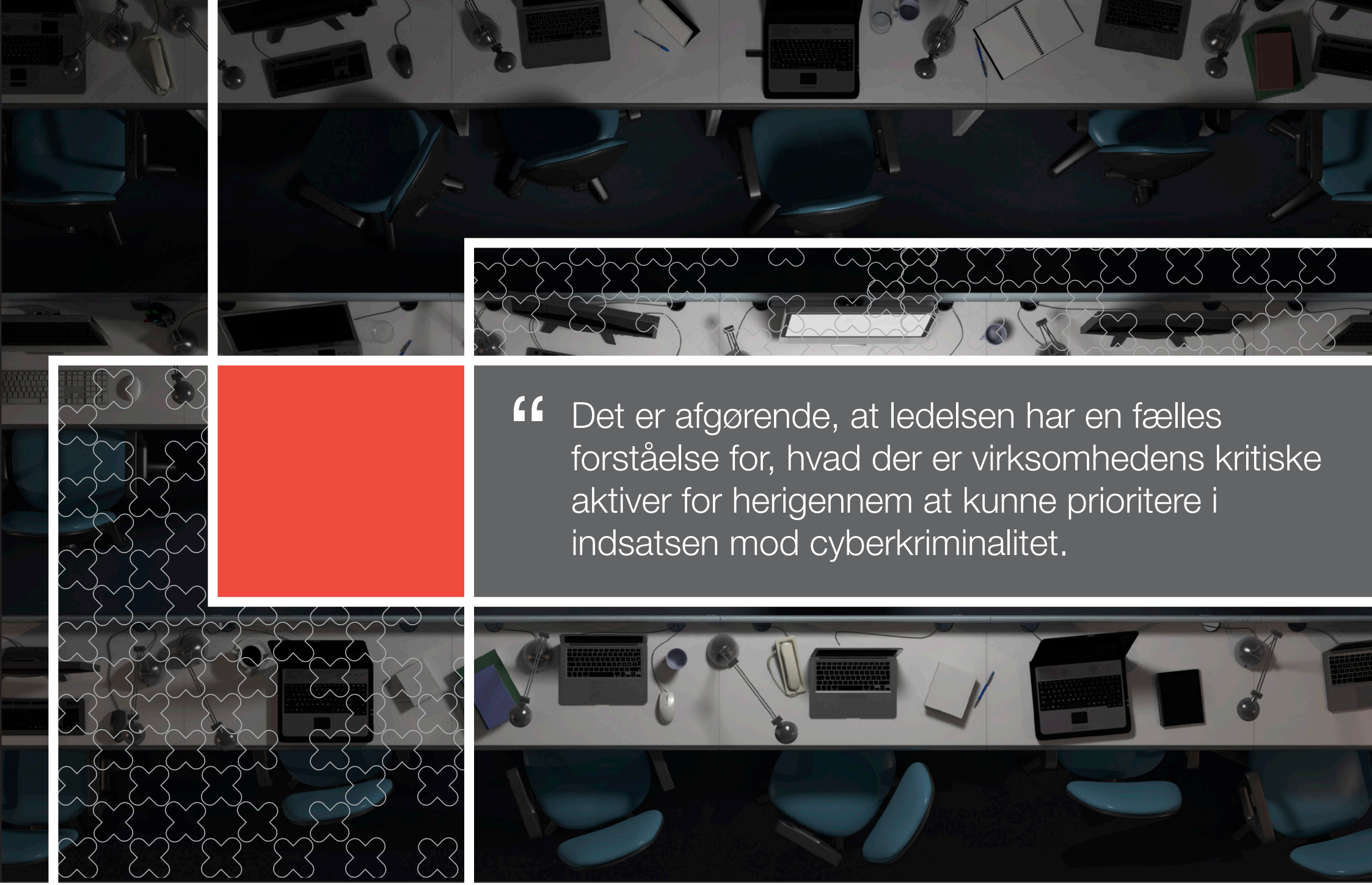
+ For virksomheder med høj priskonkurrence er det afgørende at beskytte informationer omkring eksempelvis prisaftaler og detaljerede kalkuler på produktionsomkostninger. Hvis konkurrenterne kender priser og kalkuler, så mister virksomheden en væsentlig fordel.
+ Virksomheder, der er baseret på onlinesalg er afhængige af at være tilgængelig online -eller oppetid. Hvis kunderne ikke har adgang til hjemmesiden, så sælger virksomheden ingen produkter.
+ Forskningstunge virksomheders kritiske aktiver er eksempelvis den forskning, der ligger bag produkterne. Hvis konkurrenter får adgang til forskning, opskrifter osv., så mister virksomheden sin konkurrencefordel.

+ Opsummering: **De vigtigste aktiver**

+ Cybersikkerhed handler om at sikre forretningens væsentligste aktiver. Med CFO'en som central figur er det den samlede ledelses opgave at skabe en fælles forståelse for virksomhedens mest forretningskritiske aktiver. Ledelsen skal finde svaret på, hvad der er det værste, der kan ske i tilfælde af et cyberangreb.

Forslag: **Sådan kommer du videre**

+ Saml ledelsen i en workshop med fokus på det digitale trusselsbillede.
+ Fokusér på hvilke dele af forretningen, der er mest kritisk at beskytte.
+ Formulér hvad der er det værste, der kan ske, og hvilke konsekvenser et cyberangreb vil have for forretningen.
+ Skab forståelse for hvilke data, it-systemer og it-infrastruktur, der er involveret heri.



> “ Det er afgørende, at ledelsen har en fælles forståelse for, hvad der er virksomhedens kritiske aktiver for herigennem at kunne prioritere i indsatsen mod cyberkriminalitet.

Teknologivalg

Her tager vi fat på det teknologiske setup i virksomheden. Du får en række gode råd til, hvordan I bedst skaber overblik over nuværende teknologiske forsvar, samt hvordan I holder det eksisterende forsvar op mod trusselsbilledet og konkretiserer behovet for yderligere sikring. Alt dette med det formål at prioritere investeringer i et teknologisk forsvar for virksomhedens sårbare aktiver.

Teknologi og teknologivalg

Få styr på teknologien – inhouse og eksternt

Karakteren af virksomhedens teknologiske infrastruktur og setup er en afgørende faktor for virksomhedens cyber-sikkerhedsniveau. Cyberkriminelle udnytter sårbarheder i virksomheders systemer og infrastruktur, og derfor er det afgørende, at ledelsen foretager teknologivalg, der beskytter virksomheden optimalt mod cyberkriminalitet.

Det er meget vigtigt at understrege, at cybersikkerhed ikke kun handler om virksomhedens software og hardware, men ikke desto mindre er netop det teknologiske forsvar en helt afgørende faktor for cybersikkerheden.

De teknologiske valg, man foretager i virksomheden, er som følge heraf determinerende for, hvordan virksomheden står rustet mod cyberhændelser og konsekvenserne heraf.

Det er helt naturligt, at CFO'en og ledelsen foretager en grundig analyse af det teknologiske setup som en del af hele processen omkring det cyberstrategiske fundament.

Målet er at kende svaret på, hvad der kendetegner det nuværende teknologiske setup, og hvilke teknologiske valg, der er taget hidtil. Og på den baggrund skal virksomheden finde ud af, hvilke valg der fremadrettet skal tages for bedst muligt at beskytte de kritiske aktiver, der er blevet identificeret.

Her skal det bl.a. afgøres, hvad og om der skal outsources, og hvad virksomheden selv skal drive. Dernæst skal virksomheden skabe overblik over, om teknologivalgene beskytter forretningen tilstrækkeligt. Disse svar og løsninger skal findes i tæt samarbejde med virksomhedens it-ansvarlige og evt. it-servicepartnere i tilfælde af, at man har outsourcet.

Virksomheden ønsker klarhed over følgende:

- Hvordan er det eksisterende teknologiske forsvar?
- Passer det med de identificerede trusler og risici?
- Hvad er behovet for yderligere sikring?
- Hvad er teknologiens muligheder og begrænsninger?
- Har vi prioriteret investeringer i et teknologisk forsvar for virksomhedens mest sårbare aktiver?

Arkitekturområdet
PAVA-konceptets fokus på arkitektur medvirker til et passende design og implementering af tekniske løsninger til beskyttelse af forretningens aktiver (Assets).

Valideringsområdet
Et centralt element for alle sikkerhedsmekanismer er en validering af, at beskyttelsen er effektiv. Valideringsområdet beskriver de aktiviteter, der skal medvirke til løbende at opdage og verificere svagheder i virksomhedens tekniske og organisatoriske kontroller.

Behovsafklaring og kravsspecifikation

Krav til it-leverandør

- Modsvarer leverandørens sikkerheds-bestemmelser reelt vores behov og risici, eller er der blot tale om en standardaftale, hvor vores forretning ikke nødvendigvis får den rette beskyttelse?
- Er der løbende opfølgning på leverandørens sikkerhedsniveau, foretages der bl.a. løbende sårbarhedsscanninger? Får leverandøren foretaget regelmæssige penetrationstest? Har vi modtaget en revisionserklæring, der beskriver det aktuelle sikkerhedsniveau?
- Har vi indblik i, hvordan leverandøren håndterer løbende opdatering og konfiguration af systemer?
- Har vi indblik i, hvordan leverandøren håndterer adgangsstyring til vores systemer og data? Hvor mange administrative medarbejdere kan tilgå vores systemer?
- Er der en effektiv proces for hændelseshåndtering, der gør, at vi kan komme i drift inden for et givent tidsrum? Svarer dette til vores forretnings krav?
- Er der en klar ansvarsfordeling og en veldefineret snitflade mellem leverandørens beredskab og vores beredskab, der gør det muligt at kommunikere hændelser til relevante interessenter og minimere skader og tab?

Outsourcing

- Sikkerheds-krav, der af-spejler risikoen
- Leverandørens sikkerhedsniveau
- Løbende opfølgning
- Ansvarsfordeling

- Systemer
- Overvågning
- Kompetencer
- Back-up Recovery

Inhouse

Krav til egen it-afdeling

- Har vi tilstrækkelige processer og teknologi til at styre brugeres adgang til systemer og data?
- Har vi de rigtige systemer til at forhindre uønsket adgang til kritisk data?
- Får vi løbende testet og opdateret vores kritiske systemer?
- Kan vi detektere, identificere og overvåge hændelser, mens de sker?
- 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?
- Er der en tilstrækkelig backup, der kan medvirke til effektiv genetablering?

Teknologivalget er vigtigt

Der er en række konkrete teknologivalg, der skal tages i forhold til at beskytte virksomhedens aktiver mod cybertruslen. Det drejer sig bl.a. om, hvordan brugernes pc'ere er beskyttet, om infrastruktur- og netværkssikkerhed, bruger- og identitetsstyring, ligesom det drejer sig om systemer til logning, til at opdage potentielle angreb og til at forebygge ubudne gæsters indtrængen.

+

Case: **Risiko ved mangelfuld eller dårlig netværkssegmentering:**

PwC's Incident Response Team møder indimellem hosting-leverandører, der bliver ramt af malware, og som grundet dårlig eller mangelfuld netværkssegmentering er skyld i, at kunder udsættes for cyberhændelser. Selvom man som virksomhed har en rigtig god cybersikkerhed, kan man blive ramt, hvis hostingleverandøren ikke har det. I et konkret eksempel havde hostingleverandøren ikke styr på netværkssegmenteringen, så da en af deres kunder blev ramt, så medførte det, at alle kunder blev ramt. Det gik så galt, at man var nødt til at slukke for internettet. Og i sådan en situation vil det være godt med en aftale om fx garanteret oppetid og maksimal nedetid.

Erfaringer fra PwC Danmarks Incident Response Team

Andre teknologispørgsmål, som en CFO bør sikre sig, at virksomheden forholder sig til, er:

End-point sikkerhed: Hvor meget skal den enkelte brugers enheder sikres, fx i relation til om brugeren skal have tilladelse som lokaladministrator på sin pc eller ej. Skal brugerens pc krypteres, så data ikke kan tilgås, hvis den bliver stjålet?

Netværkssikkerhed: Hvilke sikkerhedsmekanismer kan bygges ind i netværket? I hvor høj grad skal netværket segmenteres, så ondsindet kode ikke så let spredes over nettet? Skal vi have network access control, så vi har mere styr på, hvilke enheder, der kobler sig til vores netværk?

Log management: I hvor høj grad skal vi overvåge og logge, hvad der sker på vores netværk og på vores centrale applikationer? Hvilke aktiviteter skal logges? Skal vi behandle vores logs intelligent gennem et SIEM (Security Incident & Event Management) System, så vi kan få alarmer, når en given handling forekommer?

Intrusion Detection System og Intrusion Prevention System: Systemer, der ud fra en række opsatte regler kan opdage eller blokere for en hændelse.

Husk at involvere it-afdelingen og it-serviceleverandører i relevante teknologiske spørgsmål. Det kan også være en fordel at involvere eksterne eksperter, der kender de teknologiske muligheder mere generelt.

Klare fordele ved outsourcing, men vær kritisk

Et af de centrale spørgsmål er, om I bør outsource hele eller dele af it-driften, og dermed det teknologiske forsvar, og hvordan man sikrer sig, at det gøres rigtigt. Der kan være klare fordele ved at outsource driften af it-systemer og dermed også dele af sikkerheden til en ekstern leverandør, der har det som sin kerneforretning at drive it og dermed bør have bedre forudsætninger for at beskytte virksomheders kritiske data.

Men selvom man kan outsource sine it-systemer, kan man ikke outsource ansvaret. Derfor må man stadig gøre forarbejdet ordentligt, så man sikrer, at ens systemer og data er tilstrækkeligt beskyttet, og at helt specifikke sikkerhedskrav stilles til leverandøren.

Mange virksomheder har allerede outsourcet deres it-systemer, men sikkerhedsniveauet er ikke statisk, og selvom leverandørerne henad vejen tilpasser deres ydelser og produkter, er der løbende et behov for at sikre, at aftalen også matcher virksomhedens behov og risici.

Få hjælp med en revisionserklæring

Har virksomheden ikke selv kompetencerne i huset til at undersøge og sikre, at kravene overholdes, kan en revisionserklæring hjælpe. Revisionserklæringen kan give virksomheden vished for, om leverandøren lever op til virksomhedens specifikke krav til sikkerhed.

+

Opsummering:
Teknologivalg

+ Ligeså vigtigt det er at forstå, at cybersikkerhed ikke kun er et spørgsmål om hardware og software, ligeså vigtigt er det at forstå, at teknologi er en afgørende del af et effektivt cyberforsvar. Med CFO'en som central figur er det den samlede ledelses opgave at skabe et overblik over virksomhedens teknologiske cyberforsvar. Det gælder både i virksomhedens egen it-afdeling og eventuelle it-leverandører.

Forslag:
Sådan kommer du videre

+ Skab overblik over det nuværende teknologiske forsvar og beskyttelsesniveau ift. de vigtigste aktiver for forretningen.
+ Gå i dialog med egne it-ansvarlige og eksterne it-servicepartnere med fokus på sikkerhed (ikke drift).
+ Afdæk om der er allokeret tilstrækkelige ressourcer med de rette teknologiske kompetencer til at løfte opgaven.
+ Find ud af, om I har de rette teknologiske kompetencer selv, eller om der er behov for ekstern hjælp.

> Cyberkriminelle udnytter sårbarheder i virksomheders systemer og infrastruktur, og derfor er det afgørende, at ledelsen foretager teknologivalg, der beskytter virksomheden optimalt mod cyberkriminalitet.

Håndtering af brugere og adgange

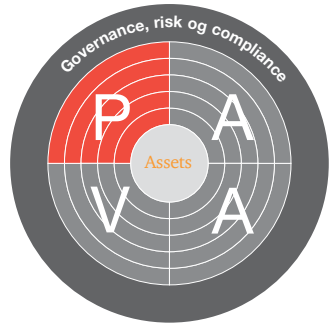
I dette afsnit går vi tættere på virksomhedens bruger- og adgangsstyring – et af de mest grundlæggende elementer inden for cybersikkerhed. Du får en række gode råd til, hvordan man laver politikker for adgang til virksomhedens systemer med det formål at sikre, at kun de rette personer har adgang.

Bruger- og adgangsstyring

Access Management – også kaldet bruger- og adgangsstyring – er et at de mest grundlæggende elementer, når det kommer til at beskytte virksomheden mod cyber- og informationssikkerhedshændelser.

Det er vigtigt for virksomheden, at de rette medarbejdere har adgang til de rette data og systemer. På samme måde er det i et sikkerhedsperspektiv afgørende, at det kun er de personer, der skal have adgang, som får tildelt adgang – baseret på et arbejdsbetinget behov. Jo flere brugere, man har, og jo bredere adgange man har til systemer og data, des større er sandsynligheden for kompromittering. Derfor er det vigtigt at begrænse både, hvem der har adgang til systemerne, og hvad de har adgang til. Styring af adgangen til persondata er ligeledes et lovkrav i henhold til GDPR.

Cyberkriminelle har særligt gode betingelser for at gøre skade på virksomheden, hvis virksomhedens brugere har for brede adgange. Hvis en ekstern angriber kan kompromittere en brugers computer, evt. gennem en phishingmail, så kan angriberen tilgå samme (brede) adgange som brugeren, hvis der ikke er andre beskyttelsesforanstaltninger på plads. Det er blot et par af årsagerne til at kigge processerne omkring adgang til virksomhedens systemer igennem. De rette processer indebærer, at man tildeler rettigheder til brugere ud fra et arbejdsbetinget behov. I arbejdet med at få styr på bruger- og



Procesområdet
Processer for adgangsstyring skal medvirke til at sikre en ensartet tilgang til styring af brugeres rettigheder. Denne standardisering giver en højere grad af sikkerhed og mindre personafhængighed.

+

Case:
Ransomware lukker produktionsvirksomhed

Hændelse:: En lille sjællandsk produktionsvirksomhed med 20 medarbejdere bliver over natten hacket, og al deres data er krypteret, da de møder ind på arbejde om morgenen. På skærmen står en besked om, at virksomheden kan få genskabt adgang til deres data mod at betale løsesum på 25.000 USD, svarende til ca. 150.000 kr.

Konsekvens: Uden data kan virksomhedens udekørende teknikere ikke se deres opgaver og betjene deres kunder, ligesom bogholderiet ikke kan se, hvilke kunder der har betalt og hvem der ikke har. Virksomheden må ringe rundt til kunder for at rekonstruere de forestående og udførte opgaver og skabe klarhed over betalingsstatus.

Metode: Hackerne har formentlig ikke i første omgang målrettet angrebet mod denne virksomhed, men har sweepet internettet for servere med forældet sikkerhed. Er serveren af ældre dato og ikke opdateret, så er der gode muligheder for hackeren for med almindelig kodebryder-software (brute force), hvor en maskine ganske enkelt begynder at knække koderne ved at køre alle kombinationer igennem fra a til å. Derefter har hackeren installeret ransomware, der har sørget for resten.

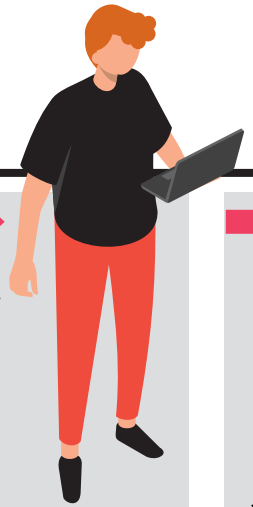
Erfaringer fra PwC Danmarks Incident Response Team

Brugerstyring

Tiltrædelser
Ansættelse af nye medarbejdere

Vær opmærksom:

- ✓ Tildeling af rettigheder bør ske på baggrund af medarbejderens forventede rolle.
- ✓ Rettigheder bør tildeles ud fra arbejdsbetinget behov og princippet om "least privilege", dvs. man ikke har adgang til mere end nødvendigt.
- ✓ Man bør ikke kopiere en eksisterende brugers profil, da en eksisterende bruger kan have akkumuleret flere rettigheder end nødvendigt.



Ændringer
Mobilisering af medarbejdere, der skifter rolle/afdeling i virksomheden

Vær opmærksom:

- ✓ Brugere akkumulerer typisk rettigheder over tid.
- ✓ Ved rolleskift er det god praksis at fjerne alle eksisterende rettigheder og tildele på ny, som ny medarbejder.

Fratrædelser
Ophør af profiler og adgange for medarbejdere, når ansættelsesforholdet stopper

Vær opmærksom:

- ✓ Luk ned for brugerens adgang til alle systemer og cloudløsninger.
- ✓ Virksomheden bør sikre, at der er en solid proces for at styre – og fjerne – adgange, både de der er styret via AD (virksomhedens centrale brugerregister), og dem der ikke er, så medarbejderen ikke kan tilgå systemer efter ansættelsens ophør.

adgangsstyring, er det oplagt at fokusere på Tiltrædelser, Ændringer og Fratrædelser. Mange virksomheder arbejder eksempelvis med, at man ved oprettelse af nye brugere (Tiltrædelser) tildeler brugeren de samme rettigheder som "en lignende kollega." Det kan være farligt, fordi man muligvis glemmer, at vedkommende har fået akkumuleret rettigheder eller har nogle specifikke og priviligerede adgange. Det samme gør sig gældende, når en medarbejder får nye opgaver eller flytter til en anden afdeling (Ændringer). Her er det vigtigt at opdatere medarbejderens adgange ud fra de nye arbejdsbetingede behov, og at man ikke blot tilføjer nye adgange, men også fjerner dem, der ikke er relevante i den nye funktion. Og når en medarbejder stopper (Fratrædelser), er det vigtigt, at man får afviklet brugeren i alle systemer.

Relevante spørgsmål:

- Er der politikker og processer for, hvem der har adgang, hvad de har adgang til og hvorfor?
- Overholdes evt. politikker?
- Hvad er processen for oprettelse og tildeling af brugerrettigheder?
- Hvad er proces for at sikre, at brugere med arbejdsbetingede behov, har adgang? Hvor ofte kontrollerer vi denne adgang?

