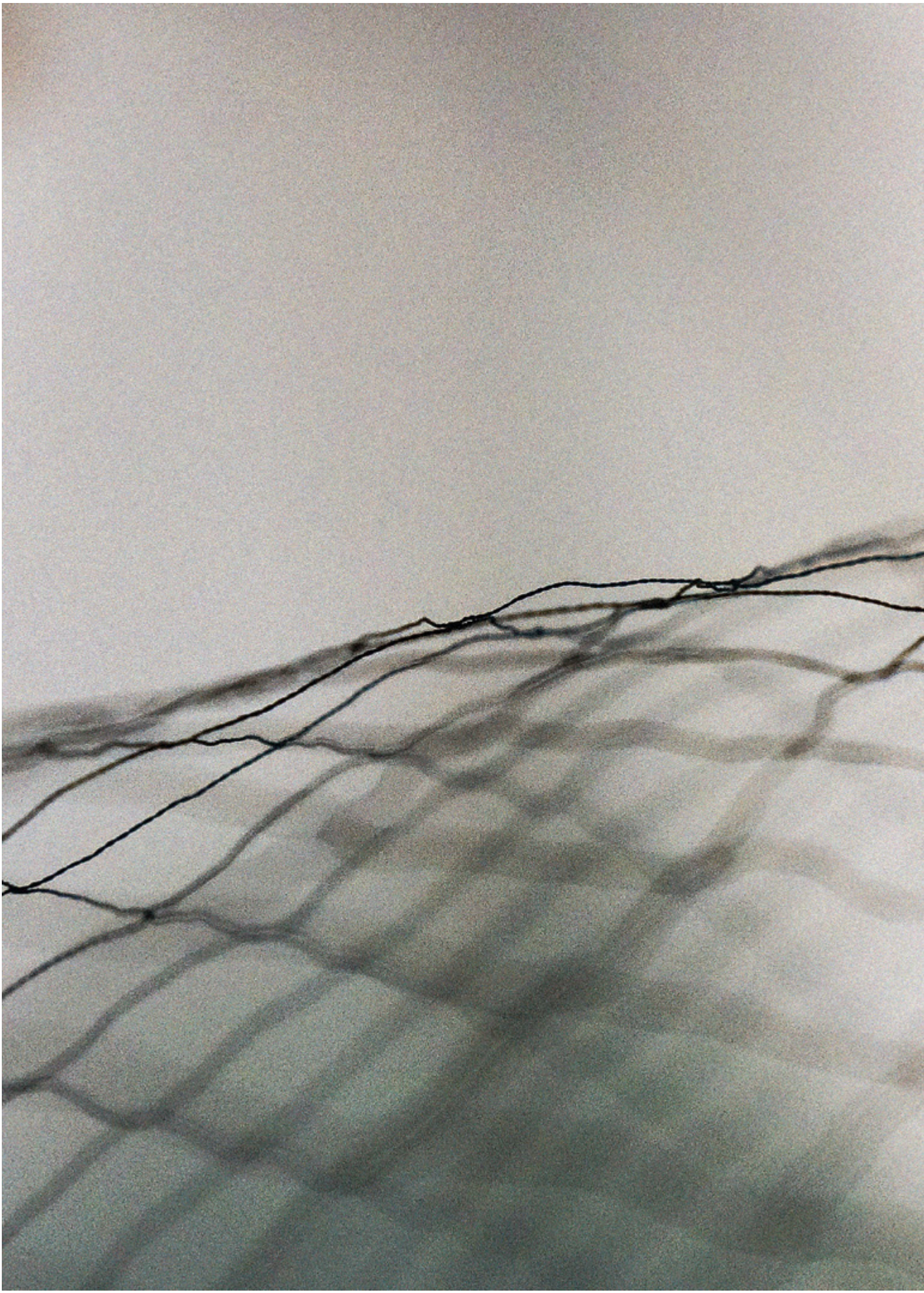
Guide til risikostyring

Risikostyring i forhold til cyber- og informationssikkerhed for smv'er

DANSK STANDARD



Guide til risikostyring

Risikostyring i forhold til
cyber- og informationssikkerhed
for smv'er

Guide til risikostyring
Risikostyring i forhold til cyber- og informationssikkerhed for smv'er
DS/INF 10017:2023