+

Opsummering:
Brugere og adgange

+ Bruger- og adgangsstyring er en afgørende nøgle til at sikre virksomhedens aktiver. Gennem en konsistent styring af, hvilke medarbejdere og samarbejdspartnere, der har adgang til systemer og data, kan man reducere risikoen for kompromittering, hvis man udsættes for et cyberangreb.

Forslag:
Sådan kommer du videre

+ Få overblik over politikker og processer i forhold til bruger- og adgangsstyring.
+ Fokusér indsatsen på de typiske brugersituationer (Tiltrædelser, Ændringer og Fratrædelser).
+ Etablér en løbende kontrol af, om brugeradgange matcher de arbejdsbetingede behov og korriger, hvis ikke de gør
+ Review af sikkerheden i AD (virksomhedens centrale brugerregister).

Beredskabsplanlægning

I dette afsnit hjælper vi dig med at få et overblik over, hvad du bør have styr på for at være bedst muligt forberedt på, at en alvorlig hændelse rammer virksomheden. Vi giver her nogle gode råd til, hvordan du etablerer et operationelt beredskab og sørger for, at alle er bekendte med, hvad der skal til for at sikre, at virksomheden kommer igennem en alvorlig cyberhændelse på bedst mulig vis, når uheldet er ude.

Få styr på beredskabet, inden uheldet sker

En af de væsentligste forudsætninger for at en virksomhed kan minimere konsekvenserne af et cyberangreb og hurtigt komme på banen igen er at have et operationelt beredskab. Det handler om at være godt forberedt ved bl.a. at have identificeret de mest kritiske forretningsgange og understøttende systemer, samt have etableret processer for hændelseshåndtering, krisehåndtering og nødberedskab. En alvorlig cyberhændelse er mere end en it-opgave, da den i yderste instans kan have fatale konsekvenser for virksomheden og bør derfor behandles på flere niveauer i organisationen.

Procesområdet
Et passende beredskab består af operationelle processer og procedurer såvel som en klar organisering af roller, så håndteringen af hændelser bliver mindre personafhængig.

Valideringsområdet
Regelmæssige beredskabsøvelser validerer, om beredskabet kan håndtere hændelser effektivt, eller om der skal foretages forbedringer.

Cybertruslen er mere relevant end nogensinde før. Ledere i dansk erhvervsliv mærker nærmest dagligt konsekvensen af den betydelige stigning i cyberkriminalitet, der er sket de seneste måneder og år. Der bliver fortsat stillet stigende krav til cybersikkerheden i både store og mindre virksomheder. Det er ikke længere sådan, at det er et spørgsmål, om man bliver ramt af en hændelse, men nærmere hvornår det sker. Ifølge PwC's Cybercrime Survey 2022 er det fjerde år i træk, at mere end hver anden danske virksomhed eller organisation har været udsat for en cyberhændelse.

Cyberhændelser er som udgangspunkt designet til at skabe alvorlige forstyrrelser af virksomhedens aktiviteter med det formål at ramme virksomheden på en måde, så det har stor økonomisk skade. Når man som ledelse skal etablere et beredskab, er det derfor helt afgørende, at man tager udgangspunkt i de forretningsaktiviteter og -processer, der er mest kritiske for virksomhedens fortsatte drift. Ved at identificere de aktiviteter, som har størst indflydelse på virksomhedens indtjening (nuværende eller fremtidige), kan man prioritere et passende beredskab, der kan bidrage til at minimere skaden i tilfælde af, at man bliver ramt af et cyberangreb.

BEREDSKABSPLANLÆGNINGENS 5 FASER

5. Løbende forbedring
Trusler er ligesom virksomheden ikke en statisk størrelse. De vigtigste forretningsfunktioner vil ændre sig og udvikles over tid. Det samme vil de trusler, de står over for. Derfor er det vigtigt at genbesøge og opdatere ens beredskab regelmæssigt og efter større ændringer.

1. Forstå forretningen
Hvad er mest kritisk at beskytte i en krisesituation? Hvilke funktioner kan undværes, og hvilke er afgørende for at sikre produktionen?

4. Træn og test
De mest effektive planer er velafprøvede og forankret i organisationen. Medarbejdere bør være bekendt med deres rolle og med de planer, der understøtter beredskabet.

2. Strategi selektion
Hvordan fortsættes aktiviteterne bedst muligt, og hvordan genoprettes forretningens kernefunktioner. Forbered aktiver og ressourcer, der er nødvendige.

3. Planlæg og implementér
Udarbejdelse af planer for de identificerede kernefunktioner under hensyntagen til genopretningsstrategier, tilgængelige ressourcer og forebyggende foranstaltninger.

Hvordan forbereder man sig, inden uheldet rammer?
En ansvarlig ledelse bør have indsigt i virksomhedens generelle trusselsbillede, såvel som de mitigerende processer og arbejdsgange, der har til formål allerførst at forebygge cyberhændelser og dernæst sikre, at alvorlige hændelser bliver identificeret og håndteret hurtigt og effektivt, når uheldet er ude. Det er vigtigt, at ledelsen via grundig beredskabsplanlægning sikrer, at disse processer og arbejdsgange bliver klarlagt og indarbejdet, så virksomheden formår at handle effektivt og målrettet, når der opstår en cyberhændelse. De rette teknologivalg samt en god awareness-kultur kan være med til at understøtte en hurtig identifikation af cyberhændelser.

En ansvarlig ledelse bør på samme måde have forberedt et beredskab, der træder i kraft, når uheldet opstår. Cyberhændelser kan i værste fald være fatale, hvis de ikke håndteres effektivt. Cyberhændelsernes alvorlighed kan medføre, at ledelsen er nødt til at indføre særlige retningslinjer og arbejdsgange, der bliver sat i spil, når en krise opstår.

Beredskabets væsentligste formål

1. Sikre indtægter og produktivitet i tilfælde af at en uforudset hændelse indtræffer.

2. Reducere omkostninger ved en hændelse, ved at man kan eksekvere hurtigt og har mitigerende tiltag på plads.

3. Prioritere tiltag i forhold til kritiske funktioner.

4. Sikre en hurtigere tilbagevenden til normalen.

5. Sikre organisationens omdømme og relationer til eksterne og interne interessenter.

6. Opnå stærkere og bedre beslutningsgrundlag samt deraf færre negative konsekvenser ved uforudsete hændelser og ændringer.

+

Case: **Forældede servere lukker leverandør af byggematerialer**

En byggemarkedskæde med mange fysiske butikker er i gang med at outsource driften af sine servere til en ny it-serviceleverandør. Serverne, der flyttes, viser sig at have meget lav sikkerhed, og snitfladerne til den nye serviceleverandør er ikke på plads, da virksomheden bliver ramt af et hackerangreb. Hændelsen rammer mange af virksomhedens it-systemer og påvirker store dele af forretningen. Butiksmedarbejdere er nødt til at skrive alt ned på papir, bl.a. hvilke håndværkere der henter hvilke varer og hvornår. Som dagene går, bliver det i stigende grad svært at holde overblik med hvilke varer, der er på hylderne og hvad der skal bestilles hjem. I fem hele dage kan virksomheden slet ikke modtage ordrer fra og levere varer til dens kunder.

På grund af et manglende overblik med it-dokumentation og en uafprøvet backup, tog det 13 dage fra hændelsen indtraf, til it-systemerne og størsteparten af forretningen var kørende igen. Dvs. næsten to uger, hvor virksomheden ikke kunne servicere sine kunder effektivt.

Efter hændelsen opdagede virksomheden, at en del kunder var begyndt at handle hos andre byggemarkeder og det tog næsten et år inden omsætningen var på samme niveau som før hændelsen.

Ved at have arbejdet med nogle enkle nødplaner for butikkerne, kunne man bedre have serviceret kunderne, sikret lagerføring af de mest anvendte varer og holdt omsætningen på et passende niveau. Ved at have arbejdet med it-beredskabet, ville det have været muligt at genetablere it-systemerne hurtigere og minimeret skaden.

Erfaringer fra PwC Danmarks Incident Response Team

Beredskabets ændrede beslutningsgange

Når virksomhedens ledelse vurderer, at man er udsat for et cyberangreb, som ikke kan løses indenfor en acceptabel tidshorisont eller, som vil have høje forretningsmæssige konsekvenser, så skal man beslutte at iværksætte et beredskab, der i nogle tilfælde medfører andre beslutningsgange end under normal drift. Cyberhændelser kan sammenlignes med en brand, der sætter alle kendte spilleregler ud af funktion. Når det brænder, er det eksempelvis indsatslederen og ikke den administrerende direktør, der styrer slagets gang. På samme måde kan en it-chef eller en pålidelig ekstern incident-leder have styringen under en alvorlig og kompleks cyberhændelse.

Væsentligt er det dog, at ledelsen har taget initiativ til at beskrive, hvem der har ansvar for hvad, når hændelsen sker. Med andre ord skal alle kende deres roller og ansvar i det øjeblik, beredskabet træder i kraft.

Formålet med beredskabet

Beredskabet er tredelt og har til formål, så vidt det er muligt, at sikre fortsat produktivitet og drift, begrænse skaderne og sørge for en hurtig tilbagevenden til normalen. Grundlæggende drejer det sig om at være i stand til at opdage hændelser tidligt, at kunne agere undervejs og have en evne til at komme 'på benene igen' bagefter.

Begræns skaden

Krisehåndtering

Fortsæt driften

Forretningens nødplaner

+ Det er vigtigt at holde kritiske forretningsprocesser kørende, for at virksomheden bedst muligt kan servicere dens kunder og generere omsætning samt likviditet under en alvorlig hændelse.

+ Kriseledelsen skal minimere omfanget af negative forretningskonsekvenser ved et cyberangreb - både på kort og længere sigt. Beredskabets indsats skal sikre virksomhedens omdømme og bevare gode relationer til kunder, leverandører og samarbejdspartnere. Kriseledelsen skal sikre, at der er overblik over tilgængelige interne og eksterne specialistressourcer ved eksempelvis at have en Incident Respons (IR) aftale med en leverandør, vurdere og koordinere indsatsen for at begrænse påvirkningen af virksomheden. Kriseledelsen skal sørge for, at der kommunikeres effektivt internt og eksternt.

Tilbage til hverdagen

Genetablering af normal drift

+ It-afdelingen eller virksomhedens It-leverandør vil typisk stå for at skulle genetablere den normale drift. Det kan omfatte genopbygning af den tekniske infrastruktur, geninstallering. af systemsoftware og indlæsning af backupdata, inden forretningen kan bruge de normale systemer.

I beredskabsplanlægning er det en god idé at udarbejde enkle og operationelle kommunikations- og handlingsplaner for de hændelsesscenarier, som virksomheden har identificeret som værende mest relevante. Det handler om at beskytte de kronjuveler, man har identificeret som afgørende for virksomhedens fremtidige eksistens. Kommunikations- og handlingsplanerne skal løbende gennemgås, øves og opdateres i forhold til virksomhedens egne oplevelser, men evt. også med inspiration fra hændelser der sker uden for virksomheden.

Den bedste beredskabsdokumentation er ikke nødvendigvis meget detaljeret, da man i en krisesituation ikke har tid til at læse komplekse dokumenter. Dokumentationen bør i bund og grund udgøres af tjeklister, der sikrer, at beslutningstagere ikke glemmer vigtige aktiviteter, som fx om et persondatabrud skal rapporteres eller om ens cyberforsikring skal aktiveres, samt indeholder væsentlige kontaktinformationer til eksterne specialister, kritiske leverandører og nøglemedarbejdere.

Netop spørgsmålet om, hvem man skal tilkalde, er vigtigt at have overvejet og besluttet, inden man står i en krisesituation. Et alvorligt cyberangreb er komplekst og kræver specialistressourcer, der ofte ikke findes i egen virksomhed eller hos ens It-driftsleverandør.

Handlingsplaner vil være med til at tilsikre, at den rette organisering er på plads til at håndtere de mange opgaver, herunder de tekniske og forretningsmæssige dele af en kompleks hændelse. Kommunikationen under en cyberhændelse er en vigtig og central disciplin, og det bør være afstemt, hvor ansvaret for kommunikation ligger og til hvilke interessenter, der skal kommunikeres - fx medarbejdere, kunder, leverandører og bestyrelse. Virksomheden bør også planlægge, *hvordan* man vil kommunikere, hvis de almene kommunikationskanaler ikke er tilgængelige.

Effektive beredskabsplaner kræver, at man træner dem

Et centralt element i enhver beredskabsplanlægning er træning. Det er vigtigt, at virksomheden ikke blot får lavet den nødvendige forberedelse til at håndtere en given hændelse, men at organisationen øver sig i at håndtere relevante scenarier. Således at dem, der har særlige opgaver bliver fortrolige med deres rolle i en given situation. Træning kan dække alt fra skrivebordsøvelser over scenariebaserede øvelser til virkelighedsnære øvelser, hvor man også tester de tekniske muligheder for genetablering. Fælles for dem alle er, at man øver ens færdigheder, træner samspillet og identificerer eventuelle svagheder og forbedringsmuligheder samt agerer på disse.

Forslag:
Sådan kommer du videre

+ Etablér beredskabsplaner, der tager udgangspunkt i kritikaliteten af virksomhedens vigtigste forretningsprocesser.
+ Sørg for, at I har en plan for krisehåndtering på plads.
+ Etablér et it-beredskab, der skal sikre, at it-systemer kan genetableres, når de er blevet kompromitteret.
+ Udform nødplaner, der beskriver, hvordan kritiske forretningsprocesser kan videreføres i det tidsrum, de understøttende it-systemer er ude af drift.

Ingredienserne i et passende beredskab

- En proces for hændelseshåndtering (Incident Management).
- Et it-beredskab, der skal sikre, at it-systemer kan genetableres, når de er blevet kompromitteret (Disaster Recovery Plan).
- En krisehåndtering (Crisis Management) der kan understøtte de nødvendige beslutninger, sikre tydelig og effektiv kommunikation, håndtering af medarbejdere, kunder og øvrige interessenter, når hændelsen har en karakter og omfang, der udgør en krise for virksomheden.
- Forretningsnødplaner (Business Continuity Plan) der understøtter, at den enkelte forretningsproces kan videreføres i det tidsrum, de primære understøttende it-systemer er utilgængelige.
- Er der en klar rollefordeling, der involverer it, ledelse, kundehåndtering og kommunikation?

+

Opsummering:
Beredskabsplanlægning

+ God forberedelse er nøglen til effektiv håndtering af en cyberhændelse. Ved at identificere de vigtigste forretningsgange og de systemer der understøtter dem, kan virksomhedens ledelse etablere et passende beredskab, der er med til at reducere konsekvenserne for forretningen.

> “ Cyberhændelse er mere end en it-opgave, da den i yderste instans kan have fatale konsekvenser for virksomheden og bør derfor behandles på flere niveauer i organisationen.

Adfærd og awareness

Her handler det om at få etableret en naturlig sikkerhedskultur i virksomheden, og at organisationen har et integreret fokus på beskyttelse af virksomhedens aktiver. Det drejer sig om at få et strategisk fokus i ledelsen, få etableret tilstrækkelige politikker og retningslinjer, samt igangsat et program for at højne vidensniveauet blandt medarbejderne. Der skal skabes awareness omkring sikkerhed og den afgørende rolle, medarbejderne kan spille i kampen mod de cyberkriminelle. Der skal sikres løbende træning og videndeling om aktuelle risici og hændelser.

Skab en sikkerhedskultur

Sikkerhedskultur gennem videndeling

Den menneskelige faktor er helt afgørende i forhold til at sikre virksomheden mod cyberangreb. Cyberkriminelle er eksperter i at finde metoder, der 'narrer' medarbejdere til at 'åbne døren' til virksomhedens systemer, og derfor handler det for ledelsen om at styrke cybersikkerhedskulturen i organisationen. Hvor medarbejderne uvidende kan udgøre den største risiko for virksomheden, så kan bevidste medarbejdere være med til at løfte sikkerhedsniveauet betragteligt.

Strategier og planer er væsentlige for cybersikkerheden, men følges de ikke op af korrekt adfærd hos medarbejdere, er man lige vidt. Den høje vækst i phishingmails, malware og ransomware, der er rettet mod medarbejdere på alle niveauer, stiller ikke bare store krav til virksomhedens tekniske sikkerhedsforanstaltninger, men også til den digitale adfærd i virksomheden.

Netop medarbejdere og deres adfærd er formentlig den største risikofaktor i forhold til cybersikkerhed. 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", så det er helt afgørende at skabe awareness og forankre en sikkerhedskultur i organisationen.

Tilløb til en sikkerhedspolitik

Arbejdet med awareness kan bl.a. ske gennem opstilling af 'best practice'-kriterier, udarbejdelse af medarbejderinddragende aktiviteter og videndeling fra den løbende overvågning af cybertruslen. Grundlaget for en cybersikker adfærd er, at der er defineret en sikkerhedspolitik for, hvad man må og ikke må – og hvordan man i konkrete situationer skal opføre sig. Denne bør være så konkret som mulig og bl.a. indeholde politikker for acceptabel adfærd og eksempler på "best practice".

'Awareness' i organisationen

Arbejdet med at etablere og fastholde en sikkerhedskultur i virksomheden er en fortløbende proces. Derfor er løbende kommunikationskampagner, uddannelse, test og evaluering nøgleord, når det kommer til at skabe opmærksomhed og viden om cybersikkerhed og sikker it-adfærd.

Adfærdsområdet
PAVA-konceptets fokus på adfærd er centralt i et sikkerhedsprogram. Træning og awareness-aktiviteter skal medvirke til at løfte medarbejdernes bevidstheds- og kompetenceniveau i forhold til at beskytte virksomhedens informationer og aktiver.

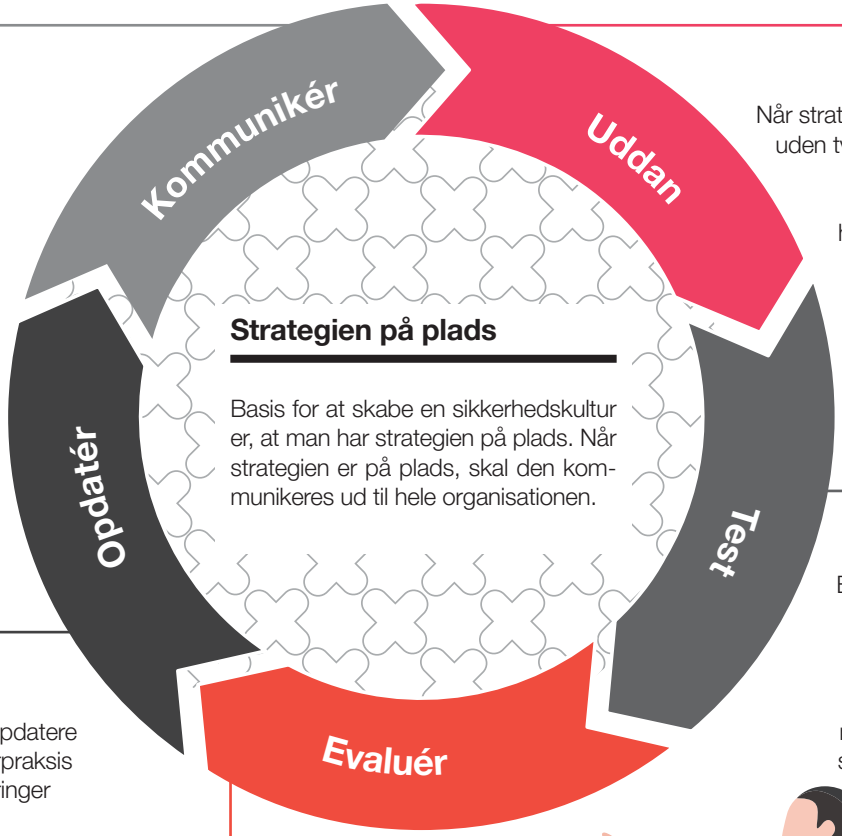
Kommunikér

Sørg for at få strategien ud i hele organisationen. Hvad er det, vi gør, hvorfor gør vi det, og hvad betyder det for medarbejderne?

Det kan være en god idé at kommunikere jeres sikkerheds-strategi til kunder og samarbejdspartnere og sende nogle stærke signaler om, at I tager cyber-sikkerhed alvorligt.

Opdatér

Sørg for løbende at opdatere virksomhedens cyberpraksis på baggrund af ændringer i trusselsbilledet eller organisationen og kommunikér dette til medarbejderne.



Uddan

Når strategien er meldt ud, vil der uden tvivl være et behov internt i organisationen om at få klar besked i forhold til, hvordan medarbejdernes dagligdag forandres. Det er en god idé at uddanne medarbejderne i de specifikke situationer, hvor de skal være særligt påpasselige, fx mailhåndtering.

Test

En helt klassisk metode til at styrke organisationens sikkerhedskultur er løbende tests. Det kan fx være at teste, hvordan medarbejderne håndterer simulerede phishingmails.

Evaluér

Evaluér om det nuværende kendskabsniveau blandt medarbejderne er tilstrækkelig.

CFO'ens opgaver er:

- Sikre at virksomheden kommunikerer, at den vil have en mere sikker adfærd
- Sikre at den ønskede adfærd defineres – sikkerhedspolitik med "best practice"-eksempler og "acceptable use policies"
- Videndeling om cybersikkerhed – dele information fra overvågningen
- Sørge for træning af medarbejdere – fx krisestyrings-, GDPR- og phishingøvelser. Sørge for uddannelse via fx e-learningprogrammer og videndeling
- Sørge for test af medarbejderne
- Evaluere, rapportere og gentage, hvis nødvendigt.