Projektnummer: M362545

Tryk: Dansk Standard
Udgivet 2023

Udgivet af Dansk Standard
Göteborg Plads 1
2150 Nordhavn
Telefon: 39 96 61 01
ds@ds.dk
www.ds.dk

Dette er en POD-publikation
Printet i Danmark

1. oplag

Guiden er udarbejdet af Alexandra Instituttet og Dansk Standard

Indholdsfortegnelse

Forord

Denne guide er udarbejdet af Alexandra Instituttet og Dansk Standard. Guiden er udviklet i samarbejde med en række danske små og mellemstore virksomheder (smv'er) og fageksperter, der har givet input til guiden via workshops og en efterfølgende kommenteringsrunde. Guiden er støttet af henholdsvis Cyber Hub og Erhvervsstyrelsen. Ambitionen er, at denne guide bliver et værdifuldt værktøj til risikostyring for danske smv'er i deres arbejde med cyber- og informationssikkerhed.

Introduktion

Cyber- og informationssikkerhed er gennem de seneste år kommet på flere virksomheders dagsorden. Det er sket i takt med, at cyberangreb ikke længere er noget, der kun rammer enkelte virksomheder, men er blevet en reel trussel, som alle virksomheder bør forholde sig til. Det understreges yderligere af Center for Cybersikkerheds trusselsvurdering, hvor truslen fra cyberkriminalitet vurderes at være meget høj[1]. Samtidig begynder myndighederne i stigende grad at stille krav til cyber- og informationssikkerhed i forbindelse med ny regulering som fx Cyber Security Act, Cyber Resilience Act og det nye NIS-direktiv, hvilket vil få betydning for virksomhederne i de kommende år.

Og det halter en smule med de danske smv'er i forhold til cyber- og informationssikkerhed. En analyse fra Erhvervsstyrelsen viser, at 40 % af de danske smv'er har et for lavt digitalt sikkerhedsniveau i forhold til deres risikoprofil. Dertil kommer, at 24 % af smv'erne ikke anvender de mest basale sikkerhedsforanstaltninger som opdateringer og backup[2], og det kan få store økonomiske konsekvenser for virksomhederne. Det er virksomheden POM Industries, der i 2021 fik standset al produktion på grund af et ransomwareangreb, et eksempel på. Først efter knap en uge fik virksomheden genskabt deres backup og kunne genoptage produktionen[3].

Det er derfor vigtigt, at virksomheder og organisationer er bevidste om og arbejder systematisk med cyber- og informationssikkerhed for at kunne bevare kontrollen og holde forretningen kørende, selvom der skulle komme bump på vejen i form af fx cyberangreb. Man kan dog hurtigt bruge mange ressourcer, hvis man blindt investerer i sikkerhed.

Et væsentligt element i cyber- og informationssikkerhed handler også om at finde et passende niveau af sikkerhed, således at man får adresseret de rigtige risici først. Et godt udgangspunkt for at højne sit sikkerhedsniveau er derfor at få kortlagt sin risikoprofil og begynde at arbejde konkret med håndteringen af disse risici.

Og det er netop formålet med denne guide: At samle gode råd om og præsentere redskaber til hvordan man kan arbejde konkret med risikostyring i forhold til cyber- og informationssikkerhed.

Guiden tager sit afsæt i standarder. Standarder spiller en særlig vigtig rolle i arbejdet med risikostyring, da de netop repræsenterer en systematisk tilgang. Standarder er udtryk for best practice og er udarbejdet af eksperter fra hele verden. Standarders formål er at skabe fælles retningslinjer og en fælles tilgang. For en mindre virksomhed kan standarder ofte virke uoverkommelige. Målet med denne guide er således også at forklare standardernes tilgang til risikostyring i et forenklet sprog og anvende konkrete eksempler.

Målgruppen for guiden er smv'er, der gerne vil i gang med at arbejde med risikostyring, men ikke nødvendigvis har den store forhåndsviden. Større virksomheder vil dog også kunne finde inspiration i guiden.