+

Opsummering:
Sikkerhedskultur

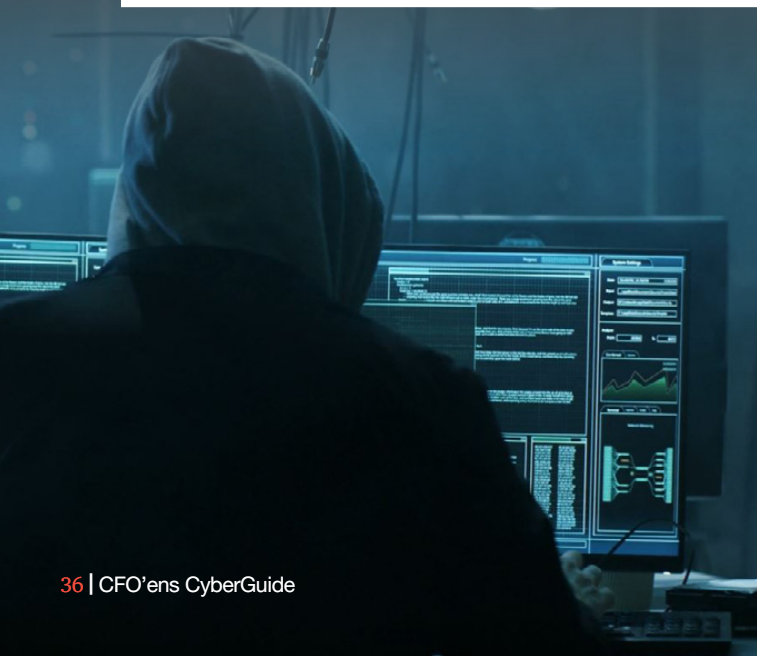
+ Den menneskelige faktor er en af de største årsager til, at hackere lykkes med hackerangreb. Sørg derfor for, at medarbejderne kender virksomhedens cybersikkerhedspolitik og uddan dem i at efterleve den.

Forslag:
Sådan kommer du videre

+ Etablér en klart kommunikeret sikkerhedspolitik, der tydeliggør korrekt adfærd.
+ Udarbejd løbende medarbejderinddragende aktiviteter og videndeling – som kampagner, uddannelse og testaktiviteter.
+ Lav en løbende evaluering og rapportering på tiltagene og gentag disse, hvis nødvendigt.

Incident Response - sådan håndterer jeres virksomhed bedst en cyberhændelse

I dette afsnit viser vi, hvordan du som CFO kan sikre, at virksomheden er forberedt bedst muligt på at håndtere en cyberhændelse. Vi ser på Incident Response, som dækker over de handlinger, der foretages for at undgå eller reducere de negative effekter af et cyberangreb - og giver gode råd til, hvordan virksomheden opnår optimal robusthed over for cybertrusler. Derudover ser vi på, hvordan I forbedrer jeres parathed til at håndtere hændelser, når de opstår.



Som følge af digitaliseringen har cyberangreb som oftest en voldsom effekt, og ligesom det digitale forsvar bliver mere raffineret, gør de digitale angreb det samme. Derfor skal alle virksomheder være i stand til hurtigt at reagere på og komme sig efter et cyberangreb. Det kræver, at organisationen er godt forberedt. En væsentlig forudsætning for at minimere konsekvenserne af et cyberangreb og hurtigt komme på benene igen er, at man er forberedt på at håndtere hændelsen – at man har styr på sin Incident Response.

Der er flere årsager til, at virksomheder i dag er afhængige af effektiv Incident Response. Først og fremmest handler det om at sikre virksomhedens drift og i sidste ende eksistens ved at kunne håndtere cyberangreb hurtigt og effektivt. Derudover er der hensynet til kunder, leverandører og samarbejdspartneres sikkerhed. Endelig er der reguleringer som GDPR, NIS2 og DORA, som stiller øgede krav til virksomheders evne til at håndtere cyberhændelser. Operationel robusthed er blevet et centralt regulatorisk krav i flere industrier, med særligt fokus på cybersikkerhed, efterhånden som virksomheder bliver mere teknologiafhængige og forbundne. GDPR og NIS2 kræver eksempelvis, at organisationer reagerer med det samme, og at man indrapporterer til myndighederne inden for hhv. 24 og 72 timer efter en cyberhændelse.

En eventuel inddragelse af en ekstern part under en hændelse, uden tilstrækkelig forberedelse, kan forsinke reaktionen betydeligt på grund af den nødvendige tid til onboarding. Derfor er det væsentligt, at virksomheden har forberedt sig grundigt på, hvad der skal ske før, under og efter et cyberangreb.

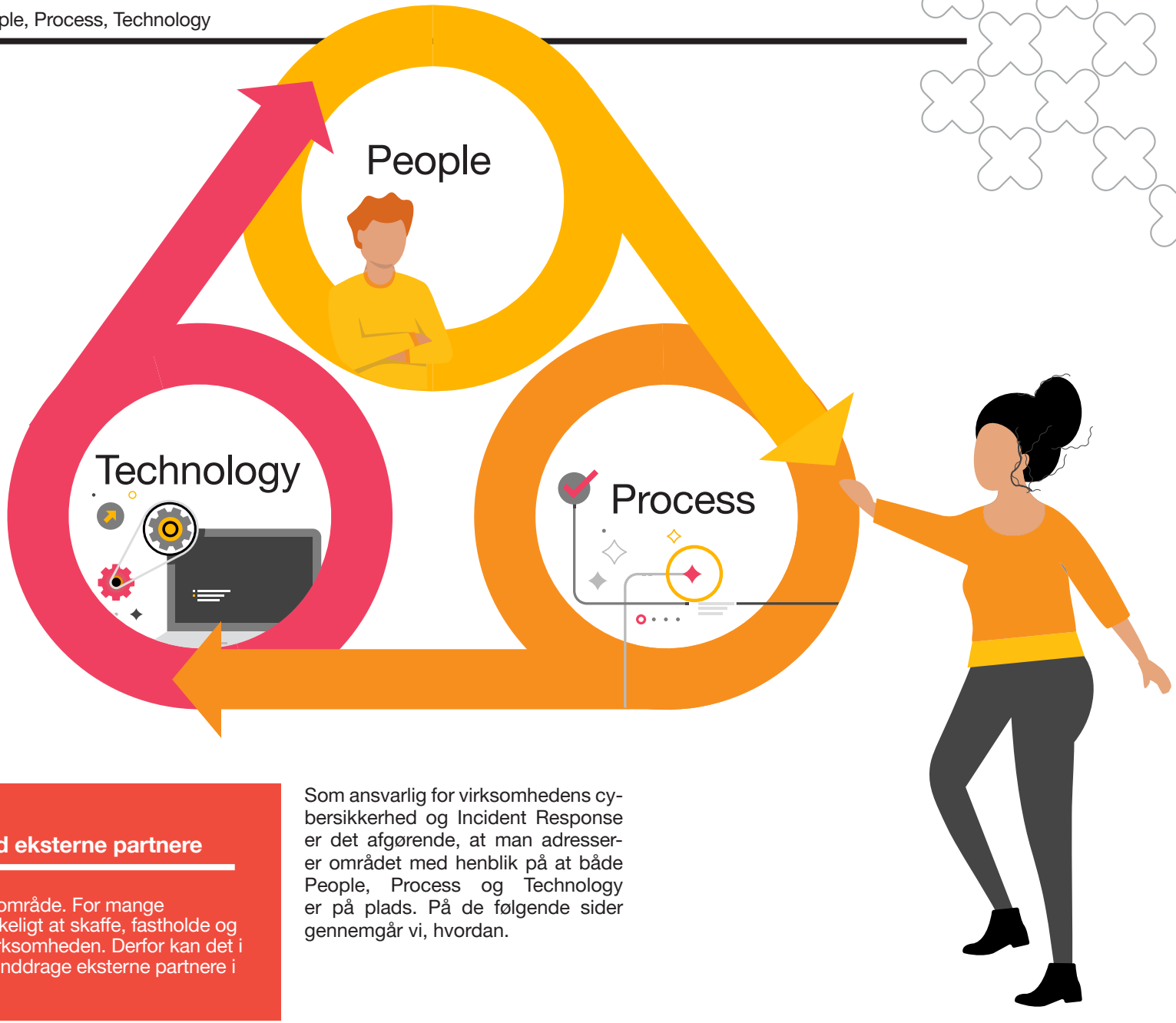
Denne guide hjælper med at forberede dig på det værste og øge både din robusthed over for cybertrusler og din parathed til at kunne håndtere hændelser, når de opstår. Samtidig forbereder den dig til at styrke virksomhedens digitale forsvar efter et cyberangreb.

Sådan gør du før en hændelse

I en tid, hvor det digitale trusselsbillede skaber tiltagende udfordringer, og hvor virksomhedernes drift og eksistens i høj grad udfordres af stadig mere komplekse og destruktive cyberangreb, kan det at være velforberedt gøre hele forskellen, når man står over for et angreb. Man kan således ikke forvente, at virksomheden vil kunne håndtere et cyberangreb eller en cyberhændelse effektivt medmindre, man har forberedt sig på forhånd.

For at etablere en velfungerende Incident Response evne, er det en forudsætning, at virksomheden har nogle grundlæggende elementer på plads. Som udgangspunkt skal ledelsen og nøglemedarbejdere kende til virksomhedens væsentligste aktiver – kronjuvelerne. Kender man ikke de vigtigste aktiver, kan man ikke planlægge og prioritere sikkerhedsindsatsen ved en cyberhændelse. Læs eventuelt afsnittene "Det cyberstrategiske fundament" og ikke mindst "Få styr på virksomhedens vigtigste aktiver" i denne guide, hvori vi gennemgår processen.

People, Process, Technology



Forslag:
Supplere interne kompetencer med eksterne partnere

+ Udviklingen går utrolig hurtigt på dette område. For mange virksomheder kan det derfor være vanskeligt at skaffe, fastholde og efteruddanne de rette kompetencer i virksomheden. Derfor kan det i mange tilfælde være en god løsning at inddrage eksterne partnere i håndteringen af cybersikkerhed

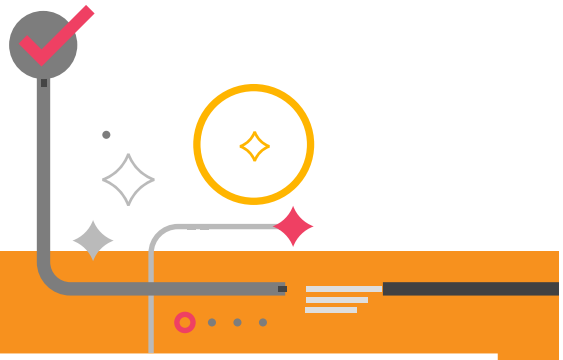
Som ansvarlig for virksomhedens cybersikkerhed og Incident Response er det afgørende, at man adresserer området med henblik på at både People, Process og Technology er på plads. På de følgende sider gennemgår vi, hvordan.

People

Når du skal etablere eller efterse virksomhedens Incident Response evner, er det vigtigt at undersøge, om virksomheden har kompetencer og ressourcer på plads (People). Typisk skal man spørge sig selv, om virksomheden har både de nødvendige kompetencer og tilstrækkelige ressourcer til at reagere effektivt på en hændelse, hvis den rammer.

Herunder er nogle af de spørgsmål, du bør stille dig selv angående People:

+ Ved vi, hvilke medarbejdere, der skal håndtere en hændelse?
  - Ved medarbejderne selv, at de har den rolle og funktion, og ved resten af organisationen det?
+ Har medarbejderne de rette kompetencer?
  - Bliver deres viden opdateret løbende?
+ Er de rette værktøjer stillet til rådighed?
  - Har medarbejdere tid til at vedligeholde deres kompetencer – herunder træning af kompetencer og brug af værktøjer?
+ Har medarbejderne adgang til viden omkring Threat Intelligence? Threat intelligence omfatter viden, der øger medarbejdernes indsigt i cybertrusler og kendskab til metoder og værktøjer, der kan benyttes som forsvar.
  - Er der tilstrækkeligt med medarbejdere til rådighed til at kunne håndtere en hændelse 24/7 i en længere periode?



Process

For at virksomheden kommer godt igennem en cyberhændelse, er det bl.a. afgørende, at virksomheden har etableret klare procedurer, der gør, at man er i stand til at handle hurtigt og effektivt på cyberhændelsen. Som ledelse skal man sikre, at Incident Response-processerne er på plads, kendte og afprøvede. Det involverer identifikation, registrering, respons og genetablering af drift efter et cyberangreb. I tilfælde af et cyberangreb skal Incident Response-processen understøtte en effektiv håndtering af hændelsen, identificere og afhjælpe de negative konsekvenser. Hændelseshåndtering kan også involvere kommunikation med interessenter og offentligheden i tilfælde af større hændelser.

Her er de kernespørgsmål, du bør stille dig selv vedrørende Process:

+ Har vi et beredskab, og er den kendt af organisationen og testet/evalueret?
+ Hvordan er processerne for håndtering af Incident Response?
  - Identifikation, registrering, eskalering, respons og genetablering. Er der kommunikationsplaner?
+ Har vi planer for krisehåndtering og nøddrift af forretningen?
+ Har vi planer for genetablering efter kompromittering?

Læs eventuelt også afsnittet "Beredskabsplanlægning" i denne guide for en uddybende gennemgang.

Technology

Ligesom det langt hen ad vejen er den teknologiske udvikling, der muliggør cyberangreb, er teknologien også en væsentlig del af løsningen. Det er afgørende at have en teknologisk infrastruktur på plads, der kan beskytte mod de komplekse og varierende trusler, som en virksomhed kan stå overfor. Derfor er det vigtigt, at ledelsen har investeret i og implementeret de relevante teknologier og værktøjer, der kan opdage og efterforske en hændelse på en hurtig og effektiv måde. Har man ikke ressourcerne til at implementere sådanne teknologier, er det en god idé at inddrage en ekstern partner, som hjælper med at drifte og monitorere, fx som en Managed Service.

Her er de kernespørgsmål, du bør stille dig selv vedrørende Technology:

- Hvordan er det eksisterende tekniske forsvar?
- Har vi de rette værktøjer til at identificere trusler og risici?
- Hvad er teknologiens muligheder og begrænsninger?
- Hvad er behovet for yderligere sikring?
- Har vi prioriteret investeringer i et teknologisk forsvar for virksomhedens mest sårbare aktiver?

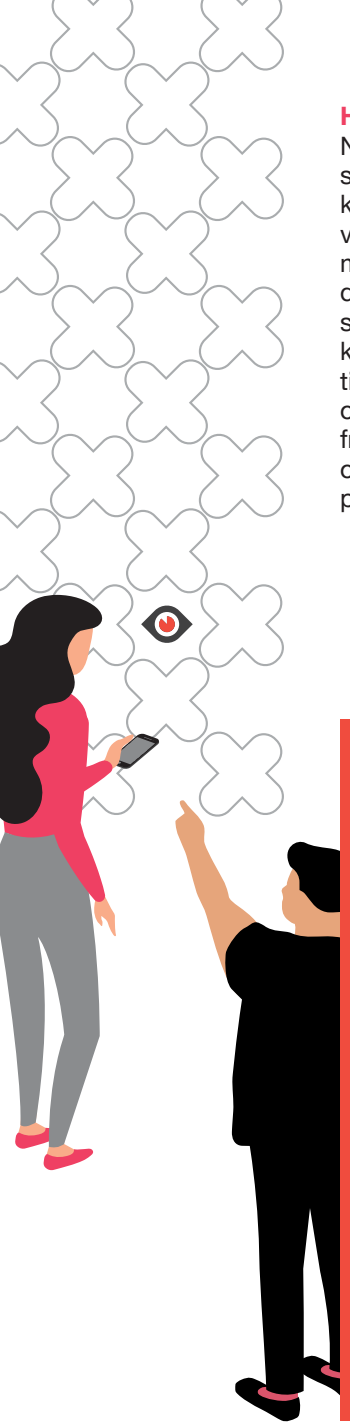
Læs eventuelt også afsnittet "Teknologivalg" i denne guide for en uddybende gennemgang.

Sådan gør du mens hændelsen står på

Hændelser kan opstå i alle former og størrelser, og som tommelfingerregel sker de aldrig på et belejligt tidspunkt, hvilket øger usikkerheden om omfanget og kompleksiteten af den potentielle konsekvens af en hændelse. Afhængigt af typen af hændelse kan og vil det ofte kræve kompetencer på tværs af tekniske, forretningsmæssige og juridiske områder for effektivt at begrænse den, udrydde truslen og hurtigt komme tilbage til normal forretningsdrift på en kontrolleret måde. Et cyberangreb på en virksomhed kan udfolde sig på mange måder, herunder phishing, malware-infektioner, ransomware osv. Disse angreb kan have alvorlige konsekvenser for virksomheder såsom datatab, forstyrrelser i forretningsprocesser, kundetab, økonomisk tab og varig skade på virksomhedens omdømme.

Mange virksomheder oplever jævnligt mindre cyberhændelser, der skaber forstyrrelser, som de fleste medarbejdere og kunder ikke opdager. Et stigende antal virksomheder oplever dog også cyberhændelser, der skaber store problemer, og som lammer virksomheden i kortere eller længere tid. Når sådanne hændelser indtræffer, er det vigtigt, at man er i stand til at opdage hændelsen og identificere de potentielle konsekvenser af denne, så man kan tage de rette beslutninger og forholdsregler i processen.

Det er vigtigt, at have en beredskabsplan på plads. Planen skal indeholde retningslinjer for, hvordan man identificerer, rapporterer og reagerer på et cyberangreb, hvordan man sikrer virksomhedens drift bedst muligt, mens angrebet står på, og hvordan man genopretter normal drift efter angrebet. Det er også vigtigt, at virksomheder uddanner og træner deres medarbejdere i at genkende og rapportere potentielle cyberangreb, da disse ofte er første forsvarslinje mod cyberkriminalitet. Beredskabsplanen skal eksempelvis også indeholde oplysninger om, hvordan man sikrer og bevarer logfiler og andre data, der kan hjælpe med at identificere angriberne og forhindre fremtidige angreb. Læs mere om beredskabsplaner i kapitlet "Beredskabsplanlægning" i denne guide.



Hændelsesforløb ved cyberangreb

Når den it-ansvarlige bliver opmærksom på, at et opstået cyberangreb kan få alvorlige konsekvenser for virksomheden, er det vedkommendes opgave at bremse hændelsen og orientere ledelsen om situationen. Ledelsen vil typisk indkalde kriseberedskabet, der i mange tilfælde består af den daglige ledelse og omfatter ledende repræsentanter fra fx it, HR, salg, produktion, logistik osv. Når en virksomhed går i nøddrift på grund af et cyberangreb, betyder det, at virksomhedens normale driftsprocesser er blevet afbrudt eller kompromitteret på en måde, der skaber alvorlige forstyrrelser i driften. Virksomheden skal reagere hurtigt og effektivt for at minimere skaden og genoprette normal drift hurtigst muligt. Dette kræver typisk en koordineret indsats fra flere afdelinger i virksomheden. I de fleste tilfælde inddrages der også ekstern assistance. I tilfælde af nøddrift er det kriseberedskabet, der midlertidigt overtager ledelsen.

+

Case:
Produktionsvirksomhed udsat for ransomware-angreb

Hændelse:: En virksomhed oplever, at de har problemer med at tilgå enkelte data, og dette bliver fejlmeldt til deres it-ansvarlige. Den it-ansvarlige kigger på serverne og konstaterer, at de har været udsat for en cyberhændelse på deres servere, og data er blevet krypteret. På den ene server dukker der et skærmbillede op fra hackerne, at virksomhedens data er blevet krypteret, og at de skal betale 2 måneders omsætning i bitcoin, hvis de vil have deres data tilbage. De har en frist på 72 timer, før deres data bliver frigivet på internettet. Virksomheden valgte ikke at betale løsesum.

Konsekvens: Virksomheden havde produktionsstop i 36 timer, før nøddrift var kørende. Der gik 80 timer før man var tilbage på normal produktionsniveau. Det tog virksomheden yderligerere 21 dage, før de havde genetableret alle deres normale forbindelser. På grund af manglende backup, var der dele af data som ikke kunne genskabes korrekt. Konsekvensen af dette var, at der var data, som ikke kunne genskabes.

Kriseberedskabets væsentlige formål

- Sikre indtægter og produktivitet i tilfælde af, at en uforudset hændelse indtræffer.
- Reducere omkostninger som følge af en hændelse ved, at man kan eksekvere hurtigt og har mitigerende tiltag på plads.
- Prioritere tiltag i forhold til kritiske funktioner.
- Sikre en hurtigere tilbagevenden til normalen.
- Sikre organisationens omdømme og relationer til eksterne og interne interessenter med den rette kommunikation.
- Opnå stærkere og bedre beslutningsgrundlag samt deraf færre negative konsekvenser ved uforudsete hændelser.

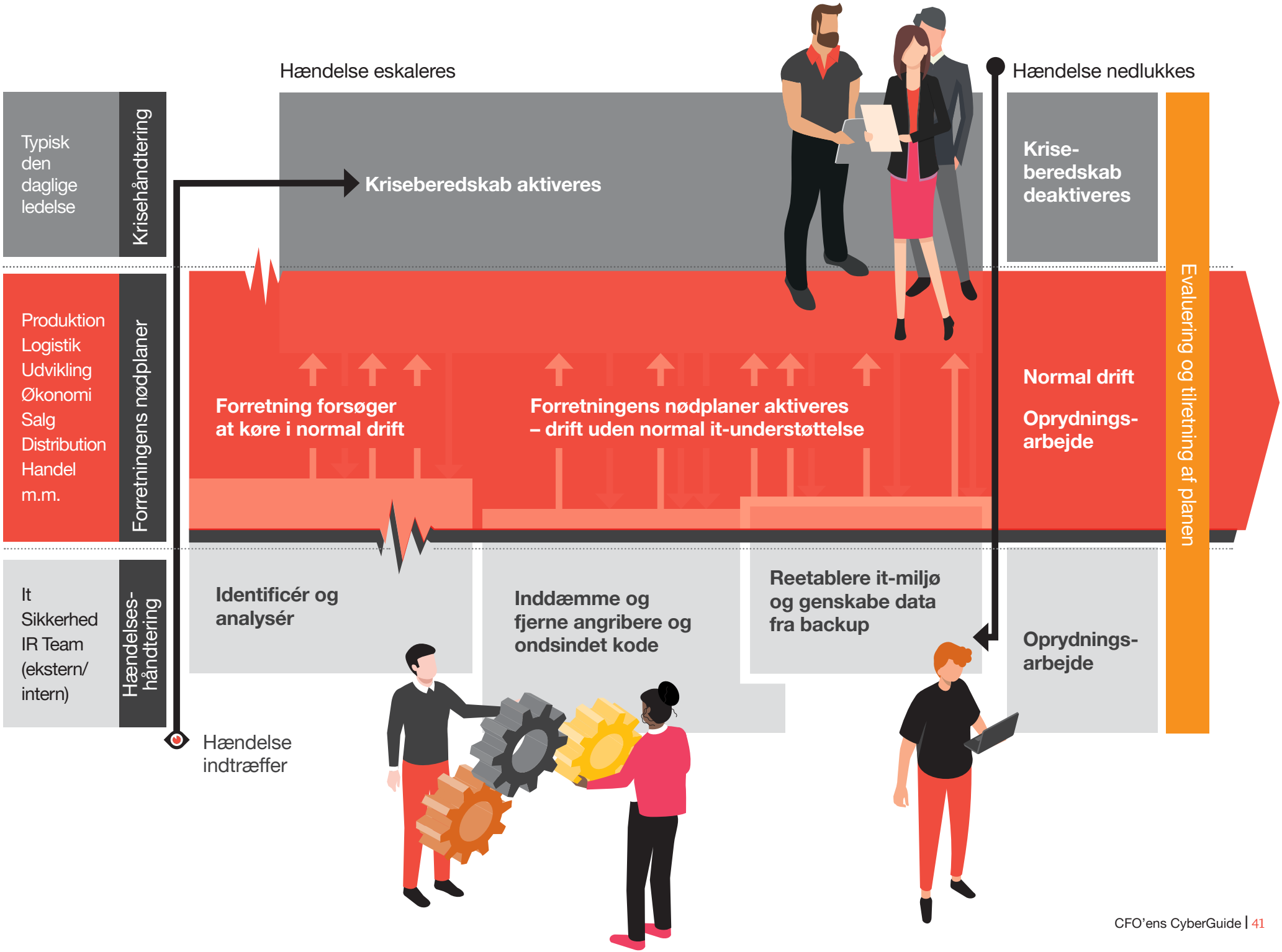
De første trin i Incident Responseprocessen vil typisk være at identificere omfanget af angrebet og isolere det berørte system eller netværk for at forhindre yderligere skade. Herefter vil virksomheden forsøge at genoprette de påvirkede systemer og data fra sikkerhedskopier eller alternative kilder.

Mens nøddriften står på, er det kriseberedskabets opgave at tage beslutninger, der først og fremmest sikrer virksomhedens indtjening under nøddriften. Det er vanskeligt at sige noget generelt om dette, fordi det bl.a. afhænger af virksomhedstype, hvilke systemer der er ramt, forventet nedetid osv. Men for de fleste virksomheder er det vigtigste at sikre leverancer til kunderne og holde indtjeningsgrundlaget i gang. Det er desuden kriseberedskabets opgave at tage beslutninger om kommunikationen internt og eksternt, håndtering af medarbejdere og eventuelle midlertidige forflytninger eller hjemsendelser. Kriseberedskabet skal tage beslutninger under hensyntagen til, at nøddrift kan vare i alt fra nogle få timer til flere uger.

Der er ikke nogen regler for, hvor ofte kriseberedskabet mødes, men det anbefales, at vigtig kommunikation og beslutningsledelse foregår via kriseberedskabet, og at beredskabsledelsen mødes jævnligt for at opdatere hinanden på status og indsatser.

Sådan gør du efter hændelsen: Styrkelse af forsvaret fremadrettet

På baggrund af analyser fra den it-ansvarlige, er det kriseberedskabet, der vurderer, hvornår hændelsen kan lukkes ned, og man kan overgå til normal drift. Tiden, det tager en virksomhed at gå fra nøddrift til normal drift efter et cyberangreb, afhænger af forskellige faktorer, herunder omfanget og kompleksiteten af angrebet, hvilke systemer og data der er blevet påvirket, og hvor godt forberedt virksomheden var på angrebet. Når virksomheden har sikret sig, at alle berørte systemer og data er blevet genoprettet, og eventuelle sikkerhedsmæssige sårbarheder er blevet løst, kan virksomheden gradvist genoptage normal drift. Det er vigtigt, at virksomheden fortsætter med at monitorere systemer og data for eventuelle resterende problemer


Hændelse eskaleres
Hændelse nedlukkes
Typisk den daglige ledelse
Krisehåndtering
Kriseberedskab aktiveres
Krise-beredskab deaktiveres
Produktion
Logistik
Udvikling
Økonomi
Salg
Distribution
Handel
m.m.
Forretningens nødplaner
Forretning forsøger at køre i normal drift
Forretningens nødplaner aktiveres – drift uden normal it-understøttelse
Normal drift
Oprydnings-arbejde
Evaluering og tilretning af planen
It
Sikkerhed
IR Team
(ekstern/
intern)
Hændelses-håndtering
Identificér og analysér
Inddæmme og fjerne angribere og ondsindet kode
Reetablere it-miljø og genskabe data fra backup
Oprydnings-arbejde
Hændelse indtræffer

eller nye forsøg på angreb og træffer passende foranstaltninger for at minimere risiko for fremtidige angreb.

En del af processen er, at der foretages en "forretningsmæssig oprydning" i tillæg til den tekniske oprydning, der er beskrevet herunder. Det gælder fx opdatering og udligning af dataregistreringer, transaktioner, lagerføring m.v., der er foretaget i nøddriftsperioden. Som en del af oprydningsarbejdet produceres en kort opsummering med de væsentligste fund om hændelsens forløb og karakteristika (hv-spørgsmål). Dette for både at dokumentere hændelsen og forbedre effektiviteten af virksomhedens Incident Response evner fremadrettet. Svarene på nogle af spørgsmålene vil ofte føre til behovet for at forstå mere detaljeret, hvordan eller om virksomhedens Incident Response fungerede.

At få en klar forståelse af, hvad der fungerede, og hvad der ikke fungerede, giver mulighed for at konkretisere forbedringsmuligheder og forstå, hvordan man bedst kan udnytte ressourcerne på cybersikkerhed bedst muligt. På baggrund heraf kan man udarbejde en plan, der derefter kan indarbejdes i et eksisterende cybersikkerhedsprogram eller ændres til andre planlagte sikkerhedsaktiviteter.

Tal om jeres erfaringer på en workshop

- Gennemgå hændelsesforløbet i detaljer
- Forstå årsagen til cyberhændelsen og udfaldet af denne
- Identificér kritiske sikkerhedsfunktioner
- Opnå enighed om effektiviteten af Incident Response-processen og de eventuelle nødvendige ændringer
- Opdatér Incident Response-processen om nødvendigt
- Identificér påkrævede test- og træningsprogrammer.

Kapabilitetsanalyse

- Analysér den nuværende tilstand af de identificerede kritiske sikkerhedsfunktioner
- Identificér huller eller mangler i forhold til erfaringer fra hændelsen
- Vurdér hvordan de kritiske sikkerhedsfunktioner kan forbedres
- Vurdér potentielle tiltag, der kan minimere risici fremadrettet.

Projektplanlægning

- Identificér nødvendige aktiviteter og investeringer til at reducere eventuelle huller og/eller mangler i eksisterende kritiske sikkerhedsfunktioner
- Beskriv aktiviteterne i specifikke projektforslag og organisér dem i en overordnet tidsplan/rækkefølge.

Forslag: **Sådan kommer du videre**

+ Tag en dialog i den daglige ledelse, om I selv har de tekniske kompetencer i virksomheden, eller om I skal lave en aftale med ekstern samarbejdspartner.
+ Få vurderet behovet for 24/7 eller 08-16 beredskab.
+ Skab et overblik over virksomhedens kronjuveler - hvilke er mest tidskritiske at få tilbage til drift, og kan I selv få disse tilbage eller er det via eksterne leverandører?
+ Hvis I har kritiske applikationer hos leverandører, hvordan er deres beredskab, og hvilke aftaler har I med dem?

+

Opsummering: Hvem gør hvad, når hændelsen sker?

+ At være forberedt og kende egen forretning er nøgleordet for at kunne komme hurtigt tilbage i drift og undgå datatab.
+ Det er vigtigt at kunne reagere hurtigt og effektivt, både hos it-afdeling og den it-ansvarlige, men også hos den daglige ledelse, så man kan identificere hændelsen og skabe et overblik over omfang af angrebet.
+ Hvis man ikke har de rette tekniske kompetencer i virksomheden, er det vigtigt at have lavet en aftale med ekstern partner, som kan rykke ud og hjælpe, når hændelsen sker.

> “ Alle virksomheder skal være i stand til hurtigt at reagere på og komme sig efter et cyberangreb. Det kræver, at organisationen er godt forberedt og har styr på sin Incident Response.

Cybersikkerhed: Vigtig viden om

I dette nye afsnit* zoomer vi ind på samarbejdet mellem CFO og bestyrelse. Du får bl.a. indblik i, hvilke anbefalinger, der ligger i forhold til bestyrelsesarbejdet omkring cybersikkerhed. Du får desuden viden og værktøjer, så du som CFO kan facilitere samarbejdet med bestyrelsen optimalt og skabe det bedste grundlag for et effektivt samspil, der gør, at virksomheden står stærkest i kampen mod cyberhændelser.

CFO'ens samspil med bestyrelsen

I en verden, hvor cyberkriminalitet i stigende grad er en del af virksomhedens udfordringer, udviser de mest ansvarlige bestyrelser en øget interessse for, hvordan ledelsen adresserer disse komplekse trusler og stiller specifikt krav til aktiv styring af og rapportering om risici på området.

Topledere og bestyrelser er bevidste om, at cyberrisikoen kræver stor opmærksomhed. Bestyrelsen er i den forbindelse en af de væsentligste interne interessenter for CFO'en, og det er CFO'ens opgave at beskrive virksomhedens risikobillede, samt hvilke aktiviteter der bør prioriteres for at adressere risiciene.

Det er en fælles opgave for CFO og bestyrelse at sikre, at bestyrelsesmedlemmerne løbende modtager tilstrækkelig information fra direktionen – og ikke mindst også, at der sker en løbende sparring mellem direktion og bestyrelse på cyberområdet og relaterede risikoområder, herunder GDPR. Hensigten er, at begge parter til enhver tid kender risiko, strategi og status for cybersikkerheden i virksomheden.

Bestyrelsens ansvar – og CFO'ens forpligtelser

Det er bestyrelsens ansvar at sikre værdiskabelse og konkurrenceevne samt at beskytte selskabets værdier, både på kort og langt sigt (Selskabsloven § 115). Bestyrelsen er ansvarlig for selskabets strategi og opfølgning på gennemførelse af strategien – også når det gælder cybersikkerhed, da en cyberhændelse i værste fald kan påvirke såvel virksomhedens bundlinje og evne til at nå de strategiske mål, og i mange sammenhænge også have skadelige konsekvenser for samfund og borgere. Det er derfor en af CFO'ens væsentlige opgaver at dokumentere og rapportere løbende overfor bestyrelsen på virksomhedens cybersikkerhedsstrategi og den sikkerhedsrejse, organisationen er på. CFO'en skal også sørge for at orientere bestyrelsen, hvis et område ikke er prioriteret tilstrækkeligt. Derudover skal CFO'en sørge for, at der løbende følges op på rapporteringen i forhold til den handlingsplan, der er lagt som fundament for cyberstrategien.

PwC's Cybercrime Survey 2021 viser, at kun 15 % af bestyrelsesmedlemmerne angiver, at sammensætningen af bestyrelsens kompetencer i høj grad giver dyb nok viden om cyber- og informationssikkerhed. Yderligere svarer 61%, at de ikke modtager træning i cyber- og informationssikkerhed, hvilket er en væsentlig forbedring i forhold til 2020, hvor 89% angav, at der ikke var etableret et cybertrænings- og uddannelsesprogram. Læs mere om Cybersikkerhed i bestyrelser **her**.

*Udgivet december 2021

+

Case: **Håndtering af cybersikkerhed og rapportering til bestyrelsen**

Bestyrelsen i en produktionsvirksomhed ønskede indblik i, hvordan virksomheden adresserer truslen fra cyberkriminalitet, og specifikt hvordan den ville håndtere et omfattende ransomware-angreb.

Ledelsen i virksomheden fik foretaget en ekstern vurdering af dets cyberforsvar, samt en risikovurdering. På baggrund af denne vurdering fremlagde CFO'en en plan for bestyrelsen om igangsættelse af en række tiltag for at nedbringe risikoen, bl.a. en større segmentering af netværket, forbedret sikkerhed på medarbejdernes PC'ere, en række awareness tiltag overfor medarbejderne, en opdatering af virksomhedens beredskab samt en øget indsats i forhold til leverandører. Investeringen blev godkendt af bestyrelsen, som ønskede løbende rapportering på aktiviteterne og på risikobilledet.

På hvert bestyrelsesmøde (kvartalsvis) i en 2½ årig periode præsenterede ledelsen en kort status på de enkelte aktiviteter/projekter, samt berettede om eventuelle udfordringer eller hændelser. Én gang om året blev der afsat en time til at diskutere status på aktiviteterne, resultat af risikovurderinger samt rapportering fra eksterne parter, der kunne validere, om de implementerede tiltag havde den ønskede effekt på at nedbringe risikoen. Yderligere tiltag og justering af igangværende projekter blev afstemt med og godkendt af bestyrelsen for det kommende år.

6 områder, der skal rapporteres på til bestyrelsen

- Risikovurdering og sårbarhed
- Risikoappetit og strategi
- Planer, processer og beredskab
- Rapportering og kontrol
- Kultur og mennesker
- Kompetencer og organisering

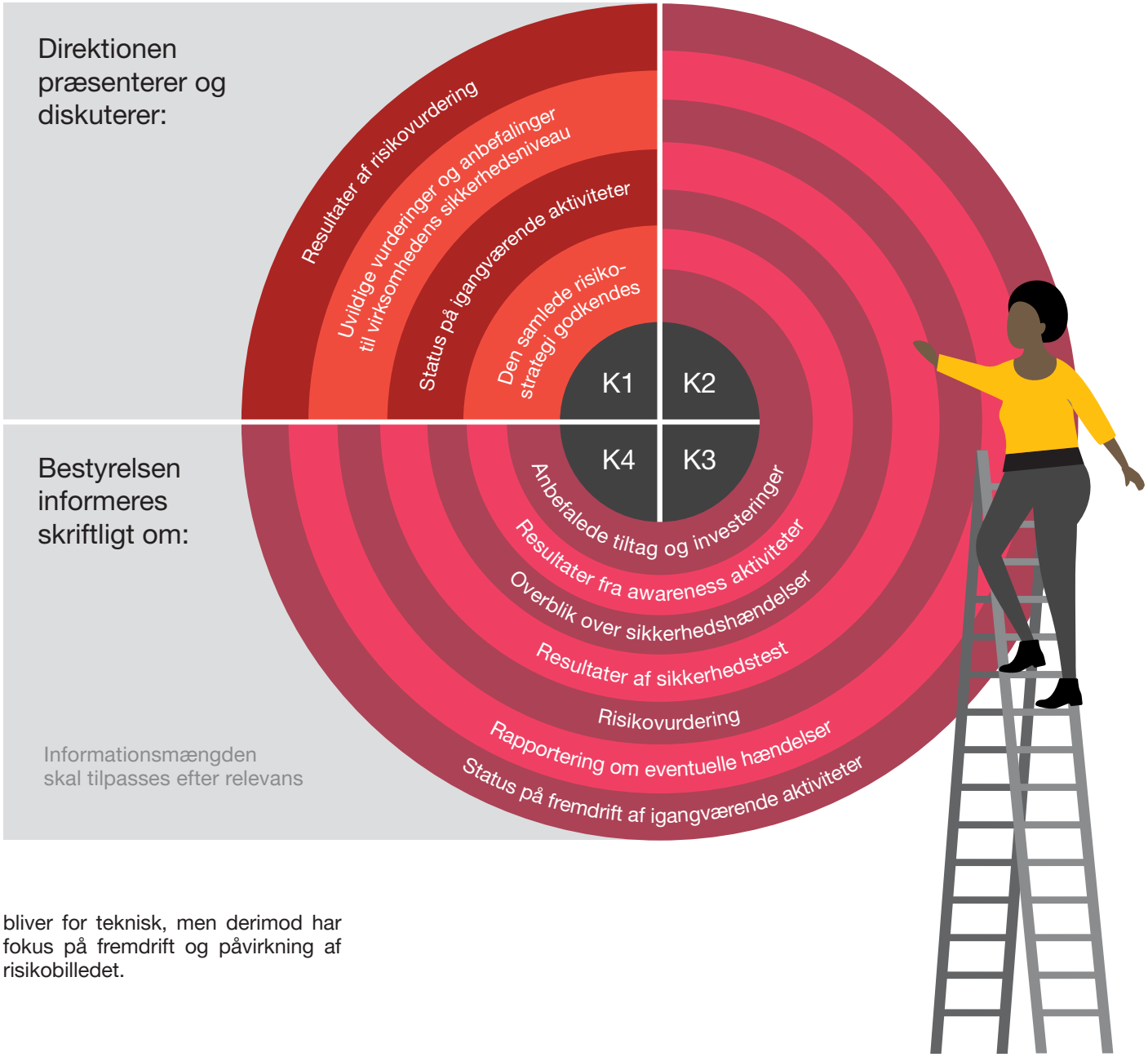
Cybersikkerhed bør integreres i bestyrelsens årshjul

Når du som CFO planlægger rapporteringen til bestyrelsen, skal samme principper som ved andre rapporteringer til bestyrelsen følges. Der er faktorer, der rapporteres på i faste intervaller, og der er faktorer som rapporteres på løbende, og når det er relevant. Det gøres typisk ved at, ledelsens rapportering til bestyrelsen kobles op på de faste årlige bestyrelsesmøder, og ved at udarbejde et årshjul, så ledelse og bestyrelse har forventningsafstemt omkring rapportering og struktur.

Det anbefales fx, at bestyrelsen minimum årligt modtager en risiko- og sårbarhedsvurdering på virksomheden fra direktionen. Desuden bør bestyrelsen minimum årligt tage stilling til virksomhedens risikoappetit, og det er bestyrelsens ansvar at godkende den samlede risikostrategi, inklusive de specifikke aktiviteter, som virksomheden ønsker at igangsætte for at forbedre processer, styrke arkitekturen, øge god adfærd og dermed reducere det samlede risikobillede.

Derudover er det også direktionens opgave at sikre, at bestyrelsen modtager relevant rapportering forud for hvert bestyrelsesmøde. En rapportering, der aftales indbyrdes, men kan indeholde bl.a. risikovurdering, resultater af sikkerhedstest, overblik over sikkerhedshændelser, inklusiv GDPR-relaterede hændelser, resultater fra awareness aktiviteter, anbefalede tiltag og investeringer. Ledelsen skal sikre, at denne rapportering ikke bliver for teknisk, men derimod har fokus på fremdrift og påvirkning af risikobilledet.

Virksomhedens cyberstrategi behandles årligt

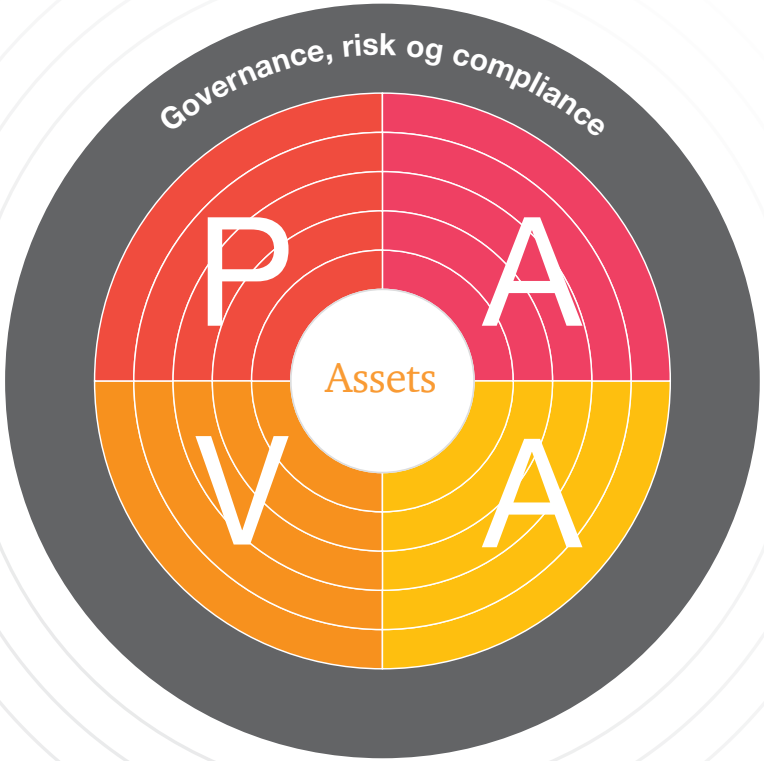


> “ Cybersikkerhed er et vigtigt element i at drive ansvarlig virksomhed. Det er ledelsens rolle at løfte dialogen om cybersikkerhed og ansvarlighed ikke bare i virksomhedens eget risikoperspektiv, men også forhold til etiske forpligtelser.

+

Få struktur på rapportering med PAVA

PwC's PAVA-koncept er en hjælp til at strukturere arbejdet med cybersikkerhed i virksomheden. PAVA er samtidig et ganske godt værktøj til at strukturere rapporteringen til bestyrelsen. PAVA-konceptet kan benyttes af både bestyrelse og ledelse (CFO) til at skabe klarhed over den samlede cyberrisiko, -strategi og handlingsplan på en måde, hvor man samtidig taler samme sprog – og dermed har optimeret processen. Det giver bl.a. bestyrelsen den nødvendige referenceramme til at stille krav til virksomhedens ledelse. Og det giver ledelsen en mulighed for at dokumentere sit arbejde overfor bestyrelsen hurtigt, effektivt og meningsfuld.