Guiden fungerer som et supplement til Erhvervsstyrelsens IT-risikovurderingsværktøj[4], men dækker bredere ved at kigge på andre parametre end virksomhedernes IT-sikkerhed og de tekniske risici.

---

[1] https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/
[2] Digital sikkerhed i danske SMV'er 2021
[3] https://sikkerdigital.dk/virksomhed/virksomhedscases/pom-industries
[4] https://virksomhedsguiden.dk/content/ydelser/it-risikovurderingsvaerktoej/fce38da7-025d-4326-98fe-c198f3ad8316/

1 Introduktion til risikostyring – sådan kommer I godt i gang

Denne guide sætter fokus på risikostyring i forhold til cyber- og informationssikkerhed. Risikostyring er kort fortalt en metode til at identificere, prioritere og håndtere sin virksomheds potentielle risici. Risici kan bestå af såvel interne som eksterne faktorer, som kan udgøre en trussel mod en virksomheds eksistens. De interne faktorer kan fx være medarbejdernes digitale adfærd eller servernedbrud, mens eksterne faktorer kan være naturkatastrofer eller hackerangreb. Risikostyring er helt centralt for en virksomhed og nødvendigt for at sikre virksomhedens overlevelse. Man vil aldrig kunne fjerne alle risici fuldstændig, men ved at have en systematisk tilgang til risici, er man bedre rustet til uforudsete hændelser, ligesom det kan bidrage til at mindske konsekvenserne. Et alarmsystem kan fx bidrage til at afværge indbrud på samme måde som en brandalarm med sprinkler måske vil kunne minimere konsekvensen ved brand.

Langt de fleste virksomheder arbejder med risikostyring i et eller andet omfang. Der er som regel styr på de økonomiske risici, og det er også de færreste virksomheder, hvor der fx ikke er en lås på hoveddøren. Men det er langt fra alle virksomheder, der arbejder systematisk med risikostyring. Især når det handler om risikostyring i forhold til cyber- og informationssikkerhed. Der er derfor et stort behov for at adressere cyber- og informationssikkerhed og systematisere arbejdet med risikostyring på linje med fx økonomiske risici.

Arbejdet med risikostyring i forhold til cyber- og informationssikkerhed er primært relevant for virksomheder og organisationer, der i en eller anden grad er digitaliserede; fx virksomheder med et digitalt faktureringssystem, mailsystem eller webshop. Men det er efterhånden de færreste virksomheder og organisationer, der kan sige, at de på ingen måde er digitaliserede. For selvom det digitale måske ikke er kerneforretningen, er det i mange virksomheder blevet et essentielt understøttende værktøj, der potentielt kan have stor indvirkning på forretningen.

Der er mange fordele ved at arbejde systematisk med risikostyring i forhold til cyber- og informationssikkerhed. For det første bidrager det til at ruste virksomheden, så den er forberedt, hvis den skulle blive udsat for fx IT-kriminalitet. Derudover kan en systematisk tilgang til risikostyring i forhold til cyber- og informationssikkerhed være et konkurrenceparameter og gøre en virksomhed mere attraktiv for kunder, samarbejdspartnere og eventuelle investorer. At have styr på cyber- og informationssikkerhed er ofte også et udpræget markedskrav, da kunder og samarbejdspartnere har en forventning om, at der er taget hånd om og stilling til en række potentielle risici.

Men hvordan kommer man godt i gang med risikostyring i forhold til cyber- og informationssikkerhed? For det første handler det om, at beslutningen om at gøre en aktiv indsats har ledelsens fulde opbakning, og at der er afsat ressourcer til arbejdet. Derefter handler det om at få delt arbejdet op i nogle overkommelige 'bidder'. Denne guide er et bud på en lettilgængelig gennemgang af en risikostyringsproces og vil gennemgå processerne i risikostyring trin for trin.

Tid, kompetencer og ressourcer (økonomi og medarbejdere) er nogle af de barrierer, der oftest afholder virksomheder fra at give sig i kast med risikostyring. Det kan være tidskrævende at starte en proces for risikostyring op, men det er godt givet ud, da det i sidste ende vil frigive mere tid til kerneforretningen, hvis man ikke hele tiden skal arbejde med krisehåndtering. I sidste ende handler det om at prioritere.