Governance, risk og compliance: Kan ledelsen demonstrere den rette governance og risikostyring?

CFO'en skal dokumentere, at man har etableret en governance omkring cybersikkerhed. At man bl.a. har et sikkerhedsudvalg eller en styregruppe for cybersikkerhed, at man har integreret de rette nøglepersoner i organisationen i risikostyringen, og at man har forankret ansvaret for cybersikkerhed i direktionen. CFO'en skal desuden sørge for, at dialogen involverer ledelsesmedlemmer fra forretningen, it og digitalisering samt eventuelt Risk Management.

CFO'en bør også kunne dokumentere, at man har foretaget risikovurdering og har en proces for risikostyring. Dette indebærer bl.a. at rapportere risici til bestyrelsen og drøfte mulige konsekvenser. Forud for dette ligger en opgave i at identificere virksomhedens "Kronjuveler" – fx kritiske forretningsprocesser og it-systemer som virksomheden er afhængig af; hvad konsekvensen potentielt vil være, hvis man rammes af et nedbrud eller en kompromittering af forretnings- eller persondata; at identificere sårbarheder/svagheder i processer/organisation/teknologi og lave en handlingsplan for udbedring af disse. Kan ledelsen acceptere restrisikoen? Bør man indgå cyberforsikring for at overføre dele af "risikoen" til en tredjepart?

Cybersikkerhed er et vigtigt element i at drive ansvarlig virksomhed. Det er også ledelsens rolle at løfte dialogen om cybersikkerhed og ansvarlighed ikke bare i virksomhedens eget risikoperspektiv, men også i forhold til etiske forpligtelser. At reducere risikoen for at skabe samfundsmæssige problemstillinger, fx som brud på menneskerettigheder, afbrydelser i forsyningskæder, miljøproblemstillinger eller påførelse af store økonomiske tab. Cybersikkerhed er et væsentligt element, man som virksomhed skal forholde til sig i forhold til ESG-agendaen.

(P) Processer: Er der etableret processer, politikker og procedurer?

Her bør CFO'en dokumentere, at virksomheden har en overordnet cyber- og informationssikkerhedspolitik, at der er politikker for bl.a. bruger- og adgangsstyring, at der er testede beredskabs- og kommunikationsplaner for håndtering af cyberhændelser, strømnedbrud osv., og at der er indarbejdet processer for risikovurdering og risikohåndtering samt krisehåndtering. Der bør være dokumentation for, at der er klare ansvarsfordelinger og opgavebeskrivelser, og at nøglemedarbejdere kender til roller, ansvar og planer.

(A) Arkitektur:
Har virksomheden etableret infrastrukturen med sikkerhed for øje?

CFO'en skal dokumentere overfor bestyrelsen, at man har tænkt sikkerhed ind i den teknologiske infrastruktur og i de teknologivalg, man har foretaget i virksomheden. Det indebærer bl.a., at virksomhedens systemer og infrastruktur beskytter virksomheden optimalt mod cyberkriminalitet. At sikkerhedskravene til infrastruktur afspejler risiko og risikoappetit. At man har styr på eventuelle leverandørers sikkerhedsniveau.

(V) Validering:
Kan det påvises, at organisatoriske og tekniske kontroller er effektive?

CFO'en bør kunne demonstrere, at sikkerhedsniveauet efterprøves regelmæssigt.

CFO'en bør således kunne vise, at virksomheden efterprøver, hvorvidt medarbejderne har et tilstrækkeligt kendskab til god sikkerhedspraksis, og om de er opmærksomme på truslerne, fx gennem phishing-test.

Det skal dokumenteres, at kritiske systemer testes regelmæssigt med henblik på at identificere svagheder.

Rapporteringen for bestyrelsen bør vise, at vigtige sikkerhedsprocesser gennemføres effektivt, fx at backup af data foretages og er valide, at kritiske systemer er opdateret, at adgange til systemer og data afspejler et arbejdsbetinget behov.

CFO'en skal i sin rapportering påvise, at leverandører lever op til deres forpligtelser, herunder god sikkerhedspraksis og virksomhedens krav.

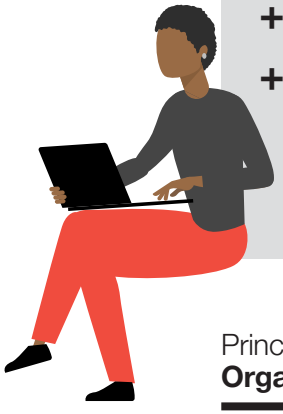
Direktionen bør regelmæssigt fremvise en rapportering, som dokumenterer en tilstrækkelig uvildig validering af virksomhedens beskyttelse på alle ovenstående punkter. I den forbindelse kan det være en fordel at inddrage eksterne parter til at gennemgå virksomhedens beredskab og foretage uvildige vurderinger af, om virksomheden er beskyttet tilstrækkeligt mod cyberhændelser og effekterne heraf.

(A) Adfærd:
Er medarbejderne gjort eksplicit opmærksomme på deres ansvar i forhold til beskyttelse af virksomhedens vigtigste informationer?

CFO'en skal dokumentere, at virksomheden har formuleret medarbejdernes ansvar for sikkerhed og persondatabeskyttelse tydeligt, fx i en politik for acceptabel brug af virksomhedens aktiver ("acceptable use policy"), at der er indarbejdet programmer for uddannelse og træning af hele organisationen, ledelse, medarbejdere og bestyrelse i relation til cyber- og informationssikkerhedstræning og -awareness. Det skal dokumenteres, hvilke test der bliver gennemført og hvorfor.

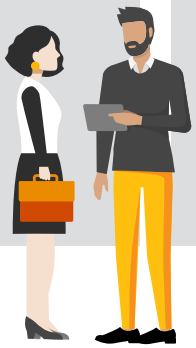
Princip 1:
Fokus på forretningskritiske cyberrisici

- Bestyrelsesmedlemmer behøver ikke at være eksperter i cybersikkerhed, men de har brug for tilstrækkelig viden om cyberrisikoen. Denne viden bør CFO og direktion sikre, at bestyrelsen hele tiden har.
- Bestyrelsesmedlemmer bør sikre, at virksomheden prioriterer investeringer i de rigtige initiativer og kapaciteter for cybersikkerhed. Det er direktionens opgave at udføre disse investeringer og dokumentere dette for bestyrelsen.
- Cyberrisikostyring bør fokusere på de ting, der kan have en reel kritisk indvirkning på virksomheden.
- Bestyrelsesmedlemmer bør have regelmæssig information fra direktionen om, hvordan kritiske cyberrisici adresseres.



Princip 2:
Organisering af sikkerhedsfunktionen

- Bestyrelsesmedlemmer bør sikre, at der etableres en stærk organisation omkring sikkerhedsarbejdet.
- Bestyrelsesmedlemmer bør sikre, at der defineres klare roller og ansvar for sikkerheden (governance, især set i forhold til rapportering til bestyrelsen).
- Bestyrelsesmedlemmer bør sikre, at der fastlægges en klar ledelsesstruktur for alt sikkerhedsarbejde i organisationen (ansvar og risiko-ejerskab i diverse forretningsenheder).
- Bestyrelsesmedlemmer bør sikre, at der udpeges én kontaktperson i bestyrelsen/topledelsen, der kan og skal rapportere løbende til hele bestyrelsen.



Princip 3:
Validér implementeringen af cybersikkerhedsinitiativerne

- Bestyrelsesmedlemmer bør sikre, at der løbende foretages verifikation af effektiviteten og tilstrækkeligheden af sikkerhedstiltagene.
- Bestyrelsesmedlemmer bør regelmæssigt modtage rapporter, der viser, at sikkerhedsinitiativet er effektivt (rapportering og handlingsplan).
- Bestyrelsesmedlemmer bør periodisk anvende en uvildig part til at kontrollere effektiviteten af initiativerne.

Princip 4:
Forbered dig på det værste – øvelser med simulerede cyberangreb

- Bestyrelsesmedlemmer bør være forberedt på at håndtere et sikkerhedsbrud og kan med fordel være en del af regelmæssige beredskabsøvelser med simulerede cyberangreb, så de kan træne deres rolle i forhold til kommunikation med eksterne interessenter, såvel som øve sig på nogle af de svære dillemaer, man kan komme i:
  - Vil vi betale en løsesum for at få adgang til vores data igen efter et ransomware angreb?
  - Hvornår er virksomheden truet på dens eksistens?
- Bestyrelsesmedlemmer bør sikre, at der er en plan for håndtering af sikkerhedsbrud.
- Bestyrelsesmedlemmernes rolle i relation til sikkerhedsbrud skal være afstemt og defineret.

Forslag:
Sådan kommer du videre

- Etablér en systematisk rapportering i forhold til bestyrelsen omkring cyberstrategi, risiko og sårbarhed.
- Sørg for at afstemme rapportering med bestyrelsen, herunder hvordan rapportering skal forekomme i relation til de planlagte bestyrelsesmøder.
- Orientér dig via de anbefalinger til bestyrelsen, der ligger fra Bestyrelsesforeningen samt PwC's Bestyrelseshåndbog.

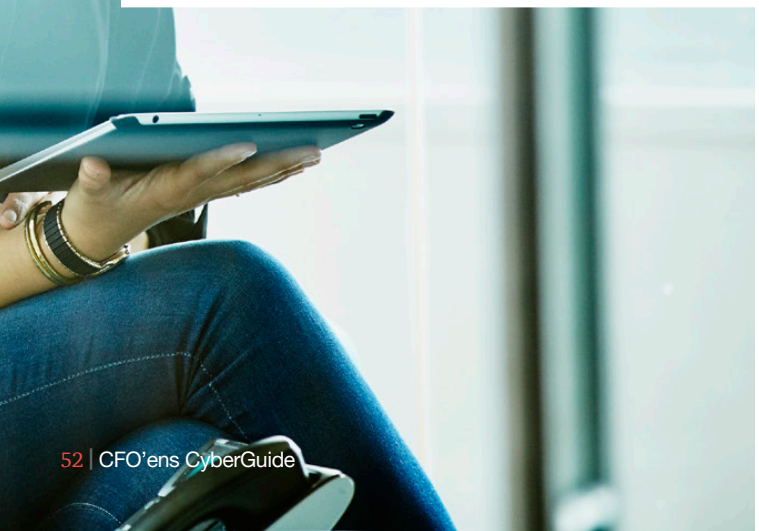
+

Opsummering:
Samspillet mellem CFO og bestyrelse

- Det er CFO'ens opgave at beskrive virksomhedens risikobillede for bestyrelsen og fremhæve de aktiviteter, der bør prioriteres for at adressere risiciene. Desuden bør bestyrelsen årligt – eller ad hoc ifm. ændringer i forretningsstrategien – tage stilling til virksomhedens risikoappetit.
- CFO'ens opgave er desuden at dokumentere og rapportere overfor bestyrelsen på virksomhedens cybersikkerhedsstrategi og handlingsplaner.
- Det er en væsentlig opgave for CFO'en løbende at orientere, hvis et område ikke er prioriteret tilstrækkeligt. Og anbefale tiltag, der bør iværksættes.
- Det anbefales, at bestyrelsen minimum årligt modtager en risiko- og sårbarhedsvurdering på virksomheden fra direktionen.

Cyberforsikring – overførsel af risiko til tredjepart

Formålet med dette afsnit er at se nærmere på cyberforsikringer. I dette afsnit hjælper vi med at skabe klarhed over, hvordan CFO og direktion kan anvende forsikringer som værktøjer til at overføre risiko til tredjepart, og på denne måde reducere noget af den skade, der kan opstå som følge af en cyberhændelse. I afsnittet ser vi desuden på, hvad man som direktion og bestyrelse bør være særligt opmærksom på, inden man tegner en forsikring, og hvordan man som ledelse forbereder sig bedst muligt for at få størst mulig værdi af en cyberforsikring.



Når det handler om cybersikkerhed, så er det vanskeligt for ledelsen at sikre sin virksomhed mod at blive ramt af cyberhændelser og eventuelle konsekvenser heraf. Det kræver en omfattende sikkerhedsindsats. Og selv da risikerer man at blive ramt. Derfor kan det for langt de fleste virksomheder være en god idé at tegne en cyberforsikring, hvis uheldet skulle være ude. Ligesom man tegner forsikringer på andre områder. På den måde kan man overføre noget af risikoen til tredjepart, nemlig forsikringsselskabet. Men det er en fordel, hvis man har sit cyberstrategiske fundament på plads, inden man tegner forsikringen.

Som vi tidligere har beskrevet under afsnittet "Det digitale trusselsbillede", har næsten 6 ud af 10 danske virksomheder (58 procent), ifølge PwC's Cybercrime Survey, været udsat for et cyberangreb det seneste år. I samme survey vurderer næsten 9 ud af 10 topledere (88 procent), at cybertruslen er deres væsentligste bekymring. Sammenholdt med de omfattende følger, der ofte er, når virksomheder rammes af en cyberhændelse, er det indlysende, at CFO og direktion bør se på, hvordan man kan tage sine forholdsregler og minimere risiko for virksomheden, også når det gælder forsikringer. I denne guide har vi indtil videre fokuseret på at give CFO'en og den øvrige ledelse en række værktøjer til at identificere og beskytte virksomhedens kronjuveler og sikre dem mod cyberhændelser generelt. Vi har også givet gode råd til at minimere de negative afledte konsekvenser, bl.a. ved at opbygge et passende beredskab.

Forsikringer er endnu et værktøj, som virksomhedens ledelse kan bruge i håndteringen af cyberrisici. Når vi ser på cyberforsikringer, og hvordan de kan benyttes som et værktøj, så er det, fordi forsikringer kan bruges til at overføre risiko fra virksomheden selv til tredjepart og derved reducere skaden ved en given cyberhændelse.

The 4T's of Risk Management

Man taler typisk om "The 4T's of Risk Management - Tolerate, Terminate, Treat, Transfer", hvor Transfer refererer til forsikring. Når man som CFO og ledelse beslutter at tegne en eller flere cyberforsikringer, er det

vigtigt, at man skelner mellem cyberforsikring og de aktiviteter, der skal forhindre, at cyberhændelser opstår. Begge aktiviteter er vigtige. Mange opfatter fejlagtigt en cyberforsikring som et alternativ til at sikre sin virksomhed mod cyberhændelser. Men det er vigtigt at understrege, at man ikke slipper for at sikre sin virksomhed mod cyberangreb og følgerne heraf blot ved at tegne en cyberforsikring. Nærmere tværtimod: En god og effektiv forsikring kræver, at man har gjort sit forarbejde omkring cybersikkerhed på forhånd og kender virksomhedens risikobillede.

Det kræver fokus på det sikkerhedsmæssige fundament at få det rette udbytte af en forsikring

Forsikringsselskaberne stiller i dag øgede krav til dokumentation for, at man som virksomhed har styr på sikkerheden og gør, hvad der er rimeligt for at beskytte sig mod de hændelser, der gør forsikringerne relevante. Man kan sammenligne det med en hvilken som helst anden forsikring. Jo bedre, du fx har sikret din bolig - ved bl.a at installere røgalarmer, særlige låse og indbrudsalarm - des bedre er du stillet, når du skal tegne en indboforsikring eller en husforsikring. Sådan er det også, når du skal skal tegne en cyberforsikring.

Hvis du kan dokumentere, at du har fundamentet på plads - dvs. at du har etableret et stærkt teknisk kontrolmiljø, sikkerhedspolitikker, en beredskabsplan, og at du træner dine medarbejdere, m.v. - så vil din forsikringspræmie også påvirkes positivt.

The 4T's of Risk Management

Tolerate

Der er risici, som man accepterer, fordi sandsynligheden for en hændelse er lav og konsekvenserne små. Her er løbende overvågning af risikoen tilstrækkelig. Et eksempel er, at de fleste virksomheder oplever konstant port-scanning af deres eksterne firewall, hvor størsteparten af disse er ufarlige.

Terminate

Nogle gange kan risikoen ved en aktivitet i virksomheden være så stor, at man som ledelse vurderer, at aktiviteten skal indstilles. Et eksempel er en virksomhed, der sælger sundhedsprodukter og overvejer at lave en portal til udveksling af informationer med samarbejdspartnere. Virksomhedens jurist vurderer, at det vil være for svært at adskille data, så de ikke indeholder følsomme persondata. Derfor udsætter man portalløsningen, indtil en passende sikring kan etableres.

Treat

I langt de fleste tilfælde vil man som ledelse handle på de mest alvorlige risici og sørge for at reducere sandsynligheden for, at cyberhændelser opstår - og samtidig handle på konsekvenserne, hvis de gør. Et eksempel er, at man har vurderet, at en hændelse vil have uacceptable økonomiske konsekvenser, hvis produktionen er ude af drift i mere end 10 arbejdsdage. Man implementerer derfor yderligere tekniske og organisatoriske kontroller og nedbringer dermed sandsynligheden for, at et så alvorligt driftsnedbrud kan forekomme.

Transfer

Man kan overføre risiko til tredjepart, for eksempel ved at tegne en forsikring. Man bør dog huske, at forsikringen ikke fjerner risikoen og derfor heller ikke fratager ledelsen for ansvar for at beskytte virksomheden mod sådanne hændelser.

+

Case: **Produktionsvirksomhed mødt med skærpede krav til cybersikkerhed**

Ledelsen i en dansk produktionsvirksomhed bliver kontaktet af sit forsikringsselskab, der stiller en række krav til cybersikkerheden i virksomheden. Forsikringsselskabet vil ikke gentegne forsikringen, medmindre virksomheden kan påvise en opdateret og afprøvet beredskabsplan, samt at adgangskontrol til systemer i produktionsmiljøet styrkes væsentligt. Forsikringsselskabet meddeler, at indtil disse to faktorer er bragt i orden, vil forsikringen være omfattet af en ekstraordinær høj selvrisiko.

Forudsætningen for den optimale forsikring er således, at CFO og direktion har indsigt i virksomhedens risikobillede, kender til virksomhedens kronjuveler, og hvordan disse er beskyttet. Det kræves af ledelsen, at man har et klart indblik i de risici, virksomheden er udsat for, og at man har taget stilling til virksomhedens risikoappetit. Desuden kræves det, at man kan dokumentere overfor forsikringsselskabet, at man har gjort, hvad man kan for at sikre virksomheden. Man kan med andre ord sige, at en god forsikring kræver, at man har sit cyberstrategiske fundament på plads.

Stigende krav og dyrere forsikringer

Ligesom cybersikkerhed er rykket højere op på dagsordenen hos virksomhederne, så har forsikringsselskaberne over de seneste par år oplevet, at de udbetaler flere og større erstatningssummer til virksomheder, der har været ramt af cyberhændelser. Derfor har forsikringsselskaberne revurderet deres egen risiko og stiller nu større krav til virksomhederne om at dokumentere, hvordan de arbejder med sikkerhed. I dag ses det ofte, at virksomheder, der ikke har gjort tilstrækkeligt for at beskytte virksomheden, enten bliver afvist af forsikringsselskabet eller mødt med en forsikringspræmie, der er omkostningstung, fordi risikoen for forsikringsselskabet vurderes som meget høj, eller forsikringen udstedes med en høj selvrisiko (op til 75 procent). Der er set eksempler på, at man ikke får den erstatning, man forventede, hvis det viser sig, at den basale sikkerhed har været for dårlig, og at man ikke har været tilstrækkelig opmærksom på betingelserne.

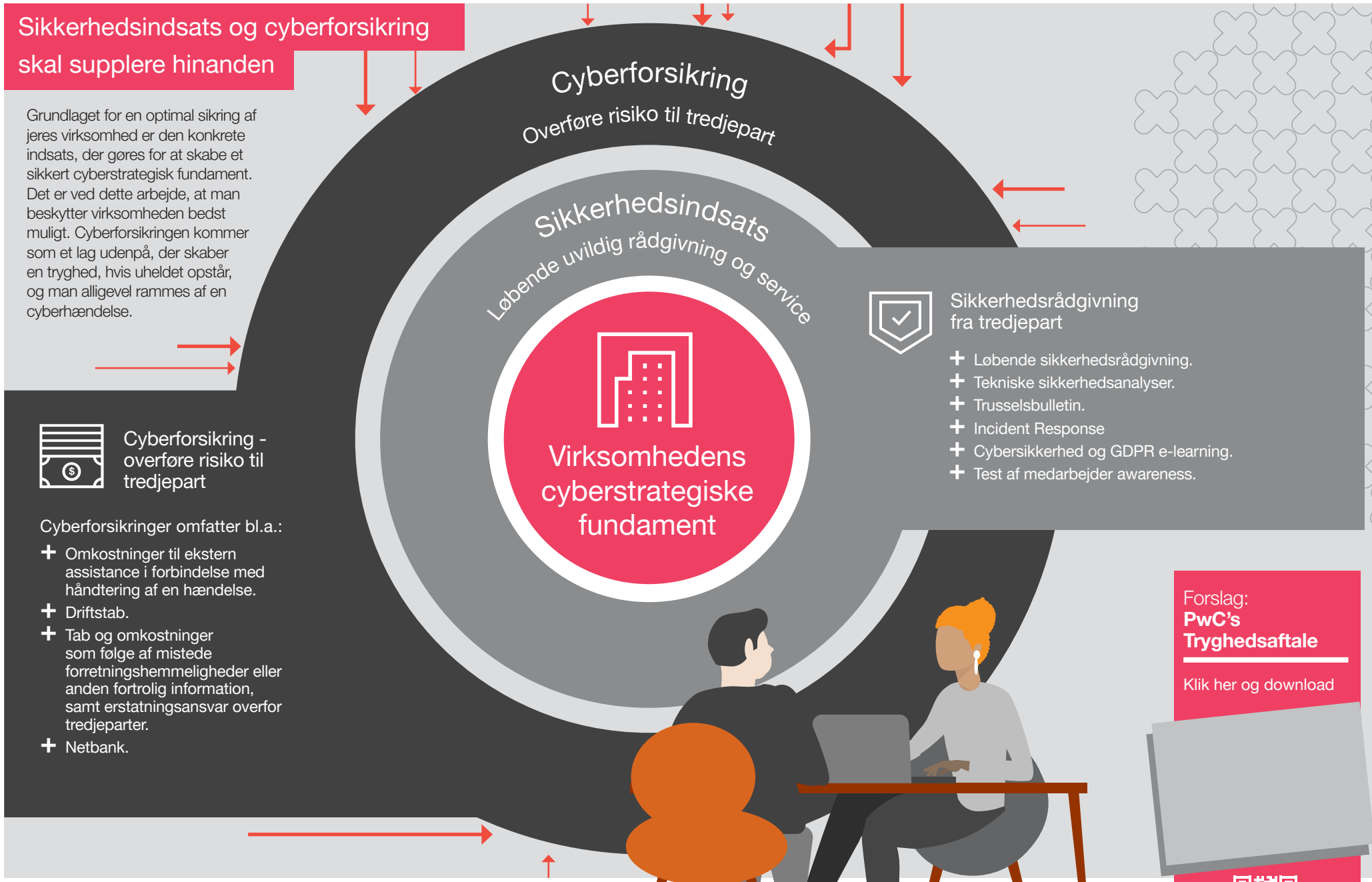
Få styr på trusler og risici, inden I tegner en forsikring

Ledelsen skal tage stilling til, hvilken forsikring og dækning der er relevant. Her handler det indledningsvist om at foretage en trussels- og risikovurdering, herunder hvad der er kritiske aktiver, hvordan de enten er beskyttet eller bør være beskyttet, samt hvilke konsekvenser der er ved en kompromittering. Ledelsen skal sikre, at der løbende foretages sikkerhedsanalyser, som er med til at skabe overblik over de tekniske sårbarheder og derudover løbende uddanne og træne medarbejderne i en adfærd, der understøtter cybersikkerhed i virksomheden.