Endelig er det vigtigt at huske, at arbejdet med risikostyring er en løbende proces, som bør gentages regelmæssigt og efter behov, da risici ændrer sig i takt med, at virksomheden og omverdenen forandrer sig. Så at arbejde med risikostyring i forhold til cyber- og informationssikkerhed handler i høj grad om en kulturændring og en ny tilgang til ens virksomhed.

Cyber- og informationssikkerhed
Cybersikkerhed og informationssikkerhed bruges som et samlet begreb igennem guiden, men man kan godt adskille dem. Informationssikkerhed handler om beskyttelse af inforamationer – og her er der tale om alle informationer, hvad enten de er digitale (på en computer, i en sky, på en server osv.) eller fysiske (fx i et dokument i et arkivskab). Cybersikkerhed handler bl.a. også om at beskytte informationer, men er kun fokuseret på digitale informationer. Cybersikkerhed handler desuden ikke udelukkende om beskyttelse af informationer, men også om forsvar af enheder eller produkter, der er koblet på internettet.

2 Præsentation af parametre og eksempler

I afsnit 3 vil risikostyringsprocessen blive beskrevet trin for trin. For at konkretisere og gøre processerne mere håndgribelige vil hvert trin i risikostyringsprocessen blive illustreret gennem konkrete eksempler. Eksemplerne er fiktive, men tager udgangspunkt i typiske virksomhedsparametre. De parametre, som eksemplerne er bygget op omkring, er

- digitalisering af virksomheden
- fortrolighed af data anvendt i virksomheden
- virksomhedens placering i leverandørhierarkiet
- antallet af brugere.

De fire ovennævnte virksomhedsparametre er udvalgt, da de alle kan have stor betydning for en virksomheds tilgang til risikostyring. Fx vil en traditionel, mindre murer- eller tømrervirksomhed sandsynligvis ligge 'lavt' på digitaliserings- og fortrolighedsparametrene, da IT måske kun bruges af bogholderiet, mens forretningen mere eller mindre er manuelt baseret. Det kan dog hurtigt ændre sig, hvis virksomheden fx har kunder med fortrolige plantegninger eller lignende, som forsvaret, fængsler eller lufthavne. Samtidig er virksomhedens IT-drift måske outsourcet til en anden leverandør, hvilket kan blive problematisk i tilfælde af problemer hos leverandøren.

Digitalisering af virksomheden
Hvor digital en virksomhed er, spiller en vigtig rolle i forhold til risikostyringen, og derfor anvendes der i guiden et parameter, der ser på hvor digital virksomheden er. I nogle virksomheder anvendes IT primært til støttefunktioner som fx bogholderiet. Et IT-nedbrud kan derfor få mindre konsekvenser, idet selve forretningen kan fungere mere eller mindre upåvirket i forholdsvis lang tid. I andre virksomheder er IT en forudsætning for forretningen (som fx en webshop), og et nedbrud kan standse al aktivitet, indtil problemet er løst.

Fortrolighed af data anvendt i virksomheden
Det andet parameter, som er udvalgt, er omfanget af fortrolige data anvendt i virksomheden, da det også har stor indflydelse på, hvordan man tilrettelægger sin risikostyringsproces. Et læk af fortrolige data vil nemlig ikke kun få konsekvenser for virksomheden selv, men kan også have personlige konsekvenser for medarbejdere, kunder, leverandører mm. Langt de fleste virksomheder behandler fortrolige data i forbindelse med lønsystemer, men derudover er det ikke sikkert, at de behandler fortrolige data. Hvis virksomheden fx arbejder inden for sundhedssektoren eller inden for forsvarsindustrien, er det naturligvis oplagt, at fortrolige data skal beskyttes. I forhold til en B2B-virksomhed er det ikke sikkert, at de behandlede data er videre fortrolige.

Virksomhedens placering i leverandørhierarkiet
Stort set alle virksomheder samarbejder med andre virksomheder; enten som leverandør eller som aftager af ydelser. Disse relationer er også vigtige at forholde sig til i forbindelse med risikostyring, da potentielle risici kan have konsekvenser for andre uden for ens egen organisation. Hvis man fx leverer ydelser til en organisation, som grundet sin natur er særligt udsat for cyberangreb, kan man opleve selv at blive et mål for cyberkriminalitet. Ligeledes kan man selv have outsourcet (kritiske) dele af sin forretning til en underleverandør, fx hosting af webshop hos ekstern leverandør. I sit risikostyringsarbejde bør man se på, hvilke dele leverandøren har ansvaret for. Ud fra dette bør man have afklaret sikkerhedsmæssige forhold med sine leverandører og kunder.

Antallet af brugere
Et sidste parameter, som også kan have indflydelse på risikostyringsprocessen, er antallet af brugere, som i denne sammenhæng er alle de berøringsflader, virksomheden har. Det kan fx være kunder og samarbejdspartnere eller andre, som virksomheden er i berøring med. Jo flere berøringsflader der er, jo flere potentielle risici kan der være at forholde sig til. Samtidig vil et større antal brugere også medføre, at flere vil være berørte af en evt. hændelse, og dermed bliver konsekvensen større.

EKSEMPLER ANVENDT I GUIDEN

Med udgangspunkt i de typiske parametre bliver der i det følgende givet tre eksempler på virksomheder, som er gennemgående i hele guiden. For hvert trin i risikostyringsprocessen bliver det via eksemplerne illustreret, hvordan de typiske parametre påvirker processen, og hvad man skal være særligt opmærksom på. Eksemplerne indeholder også en kort beskrivelse af, hvad man kan gøre, og hvilke resultater man kan forvente. Eksemplerne er ligeledes gengivet i anneks B, der indeholder en samlet gennemgang af risikostyringsprocessen for de tre virksomhedseksempler.

Figur 1: Beskrivelse af de tre eksempler

VIRKSOMHED A
Autoværkstedet

Mindre autoværksted
Mindre grad af digitalisering. Ingen fortrolige/personfølsomme data. Har private kunder og forskellige leverandører af materialer. Dog ikke kunder med særlige krav. Relativt få brugere.

VIRKSOMHED B
Produktionsvirksomheden

Mellemstor virksomhed
(omkring 85 ansatte), der producerer og installerer videoovervågningssystemer. Høj grad af digitalisering. Stor mængde fortrolige data. Stor snitflade med mange brugere; kunder, samarbejdspartnere, leverandører mm. Leverer til kritisk infrastruktur.

VIRKSOMHED C
Webshoppen

Lille virksomhed
(fire ansatte), der importerer vin. Høj grad af digitalisering (100 % webshop). Mange brugere af webshoppen. Nogen grad af fortrolige data. Benytter sig i høj grad af leverandører i forhold til IT-driften.

3 Risikostyring trin for trin

I dette afsnit gennemgås en risikostyringsproces trin for trin, der kobles sammen med de tidligere nævnte eksempler og parametre. Guiden tager udgangspunkt i principperne fra standarden ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks, der er en international anerkendt og udbredt standard med fokus på risikostyring i forhold til cyber- og informationssikkerhed. Der findes en række andre forskellige tilgange til risikostyring, og en håndfuld af disse er kort introduceret i anneks A.

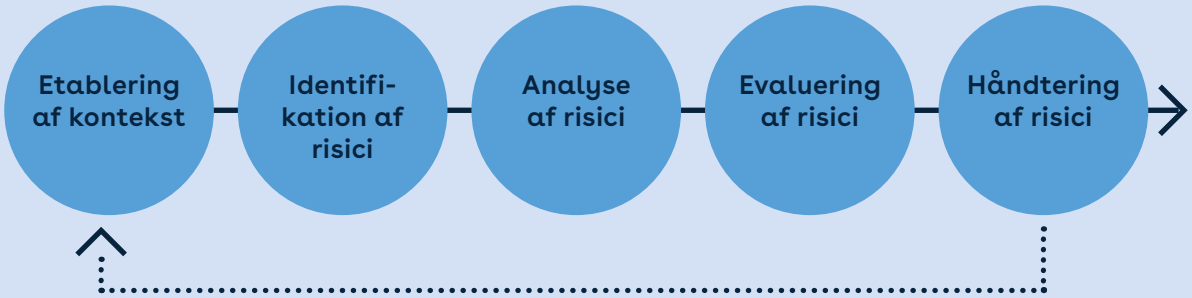
ISO/IEC 27005 deler risikostyring op i fem trin, som denne guide også tager udgangspunkt i:

- Etablering af kontekst – afdækning af virksomhedens interne og eksterne interessenter
- Identifikation af risici – interne og eksterne risici
- Analyse af risici
- Evaluering af risici
- Håndtering af risici.

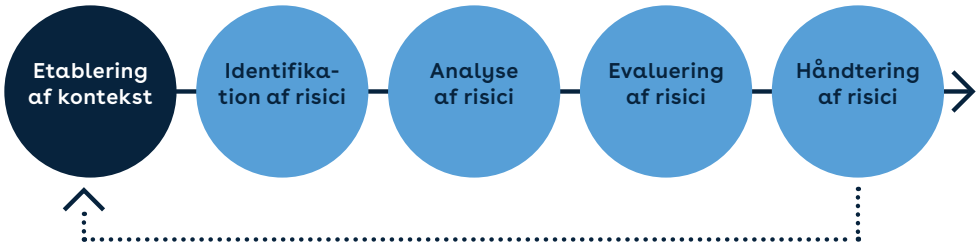
De tre midterste trin – identifikation, analyse og evaluering – udgør tilsammen det, som ofte kaldes risikovurdering. Den skelnen kan være relevant at huske, da nogle standarder og værktøjer udelukkende er beregnet til en del af den samlede risikostyringsproces. Fx håndterer ISO/IEC 27005 hele risikostyringsprocessen, mens tilgangen 'OCTAVE Allegro'[5] arbejder med risikovurdering og derfor ikke omfatter selve håndteringen af identificerede risici.

Figuren nedenfor viser den risikostyringsproces, der er gennemgående i guiden. Selvom processen er inddelt i fem trin, inddeler man ikke altid processerne så skarpt i praksis. Ofte vil identifikationen, analysen og evalueringen smelte mere eller mindre sammen (risikovurdering).

Figur 2: Risikostyringsprocessen



[5] Se anneks A for yderligere beskrivelse.



3.1 Etablering af kontekst

Da ingen virksomheder er ens, vil stort set alle virksomheder have unikke karakteristika, der skal tages hensyn til i forbindelse med risikostyringen. Det første skridt i en risikostyringsproces er derfor at etablere virksomhedens kontekst; dvs. at I skal se på jeres formål og definere, hvem der er henholdsvis jeres interne og eksterne interessenter. Formålet med denne fase er at forstå jeres virke og forberede den videre proces i forhold til risikostyring, herunder at fastlægge selve metoden for risikostyring.
I den forbindelse er der også behov for, at I afdækker, hvad cyber- og informationssikkerhed betyder for jer, og dermed udvælger de informationer og systemer, som er særligt vigtige for jer at beskytte.

Det kan sandsynligvis have alvorlige konsekvenser for jer, hvis informationer ødelægges, stjæles eller på anden vis bliver utilgængelige. Informationerne behøver ikke at være kategoriseret som persondata for at være forretningskritiske. Det kan fx også være data, som er afgørende for at holde produktionen i gang, forretningshemmeligheder eller finansielle oplysninger. Persondata er dog et eksempel på data, der er omfattet af eksterne krav (GDPR-lovgivningen). I praksis betyder det, at der kan gælde særlige krav til behandlingen af visse datatyper, som I ikke selv bestemmer. Derfor vil I til at starte med også have brug for at kortlægge, hvilke eksterne krav I eventuelt er underlagt.