I den daglige drift og i takt med at analyserne gennemføres, skal foranstaltningerne implementeres og holdes opdateret, hvor det vurderes, at der er behov. Desuden er det vigtigt at forstå de krav, der stilles til virksomheden for at tegne forsikringen. Man bør altså have stor indsigt i egen virksomhed, og hvad man konkret ønsker fra en forsikring. Dette skal holdes op mod de forsikringsprodukter, der findes på markedet.

Sikkerhedsindsats og cyberforsikring skal supplere hinanden

Grundlaget for en optimal sikring af jeres virksomhed er den konkrete indsats, der gøres for at skabe et sikkert cyberstrategisk fundament. Det er ved dette arbejde, at man beskytter virksomheden bedst muligt. Cyberforsikringen kommer som et lag udenpå, der skaber en tryghed, hvis uheldet opstår, og man alligevel rammes af en cyberhændelse.



Cyberforsikring - overføre risiko til tredjepart

Cyberforsikringer omfatter bl.a.:

- Omkostninger til ekstern assistance i forbindelse med håndtering af en hændelse.
- Driftstab.
- Tab og omkostninger som følge af mistede forretningshemmeligheder eller anden fortrolig information, samt erstatningsansvar overfor tredjeparter.
- Netbank.

Sikkerhedsrådgivning fra tredjepart

- Løbende sikkerhedsrådgivning.
- Tekniske sikkerhedsanalyser.
- Trusselsbulletin.
- Incident Response
- Cybersikkerhed og GDPR e-learning.
- Test af medarbejder awareness.

Forslag:
PwC's Tryghedsaftale

Klik her og download

Hvilken forsikring skal I vælge?

De forskellige cyberforsikringer på markedet har forskellige dækninger, og forsikringsselskaberne stiller forskellige krav til virksomheden. Derfor er det vigtigt for ledelsen at få klarhed over, hvilke dækninger der er relevante for virksomheden.

Da forsikringernes omfang og vilkår kan variere mellem de enkelte selskaber, anbefaler PwC, at virksomheden sammen med en forsikringsmægler afdækker egne behov og sikrer, at den tilbudte forsikring dækker disse behov.

Bliv klogere på egen virksomhed

Når ledelsen skal vurdere, hvordan man bedst muligt forsikrer sig i tilfælde af cyberhændelser, så handler det om at få styr på egen sikkerhed. De fleste forsikringsselskaber efterlyser dokumentation for virksomhedens nuværende sikkerhedsniveau, før der tegnes en forsikring. Det er derfor en fordel at kunne fremvise en sikkerhedspolitik, beredskabsplan og beskrivelse af, hvordan I arbejder med sikkerhed for at få de mest fordelagtige vilkår.

Typiske dækninger:

Omkostninger til ekstern assistance i forbindelse med håndtering af en hændelse

- Hjælp fra it-eksperter, advokat og andre rådgivere med henblik på at yde hjælp til at vurdere angrebet og skadens omfang.
- Hjælp fra it-eksperter til at begrænse skaden og håndtere hændelsen.
- Hjælp til håndtering af elektronisk afpresning samt rimelige omkostninger ifm. afpresning - fx løsesum.
- Hjælp til rekonstruktion af it-systemer, netværk, software og data.
- PR-omkostninger forbundet med at reducere skaden på omdømme.

Driftstab

- Hvis virksomhedens it-systemer bryder ned på grund af et cyberangreb, og virksomheden derfor ikke kan servicere kunder, opfylde forpligtelser, sælge varer og lignende. Kan være tidsafgrænset i eksempelvis op til tre måneder.

Tab og omkostninger som følge af mistede forretningshemmeligheder eller anden fortrolig information, samt erstatningsansvar overfor tredjeparter

- Økonomiske konsekvenser ved tab eller fejlbehandling af kunde- eller medarbejderdata - fx økonomiske tab som tredjepart kan have været udsat for i forbindelse med cyberangrebet på virksomheden.
- Erstatningsansvar og bøder for brud på immaterielle rettigheder, herunder GDPR.

Netbank

- Mulige økonomiske tab, virksomheden har fået som et resultat af indbrud i virksomhedens netbank.

Valg af forsikring afhænger af virksomhedens produkt og service

a. Er du en produktionsvirksomhed, er det muligvis et stop i produktionen og deraf driftstab, der har den største negative konsekvens for din forretning.
b. Behandler du mange personoplysninger (fx ved webhandel), så skal din forsikring formentlig også tilbyde assistance i forbindelse med at opfylde de gældende regler om varsling til Datatilsynet og berørte personer/kunder ved et databrud.
c. Afhænger din nuværende og fremtidige forretning af proprietær viden (fx unikke designs, opskrifter, nye teknologier, mv.), så skal du evt. overveje, om din forsikring dækker tab af fremtidig forretning som følge af en hændelse.

Sikkerhedsindsats er basis for forsikringer

Sikring og forsikring af virksomheden hænger tæt sammen. Derfor bør CFO og ledelse løbende:

- Skabe klarhed og overblik over sikkerhedsniveauet
- Træne medarbejdere i god sikkerhedspraksis
- Modtage sparring omkring det aktuelle trusselsbillede, og hvordan det påvirker virksomhedens risiko.

CFO og ledelse bør overveje følgende indsatsområder som supplement til forsikringen:

- Regelmæssig rådgivning med fokus på cybersikkerhed for eksempel ved årlige trussels- og risikoworkshops med ledelsen
- Ekstern og intern sårbarhedsscanning, der giver en løbende overvågning af eksterne forbindelser med henblik på at identificere svagheder
- Trusselsbulletin: Løbende opdatering og information om relevante cybertrusler mod forretningen
- Incident Response: Assistance til virksomheden ved sikkerhedshændelser
- Løbende træning af medarbejderne i cybersikkerhed og GDPR gennem e-learning
- Test af medarbejdernes kendskab til god praksis gennem phishingøvelser.

Ovenstående indsats kan være medvirkende til at nedbringe forsikringspræmien, og samarbejdet med eksterne specialister gør det samtidig lettere at agere hurtigt og effektivt ved en hændelse, fordi de på den måde allerede kender virksomhedens forretning, organisation, systemlandskab og infrastruktur.

Forslag:
Sådan kommer du videre

+ Få et overblik over virksomhedens kronjuveler, sikkerhedsniveau og risikoprofil.
+ Få et overblik over, om virksomheden har brug for at overføre noget risiko til en tredjepart via en cyberforsikring, og i givet fald, hvilken dækning, der er nødvendig.
+ Sæt dig grundigt ind i forsikringernes dækning, herunder krav og vilkår. Har virksomheden kontorer i udlandet, bør man sikre sig, at forsikringen gælder for disse også.
+ Sørg for, at sikkerhedsniveauet i jeres virksomhed matcher de krav og vilkår, der stilles i forsikringen. Få eventuelt en uvildig validering af sikkerhedsniveauet.

+

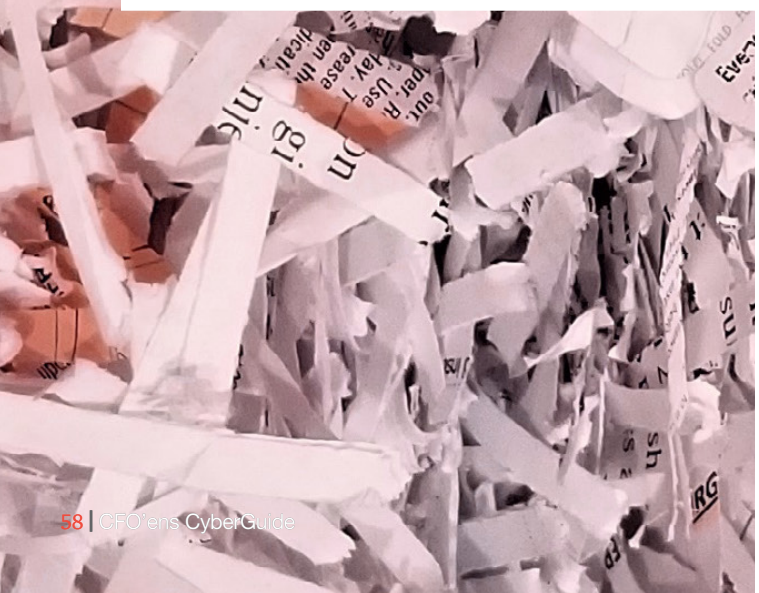
Opsummering:
Cyberforsikringer kræver styr på sikkerheden

+ Flere virksomheder vælger at tegne en cyberforsikring for at overføre noget af risikoen ved en cyberhændelse til en tredjepart.
+ Markedet udvikler sig p.t., hvilket betyder, at kravene til forsikringer strammes, og præmierne bliver dyrere. Særligt for dem, der ikke har styr på sikkerheden.
+ Den bedste forsikring opnås ved at have klarhed over sin egen virksomheds risikoprofil og ved at have det cyberstrategiske fundament på plads.

Cybersikkerhed og GDPR

– der er en sammenhæng

Formålet med dette afsnit er at give CFO'en et overblik over GDPR og de opgaver, der følger med for at efterleve reglerne. Vi ser på fordele, der er ved at leve op til GDPR-reglerne, og hvordan dette arbejde hænger sammen med cybersikkerhed. Vi viser en kort fasemodel for arbejdet – og afliver nogle af de myter, der eksisterer omkring GDPR. Afsnittet giver en overordnet gennemgang af de opgaver, som virksomheden skal løse, og hvordan CFO'en som øverste ansvarlig skal orkestrere arbejdet.



GDPR hører hjemme i 'Governance, risk og compliance' i PAVA-modellen, som beskrevet på side 15. Men GDPR er ikke alene en juridisk disciplin. GDPR har elementer i alle områderne i PAVA, og GDPR kræver derfor både en indsats på proces-, validerings-, arkitektur-, og adfærdsområdet. For at kunne efterleve GDPR skal man kunne dokumentere, hvordan kravene overholdes, og at disse er kommunikeret og implementeret i forretningen.

Governance, risk og compliance-området
GDPR er et af de primære elementer i 'Governance, risk og compliance-området'.

Beskyttelse af personoplysninger har længe været en grundlæggende rettighed, men i takt med den teknologiske udvikling og den stigende digitalisering, har EU med databeskyttelsesforordningen (GDPR) skærpet kravene til virksomheders sikkerhed og håndtering af personoplysninger.

Personoplysninger er derfor blot ét - men helt centralt - aktiv, som lovgiver har bestemt skal beskyttes. Arbejdet med cybersikkerhed har derfor mange fælles overlap med GDPR, og et fokus på at styrke cybersikkerhed vil samtidigt beskytte de personoplysninger, som er det centrale aktiv i GDPR.

Et helt centralt princip i GDPR er princippet om ansvarlighed. Det indebærer, at virksomheden er ansvarlig for, at reglerne efterleves, og at virksomhederne kan dokumentere, at reglerne reelt efterleves, ligesom det indebærer et krav om ledelsesforankring.

Alle virksomheder og organisationer, som behandler personoplysninger om EU-borgere, skal overholde GDPR ved at dokumentere, at personoplysninger håndteres sikkert og lovligt. Så det er derfor vigtigt, at procedurer og kontroller kan dokumenteres.

I dette afsnit besvarer vi følgende centrale spørgsmål:

- Hvad er formålet med GDPR?
- Hvad er ledelsens ansvar og rolle?
- Hvad er risiciene ved manglende overholdelse af GDPR?
- Hvad er fordelene ved at overholde GDPR?
- Hvad skal der til for at overholde GDPR, og hvordan styrer, måler og rapporterer ledelsen på GDPR?
- Hvordan rapporteres GDPR-arbejdet?


Databeskyttelsesforordningen (GDPR)
1. Grund-principperne (artikel 5)
2. Lovlig behandling af personoplysninger (artikel 6 + 7)
3. Persondata-beskyttelses-politikker/ retningslinjer og forretningsgange
4. Overførsel af personoplysninger uden for EU/EØS (artikel 44-50)
5. Fortegnelser over behandlings-aktiviteter (artikel 30)
6. Registreredes rettigheder (artikel 12-23)
7. Dataansvarlige og databehandlere (artikel 24-43)
8. Behandlings-sikkerhed og risiko-vurdering (artikel 32)
9. Konsekvens-analyse (DPIA) (artikel 35)
10. Håndtering af brud på person-datasikkerheden (artikel 33 + 34)
11. Databeskyttelses-rådgiver (DPO) (artikel 37-39)
Styring og ledelse, implementering, træning og awareness, drift, gennemgang, opfølgning og rapportering

Hvad er formålet med GDPR?

GDPR er en EU-lovgivning, der gælder alle virksomheder, og som fik virkning fra den 25. maj 2018, og har til formål at sikre:

- beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af deres personoplysninger
- ensartet niveau for beskyttelse af fysiske personers oplysninger i hele EU understøttet af effektiv håndhævelse af reglerne
- den frie udveksling af personoplysninger i EU og fremme digitalisering ved at skabe tillid i den digitale verden.

Hvad er ledelsens ansvar og rolle?

Virksomheden er som udgangspunkt dataansvarlig, og dermed ansvarlig for at overholde GDPR. CFO'en, direktionen og bestyrelsen har derfor ansvaret for, at virksomheden overholder GDPR.

Såfremt ledelsen ikke sikrer, at GDPR overholdes, vil det som udgangspunkt være virksomheden, der ifalder straf. Ledelsen eller en overordnet ansat, herunder direktøren, kan ifalde personligt ansvar, hvis der er handlet forsætligt eller udvist grov uagtsomhed, fx hvis ledelsen ikke har gjort noget for at overholde GDPR.

Hvad er risiciene ved manglende overholdelse af GDPR?

- **Bøder og sanktioner**
  Det er bl.a. de meget høje bøder, som har givet GDPR den store opmærksomhed. Datatilsynet kan indstille til bøder på op til 150. mio. kr. eller op til 4 % af virksomhedens samlede globale omsætning.

Mens mange europæiske tilsynsmyndigheder har pålagt flercifrede million- og milliardbøder, så har Datatilsynets bødeindstillinger hidtil været i den lave ende. Det kan dog forventes, at bødeniveauet vil stige for at leve op til kravet om EU-harmonisering og samtidigt være effektivt og have en vis afskrækkende virkning.

Datatilsynet har udstedt en vejledning til, hvordan de danske bøder skal fastsættes.

Læs om Datatilsynets vejledning her

Datatilsynet kan også udstede påbud eller forbud mod at fx ophøre brugen af et system eller ophør af en arbejdsproces, hvilket vil medføre omkostninger for virksomheden.

- **Omdømme og tab af image**
  Datatilsynet kan udtale alvorlig kritik på baggrund af en klage eller henvendelser fra fx en utilfreds kunde, tidligere medarbejder eller sågar en konkurrent. Dette kan være skadeligt for en virksomheds omdømme og dermed også omsætning. En undersøgelse viser, at de økonomiske konsekvenser ved offentlig kritik eller offentliggørelse af bøde oftest overstiger omkostningerne ved selve bøden.

Virksomheder bør dog ikke kun overholde GDPR, fordi det er lovpligtigt og på grund af de nævnte risici. Der er mange fordele forbundet med at overholde GDPR, som virksomhederne bør kende.

Hvad er fordelene ved at overholde GDPR?

Når GDPR af nogle opfattes som et benspænd for den daglige drift, forretningsudvikling og ny teknologi, skyldes det både myter og fejlfortolkninger, og at GDPR fortsat er en ny og kompleks regulering.

+

Myte 1: **"Vi behandler ikke *personfølsomme* oplysninger, så vi behøver ikke at bekymre os om GDPR"**

Falsk

Begrebet personfølsomme oplysninger er forkert og findes ikke i lovgivningen. I GDPR opererer man med begrebet personoplysninger, som dækker over enhver form for information, der kan henføres til en bestemt person. Personoplysninger opdeles i almindelige, fortrolige (cpr-nummer og strafbare forhold) og følsomme personoplysninger.

GDPR gælder derfor også, hvis du kun behandler de almindelige personoplysninger. Jo mere sensitive personoplysninger, jo højere krav stiller GDPR til sikkerheden, og jo mere skal der til, før man har lov til at behandle og bruge oplysningerne.

+

Myte 2: **"Vi er en B2B-virksomhed, som kun har virksomheder som kunder, og derfor gælder GDPR-reglerne ikke for os"**

Falsk

GDPR gælder for alle virksomheder. B2B-virksomheder behandler fx personoplysninger om deres egne medarbejdere, kontaktpersoner hos samarbejdspartnere og leverandører mv.

Behandling af oplysninger om enkeltmandsvirksomheder er også omfattet af GDPR-reglerne, idet det i praksis ikke er muligt at skelne mellem oplysninger om ejeren som individ og oplysninger om virksomheden.

Formålet med GDPR er ikke at forhindre virksomheder i at drive virksomhed. Formålet er, at vi skal drive ansvarlig virksomhed i et datadrevet samfund.

I vores samfund er der et øget behov for at udnytte de digitale muligheder til at automatisere forretningens kerneprocesser og anvende ny teknologi til at udnytte data til brugbare indsigter, der kan handles på. Brugen af cloud er i høj grad blevet standard i alle virksomheder, uanset størrelse. Den digitale udvikling gør forretning, teknologi og datasikkerhed uadskillelige.

Ved at kende fordelene, kan GDPR gå fra at udgøre en risiko til at være en aktiv konkurrenceparameter. Som CFO bør du overveje, hvordan data generelt kan anvendes strategisk.

Vejen til overholdelse af GDPR

GDPR fik virkning den 25. maj 2018, og siden da har de fleste virksomheder ydet en indsats for at overholde lovgivningen. Ikke desto mindre, har mange virksomheder anset GDPR som et projekt med et slutmål, hvor der primært har været fokus på det juridiske papirskjold.

Men GDPR er ikke et forløb, hvor virksomheden kan anses for at overholde lovgivningen efter projektets afslutning. Det er vigtigt, at kravene indarbejdes i forretningen og efterleves i den daglige drift.

For at opnå en succesfuld, effektiv og holdbar implementering af GDPR, skal virksomheden typisk gennem fem faser.

Fordele ved GDPR

Skab tillid og troværdighed
At overholde GDPR kan anvendes som en konkurrenceparameter, fx for at komme i betragtning til at blive leverandør, eller ved at styrke virksomhedens troværdighed og omdømme til kunder, medarbejdere og samarbejdspartnere.

Forenkling af forretning og arbejdsprocesser
GDPR forudsætter, at det identificeres i hvilke it-systemer, personoplysninger behandles, og til hvilke formål og hvordan. Man skal have overblik med egne arbejdsprocesser, såvel som de leverandører, der anvendes. Brug arbejdet til at forenkle processer og få "ryddet op".

Løftestang til andre projekter som fx Data Analytics
Det kan skabe høj værdi, hvis data udnyttes til datadrevne beslutninger. GDPR kan være en løftestang til at sætte andre digitaliseringstiltag i gang, herunder initiativer inden for AI, Big Data og Data Analytics. Der er mange overlap mellem GDPR og Data Analytics, som begge kræver, at man har et overblik over data, at data er korrekte, ajourførte og lovlige at bruge.

Medvirker til bedre ledelse og styring
GDPR kræver nedskrevne forretningsgange, som fortæller, hvordan kravene skal håndteres. Det resulterer ofte i en større klarhed over ansvar og roller og forbedrede beslutningsprocesser, som også kan anvendes i forbindelse med andre opgaver og projekter.

Bedre prissætning ved virksomhedssalg og nemmere finansiering
Virksomheder, som skal igennem en due diligence i forbindelse med et frasalg, vil stå stærkere, hvis de kan påvise overholdelse af gældende lovgivning og en højere organisatorisk modenhed.

Bedre forberedelse til EU's stigende regulering af data
EU anser data som måske den væsentligste ressource for EU's fremtidige vækst, som ikke bare skal beskyttes, men også anvendes gennem brugen af nye teknologier som fx Cloud, IoT, blockchain og AI. Data vil blive mere og mere reguleret, og GDPR er derfor blot en grundlæggende forudsætning for brugen af data.

Inden I går i gang med faserne, vil det være en god idé at få lavet en analyse af, hvordan virksomheden står lige nu i forhold til GDPR, fx en GDPR compliance assessment. En sådan analyse kan med fordel foretages af en ekstern og uvildig rådgiver og vil ende ud med nogle anbefalinger til det fremadrettede arbejde.

Se PwC's side om GDPR

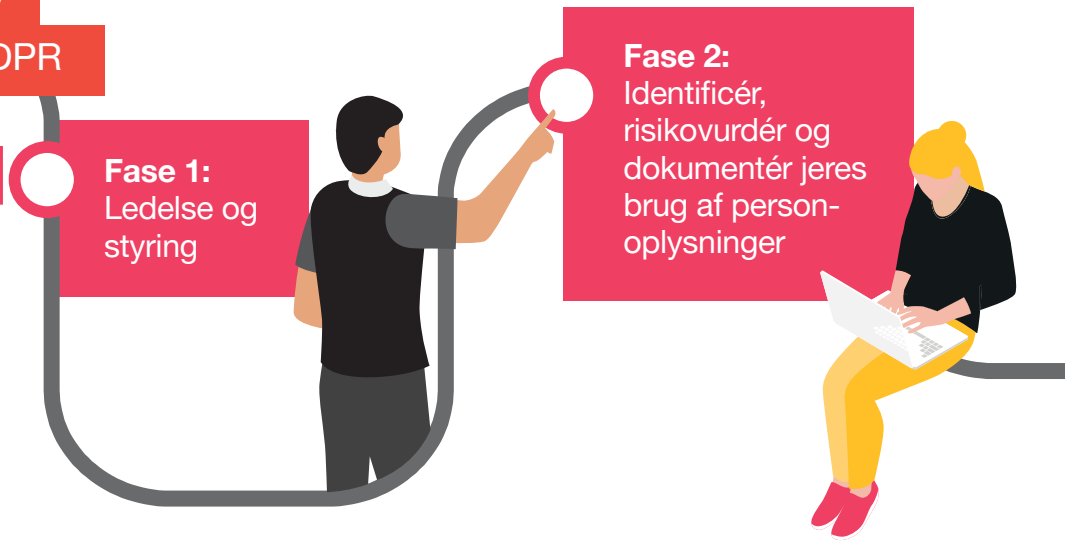
+

Myte 3: **"Det fremgår af GDPR, hvornår vi skal slette personoplysninger"**

Falsk

GDPR indeholder ingen facitliste for, hvornår personoplysninger skal slettes. Slettefrister afhænger af en konkret vurdering. Personoplysninger skal slettes, når der ikke længere er et legitimt formål ved at beholde dem. Der kan fx være anden lovgivning, som forpligter dig til at beholde oplysningerne (fx bogføringslovens 5 år). I så fald er det vigtigt, at man sletter de andre oplysninger, som ikke er relateret til selve bogføringen.

De 5 faser for effektiv implementering af GDPR



Fase 1: Ledelse og styring

CFO'en spiller en helt central rolle i den indledende fase og skal:

- Sikre forankring i ledelsen ved at udpege en GDPR-ansvarlig og sikre opbakning i ledelsen.
- Beskrive ambitionerne med GDPR-arbejdet. Vil I blot overholde kravene og undgå bøder, eller er ambitionerne højere? Vil I eksempelvis løfte virksomheden til et niveau, hvor persondatabeskyttelse bliver en konkurrenceparameter og kan styrke tilliden i relation til kunder, leverandører og det omgivende samfund?
- Etablere en organisation, som er bredt sammensat. GDPR er ikke kun et it- eller juraprojekt. Hele forretningen skal involveres, fx salg, marketing og HR.
- Sikre styring, ansvar og roller. Ansvar og roller skal være fastlagt, og det interne og eksterne ressourcetræk estimeres Der vil typisk være forskel på ansvaret i en projektfase og i den efterfølgende drift.
- Rapportere. CFO'en skal sikre sig, at fremdrift såvel som væsentlige risici bliver rapporteret.

Fase 2: Identificér, risikovurdér og dokumentér jeres brug af personoplysninger

I fase 2 skal der bl.a. skabes et overblik over, hvor der behandles personoplysninger, hvem der har adgang til dem, og hvad de anvendes til. Der skal foreligge skriftlig dokumentation.

På baggrund af kortlægningen skal det juridiske papirskjold (GDPR-dokumentationen) udarbejdes, som bl.a. omfatter en risikovurdering. Det er vigtigt at bemærke, at denne GDPR-risikovurdering adskiller sig fra de typiske it-risikovurderinger (som er beskrevet tidligere i guiden).

Omdrejningspunktet for den lovpligtige GDPR-risikovurdering er de personer, som man behandler personoplysninger om, fx medarbejdere og kunder. Man skal fx vurdere risikoen for, at personoplysninger bliver delt med uvedkommende, og hvad konsekvensen kan være for den registrerede, og hvordan man kan nedbringe denne risiko. En utiltænkt deling kan fx medføre identitetstyveri, men også fx tab af ære og velfærd. Datatilsynet har udgivet en vejledning til risikovurdering, og man kan bede sin eksterne rådgiver om hjælp til denne opgave.

Der skal udarbejdes forretningsgange for, hvordan virksomheden og medarbejderne håndterer GDPR-kravene i den daglige drift. Det er afgørende, at risici bliver rapporteret til CFO'en (eller projektsponsoren). En høj GDPR-risiko for de registrerede (fx kunder og medarbejdere) kan indebære en høj risiko for virksomheden.

Fase 3: Informations-sikkerhed

Fase 4: Understøttende GDPR-teknologier

Fase 5: Kommunikation, awareness og træning

Fase 3: Informationssikkerhed

Cyber- og informationssikkerhed spiller en central rolle i GDPR. Virksomheden skal sikre, at der implementeres passende sikkerhedsforanstaltninger eller kontroller i it-systemer og arbejdsprocesser for at beskytte personoplysningerne og forhindre, at oplysninger fx ved et uheld eller bevidst kompromitteres.

Sikkerhedstiltag er fx:

- Adgangsstyring
- Netværkssikkerhed
- Beskyttelse mod malware
- Overvågning
- Logning
- Backup
- Beredskab
- Leverandørstyring.

Hvis man har en cyberrisiko, har man som regel også en GDPR-risiko.

GDPR har et omdrejningspunkt for tilgangen til persondatabeskyttelse, der i bred forstand er risikobaseret. Jo højere risikoen er, desto strengere sikkerhedsforanstaltninger skal der implementeres for at mindske risikoen. Passende sikkerhedsforanstaltninger skal vælges ud fra den risikovurdering, som ligger i fase 2 .

Fase 4: Understøttende GDPR-teknologier

I denne fase skal ledelsen afklare, hvorvidt virksomheden har den rette teknologi til bl.a. at understøtte GDPR og dermed beskytte personoplysninger.

Teknologien til at understøtte personoplysninger vil i mange tilfælde være de samme teknologier, som benyttes til at beskytte andet data og andre aktiver i virksomheden.
Eksempler på sikkerhedsteknologier kan være logning og kryptering, men der kan også implementeres teknologier til automatisering af fx sletning. PwC har udviklet en GDPR-scanner, som både kan give overblik over data, og understøtte en automatiseret sletning.

GDPR-scanner

For uddybende information om teknologivalg henvises der til side 22.

Fase 5: Kommunikation, awareness og træning

Vi har set mange eksempler på, at GDPR bliver implementeret ved, at det juridiske papirskjold blot bliver publiceret på virksomhedens intranet, og at medarbejderne derefter forventes at efterleve nye eller skærpede regler og arbejdsgange. Ligesom andre væsentlige forandringer, så kræves det, at GDPR-kravene og forretningsgangene bliver kommunikeret på kontinuerlig basis, og at medarbejderne bliver trænet og understøttet med rådgivning og værktøjer til at løfte opgaven. Herudover er det et krav i GDPR, at medarbejdere trænes og uddannes i databeskyttelsesreglerne, og at det skal kunne dokumenteres. PwC har udviklet en række e-learnings om GDPR og cybersikkerhed, som på en effektiv og lettilgængelig måde kan træne medarbejderne, samtidigt med at det dokumenteres.

E-learnings fra PwC

Ledelsen bør være særlig opmærksom på at gøre det klart for organisationen, hvorfor det er nødvendigt, hvordan det kommer til at foregå, og hvilken rolle den enkelte har i at beskytte data.
For uddybende information om adfærd og awareness henvises der til side 32.

+

Myte 4: **"Vi indgår databehandleraftaler, så vi efterlever reglerne"**

Falsk

Man efterlever ikke alle GDPR-reglerne ved at indgå databehandleraftaler, hvor det ikke er påkrævet – tværtimod. Først og fremmest skal man vurdere sin og den anden parts rolle. Det er vigtigt at afgøre, om man er dataansvarlig eller databehandler, da kravene er forskellige.

Som udgangspunkt er det den dataansvarlige, som har ansvaret for, at virksomheden lever op til reglerne i GDPR, hvorimod databehandleren alene skal sikre sig, at denne følger databehandleraftalen mellem databehandleren og den dataansvarlige.

Det kan i øvrigt være dyrt og ressourcekrævende at indgå databehandleraftaler, hvis det ikke er påkrævet. Det kan du læse mere om i den store (og dyre) myte om databehandleraftaler.

Den store (og dyre) myte om databehandleraftaler

Hvordan rapporteres GDPR-arbejdet?

GDPR kan have stor indvirkning på virksomhedens økonomi og forretningsgrundlag. Som ansvarlig for virksomhedens finansielle sikkerhed og risikostyring, er det derfor naturligt, at CFO'en måler og rapporterer på virksomhedens GDPR-arbejde.

Omfanget og metoden af rapporteringen afhænger af, hvor langt virksomheden er med GDPR-arbejdet, hvilke målgrupper der skal rapporteres til og virksomhedens eksisterende rapporteringsmetode. Som udgangspunkt kan en virksomhed rapportere GDPR med følgende indhold:

- **Projektrapportering**
  Hvis virksomheden fortsat er i projektfasen, bør der rapporteres på projektaktiviteter og fremdrift i projektet. Evt. ligeledes på ressourceforbrug.

- **Rapportering på implementering og modenhed**
  Ved at validere og rapportere status på GDPR-arbejdet i et kultur-, proces- og teknologiperspektiv, sikres det, at der ikke alene måles og rapporteres på, om det juridiske papirskjold er på plads eller ej, men også om GDPR reelt er implementeret og efterleves. Til brug herfor, kan CFO'en anvende PAVA-konceptet, der beskrives på side 14.

- **Risici og persondatabrud**
  Ledelsen bør modtage regelmæssig rapportering om høje risici, der afdækkes som led i risikovurderingen (se fase 2), såvel som fx eventuelle persondatabrud, der forekommer i den daglige drift.

- **Opfølgning på efterlevelse af GDPR**
  Der bør årligt følges op på efterlevelse af GDPR, herunder de konkrete krav og kontroller, fx i henhold til standarden ISO 27701. Brug evt. resultatet af din GDPR compliance assessment som rapportering. Som dataansvarlig har man endvidere pligt til at føre tilsyn med sine databehandlere. I den forbindelse kan man i databehandleraftalen forpligte sin leverandør til at levere fx en ISAE 3000-erklæring vedrørende behandling af personoplysninger.

- **DPO-rapportering**
  Såfremt virksomheden har pligt til at udpege en DPO, eller har udpeget en DPO frivilligt, skal DPO'en rapportere direkte til øverste ledelsesniveau om overholdelse af GDPR.

+

Myte 5: **"Vi skal slette alt, hvis fx en kunde eller medarbejder beder om det"**

Falsk

En af de registreredes rettigheder, er retten til at få slettet sine personoplysninger af dem, der behandler dem. Denne ret er dog ikke ultimativ. Man kan fx ikke bede om at få slettet alle oplysninger, hvis man stadig har et aktivt kundeforhold, eller virksomheden har pligt til at opbevare oplysninger grundet anden lovgivning. Virksomheden skal foretage en konkret vurdering af, om den kan slette oplysningerne ved hver enkelt henvendelse, og den skal slette oplysningerne, hvis der ikke længere er et nødvendigt formål med opbevaring.

GDPR-tjekliste til CFO'en

Når du som CFO skal have en indikation af, hvor langt virksomheden er med at overholde GDPR, kan følgende spørgsmål give dig et billede. Spørgsmålene kan du måske selv svare på – eller du kan stille dem i et relevant forum hos jer:

☐ **Ansvar og roller**

- Er ansvaret for GDPR placeret hos en af jer i ledelsesgruppen?
- Drøfter I GDPR på ledelsesmøder?
- Hvem er de udførende på de enkelte GDPR-opgaver?
- Gennemfører I intern awareness?

☐ **Overblik over data og it-systemer**

- Har I overblik over, hvor i virksomheden og i hvilke it-systemer I behandler personoplysninger?
- Har I overblik over dataflowet imellem it-systemerne?
- Hvilke data opbevares lokalt hos medarbejderne, fx på deres pc eller mail?
- Har I lavet GDPR-risikovurderinger i virksomheden?
- Bruger I eksterne leverandører til behandling af personoplysninger?

☐ **Overblik over, hvor langt I er med GDPR**

- Hvor langt er vi overordnet set med efterlevelse af GDPR?
- Hvor er de største udfordringer i GDPR?
- Har I fået lavet en gennemgang af jeres efterlevelse af en ekstern part?
- Rapporteres efterlevelse af GDPR til bestyrelsen eller andre ledelseskolleger?
- Hvor mange brud på persondatasikkerheden har I anmeldt til Datatilsynet i det seneste år?

☐ **Sletning af data**

- Er der fastsat interne regler for, hvor længe data opbevares – og hvor?
- Har I fastlagt regler for, hvornår der bliver slettet data i it-systemerne, og hvem der har opgaven?
- Udføres sletningen manuelt, eller er sletningen it-understøttet?

Sådan forbereder du organisationen til NIS2 og direktivets skærpede krav til cybersikkerhed

Med NIS2 kommer der nye og mere skærpede krav til nye sektorer og et øget antal virksomheder og organisationer. I dette kapitel giver vi dig et overblik over de væsentligste elementer i det nye direktiv, hvordan du finder ud af, om jeres organisation er underlagt direktivet, og hvordan I sikrer, at I efterlever kravene.

Den stadig stigende digitalisering af samfundets kritiske infrastruktur bærer en lang række fordele med sig, men samtidig øger det behovet for at styrke cybersikkerheden i virksomheder og organisationer. I erkendelse heraf skærper EU nu kravene til cybersikkerhed i en række virksomheder og offentlige myndigheder. Det opdaterede Net- og Informationssikkerhedsdirektiv - NIS2 - fra EU udvider definitionen af samfundskritiske sektorer og stiller betydeligt skærpede krav til cybersikkerheden i virksomheder og offentlige myndigheder, der er tilknyttet disse sektorer.

Baggrunden for NIS2

Flere virksomheder og organisationer yder væsentlige, samfundskritiske tjenester og services, som i udgangspunktet altid skal holdes i drift. Disse tjenester er understøttet af digital infrastruktur, hvilket gør det mere tydeligt, at der gælder en særlig forpligtelse for de virksomheder og organisationer, som agerer operatør af samfundskritiske sektorer, ikke mindst i forhold til cybersikkerhed. Net- og Sikkerhedsinformationsdirektivet (NIS) blev indført i 2016, hvor EU-Kommissionen for første gang indførte krav til cybersikkerhed i organisationer, med det formål at øge sikkerheden i - og beskyttelse af - samfundskritiske sektorer.

NIS1-direktivet – det første af sin slags

For at forstå og håndtere kravene i NIS2 er det en god idé også at kende det oprindelige NIS1-direktiv. Med NIS1 stillede EU-Kommissionen for første gang krav til medlemsstaternes cybersikkerhed. Helt grundlæggende vurderede EU-Kommissionen nødvendigheden i at gøre en særlig indsats for at beskytte samfundets kritiske infrastruktur bedst muligt mod cyberhændelser. NIS1-direktivet udpegede derfor en række operatører, der skal beskyttes. Det gælder i sektorerne: energi, transport, banker, finansielle markedsinfrastrukturer, sundhed, drikkevandsforsyning og

Scope for NIS1

NIS1

- Sundhedsvæsen
- Transport
- Den finansielle sektor
- Digital infrastruktur
- Vandforsyning
- Energi
- Digitale serviceudbydere

Scope for NIS2

NIS2 - Essentiel

- **Energi** – forsyning, distribution, transmission og salg af energi
- **Transport** – via luft, jernbane, vej og sø
- **Finans** - kredit, handel, marked og infrastruktur
- **Sundhed** – forskning, produktion, udbydere og fremstillere af udstyr
- **Drikke- og spildevand**
- **Digital infrastruktur** – DNS, tillidstjenester, datacenter-tjenester, cloud computing, kommunikationstjenester (tele- og net), udbydere af managed services og managed security services
- **Offentlig administration**, kommuner og regioner
- **Rumfart** – software og services

NIS2 - Vigtig

- **Post- og pakkeservice**
- **Affaldshåndtering**
- **Kemiske produkter** – fremstilling og distribution
- **Fødevarer** – fremstilling, distribution og produktion
- **Fremstilling/produktion** – pharma, elektronik, optisk udstyr, maskineri, køretøjer
- **Udbydere af online markedspladser** – søgemaskiner, sociale platforme

-distribution, samt digital infrastruktur (cloud computing-tjenester, online markedspladser samt søgemaskiner).

Disse sektorer blev pålagt - som operatør af den kritiske infrastruktur - at vedtage og gennemføre konkrete foranstaltninger til styring af sektorernes cybersikkerhedsrisici. Derudover skal de også indberette alvorlige hændelser til de nationale tilsynsmyndigheder.

NIS2-direktivet skal udmøntes i bekendtgørelser senest i 2024

Det har dog vist sig, at NIS1-direktivet ikke har skabt tilstrækkeligt sikkerhedsniveau mod de cybertrusler, som EU-medlemsstaterne står overfor. Siden direktivet blev implementeret i 2018, er både digitaliseringen og cybertruslen øget, og medlemsstaterne står over for flere fælles grænseoverskridende udfordringer. Derfor har EU-Kommissionen opdateret NIS-direktivet med henblik på at sikre et højt fælles cybersikkerhedsniveau på tværs af EU. Det opdaterede direktiv – NIS2 – blev foreløbigt vedtaget i maj 2022 og skal udmøntes i bekendtgørelser senest medio 2024.

NIS2 har til formål at styrke cybersikkerheden yderligere ved at forpligte flere sektorer til at udarbejde strengere sikkerhedsforanstaltninger og øge cybersikkerhedsniveauet yderligere. På side 62 er en oversigt, som konkretiserer præcist, hvilke nye sektorer der er omfattet af NIS2.

Flere virksomheder og flere krav

Der er en række væsentlige forskelle mellem NIS1 og NIS2, som virksomhedsledere skal være opmærksomme på. Først og fremmest omfatter direktivet nu flere sektorer og skelner mellem vigtige og essentielle enheder i de forskellige sektorer. Nu er det heller ikke længere myndighederne, der udpeger de udbydere, der er underlagt direktivet. Nu gælder direktivet alle udbydere i de udpegede sektorer, bortset fra mikrovirksomheder. Hvor NIS1-direktivet omfattede bl.a. operatører af væsentlige tjenester, herunder energi, transport, finans, sundhed og drikkevand, omfatter NIS2 sektorer og aktører, der har vital betydning for både samfundsmæssige og økonomiske aktiviteter i det indre marked. Forsyningslinjer til de essentielle sektorer såsom energisektoren er omfattet samt fødevaresektoren, spildevandssektoren, affaldssektoren, rumteknologisektoren, datacenterleverandører og leverandører af sociale netværksplatforme.

Øget tilsyn fra myndighederne

Hvor der i det oprindelige direktiv til en vis grad var lagt op til en indberetningsordning, så strammer EU op på dette område. Virksomheder og ledelse kan forvente en aktiv myndighedsrolle, der indebærer løbende tilsyn. Derudover vil virksomhederne nu opleve, at der bliver stillet krav til at indberette alvorlige hændelser i løbet af 24 timer efter, at hændelsen er sket.

Øget ledelses- og bestyrelsesansvar

Ledelsen hos de virksomheder, der er omfattet af NIS2, skal godkende og sikre implementering af foranstaltninger, der ligger i NIS2. Ledelsen kan blive stillet direkte til ansvar for brud på NIS2.

Væsentlige bøder for overtrædelse

Der er lagt op til mulighed for at give store bøder til virksomheder, som ikke overholder NIS2. Direktivet skelner mellem vigtige og essentielle virksomheder og myndigheder. Vigtige organisationer kan risikere at skulle betale op til to mio. euro eller én procent af den globale omsætning, og essentielle organisationer kan potentielt få bøder på op til fire mio. euro eller to procent af den globale omsætning. Kategoriseringen i direktivet sker ud fra type og størrelse.

Fokusområder i NIS2

Herunder er nogle af de afgørende spørgsmål, der skal afklares for at sikre compliance:

- Har vi opbygget et ledelsessystem for cybersikkerhed, hvor roller og ansvar, målsætninger og governancestruktur fremgår tydeligt?
- Hvad er vores politikker og procedurer for vurdering af effektiviteten af virksomhedens sikkerhedstiltag? Hvordan tester og reviderer vi?
- Har vi politikker for risikoanalyse og relevante mitigerende sikkerhedspolitikker og -foranstaltninger for vores informationssystemer?
- Er vi i stand til at identificere risici i informationssystemer forbundet med den nuværende cybertrussel?
- Udøver vores organisation trænings- og awareness-aktiviteter, så medarbejdere i organisationen er bekendte med disse politikker og deres roller og ansvar i forbindelse med cybersikkerhed?
- Screener vi vores medarbejdere i ansættelsesprocessen, og har vi disciplinære sanktioner over for medarbejdere, der ikke overholder reglementet?
- Sørger vi for at tildele de rette adgange og rettigheder til nye medarbejdere? Og reviderer vi og lukker for adgange, der ikke længere er behov for?
- Har vi politikker for håndtering af cyberhændelser: forebyggelse, identifikation, reaktion og rapportering til relevante myndigheder?
- Er vi i stand til at opdage sårbarheder i tide og reagere på dem? Har vi politikker og processer for sårbarhedsstyring? Patcher vi rettidigt?
- Har vi politikker for virksomhedens driftskontinuitet og krisestyring?
- Hvad gør vi for at sikre driften ved en krise?
- Hvad er vores krav omkring sikkerhed i forbindelse med anskaffelse, udvikling og vedligeholdelse af netværk og informationssystemer?
- Hvordan sikrer vi, at vi kan stole på vores data? Bruger vi kryptering?
- Hvordan håndterer vi forsyningssikkerhed? Det gælder bl.a. sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem den enkelte enhed og dens leverandører eller tjenesteydere såsom leverandører af datalagrings- og databehandlingstjenester eller forvaltede sikkerhedstjenester.
- Hvordan sikrer vi, at indkøbte produkter ikke indeholder sårbarheder?

Gælder NIS2 vores virksomhed?

Som leder skal du være opmærksom på, om jeres virksomhed er en del af de nye sektorer, der ikke har været omfattet af NIS1, men som er en del af NIS2. I er selv forpligtet til at afgøre, om I er omfattet. Det næste er naturligvis, om du som leverandør eller samarbejdspartner til virksomheder i de nævnte sektorer vil blive påvirket.

Vær opmærksom på, at NIS2 sætter nogle minimumsgrænser, der betyder, at det kun er virksomheder med flere end 50 ansatte og en årlig omsætning på mere end 10 mio. euro eller en årlig balance på over 43 mio. euro, der skal efterleve kravene.

Er vi klar til NIS2?

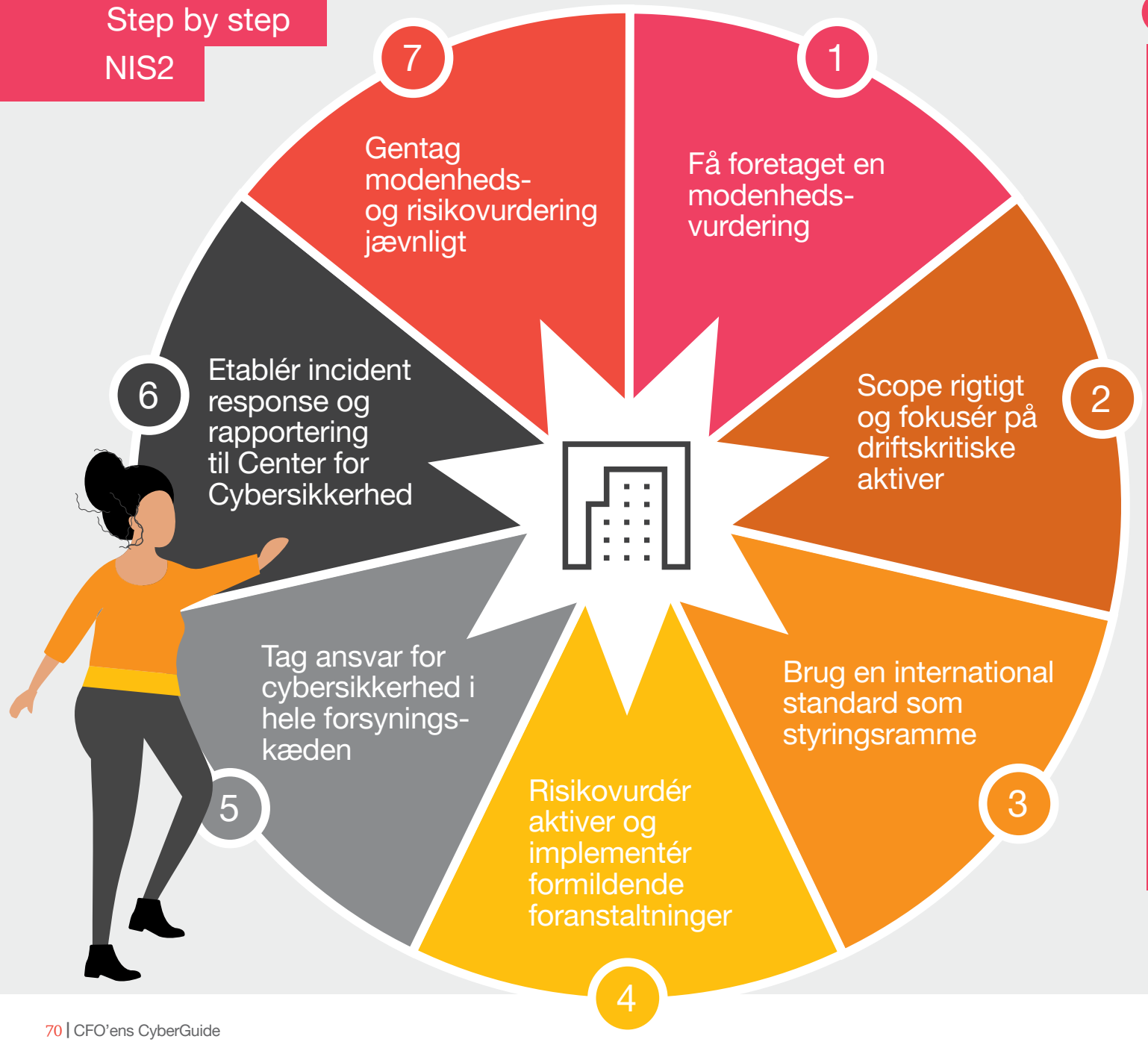
Med de nye regler stilles der skærpede krav til topledelsen, som nu vil kunne drages til ansvar for sikkerhedsforanstaltninger og til tilsynet med virksomhedens cybersikkerhed. Det kræves, at sikkerhedsniveauet matcher de aktuelle risikovurderinger. Det er med andre ord topledelsens ansvar, at virksomheden lever op til NIS2.

Det første skridt på vejen er at gennemføre en modenhedsvurdering for at afdække: Hvor står vi henne som virksomhed, hvad mangler vi for at være klar til NIS2, og hvad kræver det at nå dertil?

For at få det bedste resultat af indsatsen skal CFO'en overveje muligheden for at lave en samlet indsats, der omfatter GDPR, cybersikkerhed, NIS2 osv., og løse alle disse i et samlet cyberprogram.

> “ Som ledelse er man forpligtet til selv at undersøge, om virksomheden er underlagt kravene i NIS2-direktivet

Step by step NIS2



1 Få foretaget en modenhedsvurdering

Første skridt er at få foretaget en modenhedsvurdering af, hvor I står i dag i forhold til de krav, der stilles til jeres organisation i forhold til at efterleve NIS2-kravene. Med udgangspunkt i artikel 18 i NIS2 er det ledelsens ansvar at sikre, at virksomheden lever op til NIS2.

+ Ledelsen skal være bekendt med kravene i direktivet og risikostyringsindsatsen. Den får et direkte ansvar for, at cyberrisici bliver identificeret og håndteret, samt at kravene overholdes.
+ Øgede krav til risikostyring og robusthed betyder, at din organisation skal risikostyre og implementere både skadesforebyggende og -begrænsende foranstaltninger, der reducerer risici og konsekvenser. Minimumskrav er fx incident management, sikring af cybersikkerhed i forsyningskæder, netværkssikkerhed, adgangskontrol og kryptering.
+ Jeres organisation skal forholde sig til, hvordan I vil sikre forretningskontinuiteten i tilfælde af, at I skulle blive ramt af en større cyberhændelse. Dette indebærer eksempelvis at genoprette systemer, nødprocedurer og at etablere en kriseorganisation.
+ Jeres organisation skal have etableret processer for, hvordan I vil sikre den korrekte rapportering til myndighederne. Der stilles blandt andet krav til, at større hændelser rapporteres inden for 24 timer.

Modenhedsvurderingen giver et overblik over, hvilke konkrete områder I enten skal starte med eller arbejde videre med for at implementere kravene effektivt. Vurderingen bruges også til at få indblik i, hvilke investeringer og kompetencebehov, virksomheden har brug for, for at lykkes med implementeringen.

2 Scope rigtigt og fokusér på driftskritiske aktiver

I relation til NIS2 er det væsentligt at afgrænse jeres indsats til de driftskritiske aktiver. For at sætte scopet for arbejdet, skal I foretage en business impact analyse (BIA). Dette gør I ved først og fremmest at identificere, hvilke forretningsprocesser, der understøtter den samfundskritiske drift. Når I har identificeret de driftskritiske forretningsprocesser, skal I kortlægge alle de aktiver, der er relevante for disse processer. Det kan fx være mennesker, systemer og leverandører. Afslutningsvis skal I konsekvensvurdere aktiverne, der i så fald udgør jeres NIS2-scope.

3 Brug en international standard som styringsramme

NIS2-direktivet stiller krav til, at de omfattede organisationer implementerer et ledelsessystem for informationssikkerhed (ISMS). Internationale standarder som fx ISO 27001. ISO 27001 udgør samtidig et "best practice"-rammeværktøj for en holistisk og ledelsesforankret styring af informationssikkerhed. For at implementere et effektivt ISMS skal jeres organisation opbygge operationelle politikker, procedurer og processer for at styre informationssikkerheden. Eksempelvis skal I beslutte jer for roller og ansvar, risikoproces, målsætninger mv.

4 Risikovurdér jeres aktiver og implementér formildende foranstaltninger

NIS2-direktivet stiller krav til en risikobaseret tilgang til informationssikkerhed. I praksis betyder det, at jeres organisation skal beskrive en risikoproces, som I skal efterleve. I efterlever processen ved at risikovurdere samtlige af de aktiver, som I har identificeret som værende kritiske for jeres samfundskritiske funktion. Det vil altså sige, at I også skal risikovurdere jeres forsyningskæde og leverandører. Som en del af jeres risikohåndtering skal I implementere skadesforebyggende foranstaltninger, der formindsker jeres risici.

5 Tag ansvar for cybersikkerhed i forsyningskæden

Mange virksomheder har outsourcet væsentlige dele af deres it/ot-systemer eller indkøber produkter, der er væsentlige for virksomhedens drift, og har derved etableret forsyningskæder. NIS2-direktivet stiller krav til, at organisationer udøver risikostyring og stiller sikkerhedskrav til væsentlige leverandører i den direkte forsyningskæde til organisationen. Hvorvidt leverandører er væsentlige for organisationer i NIS-scopet afgøres af, om leverandøren har en direkte indflydelse på driften af den samfundskritiske tjeneste.

+ I energiforsyningen vil producenten af vindenergi fx være direkte afhængig af, at der bliver leveret dele til vindmøllerne, hvorfor energiproducenten skal risikostyre leverandøren af vindmøller.
+ I togtransporten vil operatøren af togdriften være direkte afhængig af, at skinner og signalprogrammer er tilgængelige og fungerer, hvorfor operatøren skal risikostyre leverandøren af disse ydelser.
+ I fødevareproduktionen vil producenten af fødevarer være afhængig af, at faciliteter, materialer og kemikalier bliver leveret. Ligeledes vil producenten være direkte afhængig af, at produktet kan transporteres til engros- eller detailhandlere, hvormed producenten skal risikostyre og stille cybersikkerhedskrav til leverandørerne.

Man kan outsource sine it/ot-systemer, men man kan ikke outsource ansvaret. Dette er tydeliggjort med NIS2-kravet om forsyningskædesikkerhed. Kravet omfatter sikkerhedsrelaterede aspekter i forbindelserne mellem den enkelte virksomhed og dens leverandører af fx sikkerhedstjenester eller datalagrings- og databehandlingstjenester.

Behovet for leverandørstyring er åbenbart, herunder at der etableres en robust risikostyring og løbende opfølgning på leverandørerne i forsyningskæden - fx i form af online monitorering, spørgeskemaer, egne audits og uafhængige revisionserklæringer.

Det er vigtigt, at der opnås konsensus om, hvor omfattende styringen skal være, også fordi mange virksomheder befinder sig midt i forsyningskæden og bliver mødt af krav fra kunder og samtidig skal stille krav til leverandører.

6 Etablér rapportering til Center for Cybersikkerhed

NIS2 stiller krav til, at organisationer skal rapportere hændelser til Center for Cybersikkerhed inden for 24 timer. Derudover skal organisationen løbende opdatere Center for Cybersikkerhed med status på hændelsen og eventuelle kompromitteringer. Formålet med kravet til rapportering er bl.a. at øge kapabiliteten på tværs af det europæiske cyberlandskab. Som ledelse kræver det, at I har etableret et incident response beredskab, der sikrer, at konkrete hændelser hurtigt bliver identificeret, rapporteret og håndteret.

7 Gentag modenheds- og risikovurdering jævnligt

Et af hovedpointerne i direktivet er, at organisationer arbejder med et risikobaseret mindset, hvilket indebærer, at man implementerer risikoprocesser i virksomheden. Idet cyberlandskabet ikke er en konstant størrelse, vil risikolandskabet være i forandring. For de omfattede virksomheder og myndigheder betyder det, at modenheds- og risikoprocessen skal gentages med jævne mellemrum, så risici bliver identificeret og mitigeret.

Opsummering

Sådan kommer du godt igang

Når I som ledelse af virksomheden har besluttet at gøre alvor af jeres tanker om cybersikkerhed, og aktivt at gå i gang med at forbedre jer på området, så er det vigtigt at være grundigt forberedt på, hvad der skal foregå.

Antallet af virksomheder, der rammes af cyberangreb er stigende, og vi har efterhånden set mange eksempler i medierne på, hvilke alvorlige konsekvener, det kan få, hvis man som virksomhed bliver ramt af et cyberangreb.

CFO'ens CyberGuide er skabt med henblik på at hjælpe virksomheder med at forholde sig til de udfordringer, der følger i kølvandet på digitaliseringen i form af cyberkriminalitet. Disse udfordringer kræver i stigende grad ledelsens opmærksomhed. Guiden giver ledelsen og CFO'en nogle konkrete råd og anvisninger til, hvordan man bedst muligt modvirker alvorlige cyberangreb og derudover, hvordan man sikrer sig, hvis uheldet skulle være ude.

Vi har her på siderne samlet en koncentreret oversigt over de afsnit, som guiden indeholder. Hvordan du opbygger et solidt cyberstrategisk fundament i tæt samspil med den øvrige ledelse og organisationen. Når du læser den, er det vigtigt, at du er opmærksom på både rækkefølge i planens fokusområder og initiativer men også den sammenhængskraft, der er imellem disse.

Initiativ/fokusområde	Formål
Det digitale trusselsbillede Løbende forståelse og overblik over de digitale trusler i relation til forretningen og konsekvenser for denne.	Skabe indsigt og viden om hvilke digitale trusler, der kan ramme forretningen, hvorfra de kan ramme, og hvilke konsekvenser de kan have på forretningens værdi og eksistens.
CFO'ens centrale rolle Med udgangspunkt i sin centrale placering i virksomhedens finans- og risikostyring, er CFO'en den naturligt ansvarlige for cybersikkerheden.	Understøtte CFO'en i at varetage sin nøglerolle ift. håndtering af cyberrisici – herunder at skabe relevant rapportering omkring cyberrisikovurdering, cyberprogram og fremdrift ift. etablerede handlingsplaner og initiativer for øget sikkerhed bredt i virksomhedens digitale økosystem.
Opbyg et cyberstrategisk fundament Støbe et cyberstrategisk fundament (ramme/program) og sæt en ambition/niveau for sikkerhedsrejsen.	Bygge den strategiske ramme, der løbende skal kunne håndtere cyberrisici og gøre det synligt og tydeligt for nøgleinteressenter, hvordan cybersikkerheden og -kulturen forstærkes og fremdriften heri.
Få styr på virksomhedens vigtigste aktiver Forstå hvilke dele af forretningen, der er vigtigst at beskytte. Herunder de kritiske processer og data, der ligger til grund for værdiskabelsen.	Som ledelse skal I skabe et fælles billede af, hvad der kan udfordre forretningens eksistens, hvis uheldet er ude og dermed skabe fokus på, hvilke sikkerhedsinitiativer der skal igangsættes og hvor.
Teknologivalg Få styr på det teknologiske forsvar – uanset om I selv varetager it-driften, eller har outsourcet denne.	Skabe en forståelse af det teknologiske sikkerhedsniveau her og nu og sæt det i relation til trusselsbilledet, samt hvad der er vigtigst for virksomheden at beskytte. Identificere hvor der er tilstrækkelig beskyttelse, og hvor der skal gøres/investeres i andet/mere.
Bruger- og adgangsstyring Skab en klar og konsekvent bruger- og adgangsstyring som en grundlæggende del af cybersikkerheden.	Med klare politikker og konsekvent identitets- og adgangsstyring for både medarbejdere og eksterne minimeres en væsentlig sårbarhed, de it-kriminelle benytter for at ramme virksomhederne hårdest muligt.
Beredskabsplanlægning Planlæg beredskab og øv dette for at stå stærkest muligt og derved minimere skaderne ved et cyberangreb.	Minimering af konsekvenserne og skaderne ved en cyberhændelse.
Sikkerhedskultur, adfærd og awareness En sikkerhedskultur skal skabes med videndeling, træning i god adfærd og som et samlet produkt af alle de gode sikkerhedsinitiativer, I iværksætter og vedligeholder.	Skabelsen af en sikkerhedskultur bredt forankret i jeres digitale værdikæde med fokus på videndeling, træning i god og sikker digital adfærd og som et samlet produkt af alle de gode sikkerhedsinitiativer I iværksætter og vedligeholder.

Nøglespørgsmål til organisationen

G Governance, risk og compliance

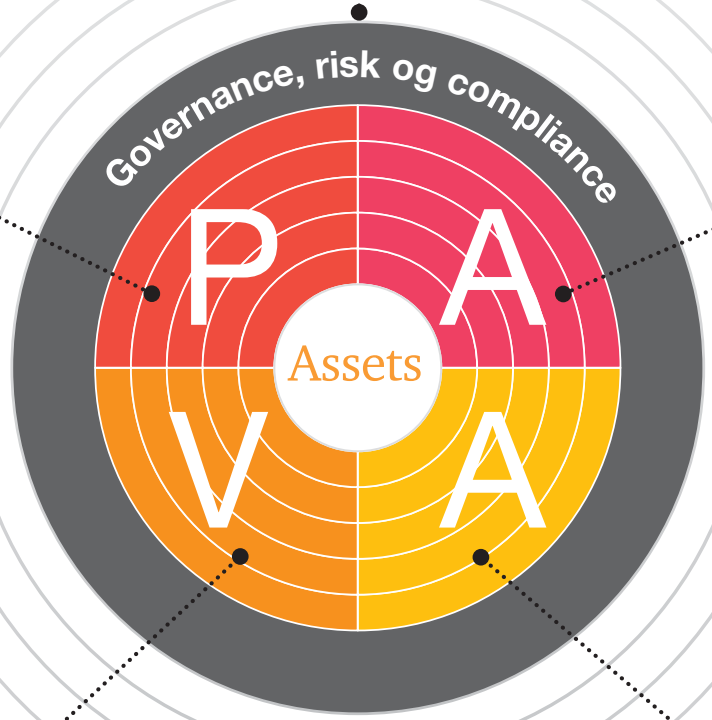
- [ ] Har vi løbende rapportering til bestyrelsen?
- [ ] Har vi identificeret forretningens vigtigste forretningsprocesser samt informationer og data?
- [ ] Har vi i ledelsen en løbende indsigt i de digitale trusler og risici for forretningen?
- [ ] Har vi overvejet en cyberforsikring og dækningerne i denne?
- [ ] Tager vi ansvar for, at vores leverandører har styr på vores cybersikkerhed?

P Procesområdet

- [ ] Har vi en procedure for sikkerhedsopdateringer – bl.a af vores kritiske systemer?
- [ ] Er vores backupprocesser effektive og beskyttet?
- [ ] Har vi adgang til eksterne specialister, der kan assistere os i tilfælde af en kompleks og omfattende hændelse?

A Adfærdsområdet

- [ ] Har vi en fast procedure for sikkerhedsopdateringer – bl.a af vores kritiske systemer?
- [ ] Har vi uddannet og trænet vores medarbejdere, og kan vi dokumentere det?
- [ ] Har vi gennemført testaktiviteter med medarbejderne som fx ved et simuleret phishingangreb?



V Valideringsområdet

- [ ] Får vi løbende testet vores sikkerhedsniveau?
- [ ] Har vi testet og trænet vores beredskab, og er det passende i forhold til vores forretningsrisici?
- [ ] Har vi etableret nødplaner for vores vigtigste forretningsgange?
- [ ] Har vi lavet et review af vores AD-sikkerhed (virksomhedens centrale brugerregister)?

A Arkitekturområdet

- [ ] Har vi to-faktor godkendelse på login (multi factor authentication)?
- [ ] Har vi implementeret Endpoint Detection and Response på brugernes PC'ere?
- [ ] Har vi styr på brugerrettigheder og især overblik med de privilegerede brugere?
- [ ] Har vi segmenteret vores netværk og benytter vi NextGen firewalls?

Vi er din partner

– lokalt og globalt

PwC's globale team inden for Technology & Security består af **3.600+** specialiserede konsulenter.

I Danmark er vi **100+** medarbejdere, der arbejder med cyber- og informationssikkerhed, privacy og data compliance.

Vores team har stor erfaring med at hjælpe danske og internationale virksomheder på tværs af industrier med at vurdere, designe, implementere og forbedre cybersikkerhedsprogrammer.

Sikkerhedscentre i København og Aarhus

- 100 dedikerede sikkerhedskonsulenter
- Data compliance, GDPR og juridiske eksperter
- Forensic eksperter vedrørende it, netværk og malware
- Infrastrukturkonsulenter.

Vores globale netværk

284.258
Medarbejdere og partnere globalt

156
Lande

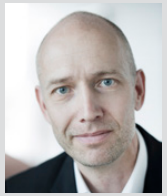
Consulting

9
PwC-kontorer
i Danmark

ServiceCenteret
+45 70 222 444

Kontakt

William Sharp
Partner
Technology & Security
T: 4040 1074
M: william.sharp@pwc.com



Christian Kjær
Partner
Technology & Security
T: 5132 1270
M: christian.kjaer@pwc.com

Anders Balslev
Director
Head of Product & Services
T: 3093 4549
M: anders.balslev@pwc.com

www.pwc.dk/cyber

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...