Fastlæggelse af rammerne for risikostyringsprocessen
For at vide hvordan I skal vurdere forskellige risici senere i processen, er det nødvendigt, at I ser nærmere på de forretningskritiske processer samt de tilhørende informationer, som er vigtige for jer at beskytte; de såkaldte primære aktiver. Der skelnes ofte mellem primære og understøttende aktiver. De primære aktiver dækker over forretningsprocesser, information og viden. De understøttende aktiver er IT-udstyr, software, hardware, personale og fysiske placeringer. De understøttende aktiver er med til at understøtte forretningsprocesserne og bidrager til, at virksomheden opbevarer og bearbejder informationer.

For at kunne udpege de vigtigste informationer, der skal beskyttes, skal både interne og eksterne forhold afdækkes:

- Virksomhedens karakteristika; strategi, mål, vision og mission. Hvad er jeres virksomhed sat i verden for at udføre? Hvilke best practices følger I? Og hvilke lov- og aftalekrav er I underlagt?
- Identifikation af interessentlandskabet og interessenters forventninger. Hvad er jeres interessenters forventninger og krav til jer, når det kommer til cyber- og informationssikkerhedsindsats? Hvordan skal disse prioriteres?
- Identifikation af forretningsprocesser. Det kan fx være spørgsmål som: Hvordan får I kunder? Hvordan udføres arbejdet for kunden? Hvordan faktureres kunden? Hvilke processer er kritiske for, at I som virksomhed kan fungere – både på kort og langt sigt?

Figur 3: Eksempel på risikoberegning

Både de interne forhold samt interessenters krav og forventninger er en hjælp til at udpege risici og muligheder. Dermed danner de også grundlag for, at I kan formulere jeres formål med cyber- og informationssikkerhed. Sådanne mål kan fx være: compliance, skabe tillid hos kunder, beskytte kritiske aktiver, sikre business continuity osv.

Forberedelse af risikostyringsprocessen og metodevalg

Til at starte med handler det også om at præcisere de næste skridt i risikostyringsprocessen, og her er det vigtigt, at I gør jer nogle overvejelser om, hvilken metode I gerne vil anvende for den videre proces. Som virksomhed kan I selv bestemme, hvilken fremgangsmåde I ønsker at følge for den videre risikostyringsproces. Men det er vigtigt, at I anvender en metode, som gør det muligt at sammenligne resultater. På dette trin opstiller I kriterier for identifikation, analyse og evaluering af risici, og I definerer kriterierne for, hvornår en risiko kan accepteres. Her definerer I også de forskellige niveauer af sandsynlighed og konsekvens. Med sandsynlighed menes sandsynligheden for, at en hændelse indtræffer, mens konsekvens dækker over, hvilken konsekvens det vil få for virksomheden.

Kvalitativ og kvantitativ tilgang til at udregne risiko

Der er flere måder, I kan udregne en risiko på, når I skal forholde jer til sandsynlighed og konsekvens. Er I en lille virksomhed, vil det oftest være nemmest at gøre det simpelt ved en **kvalitativ tilgang**. Det kan fx være en skala fra 1-4 for sandsynlighed og en skala fra 1-4 for konsekvens. For hvert trin på skalaerne har man defineret, hvad det enkelte trin betyder. Sandsynligheden på en skala fra 1-4 vil spænde fra 'meget lidt sandsynligt' til 'meget sandsynligt', og konsekvensen på en skala fra 1-4 vil spænde fra 'mindre konsekvenser' til 'katastrofale konsekvenser'.

En anden tilgang er den **kvantitative metode**, hvor I udregner sandsynlighed ud fra fx procentsatser og konsekvens ud fra tab i omkostninger, hvis en hændelse indtræffer. Det kan være tidskrævende og ofte svært at skaffe de data, der gør, at man er i stand til at benytte en kvantitativ metode, hvorfor de fleste vælger den kvalitative metode.

Metodevalg, definition af niveauer for konsekvens, sandsynlighed og risikoaccept bør være i overensstemmelse med virksomhedens politikker, målsætninger og interessenter. Sidst, men ikke mindst, er der brug for, at I træffer beslutninger om organiseringen af risikostyringsprocessen, hvor der uddelegeres roller og ansvar. Her er det vigtigt, at der udpeges en passende risikoejer, og at der fra ledelsens side naturligvis er opbakning til hele processen. En risikoejer er den, der udpeges til at have ansvaret for en eller flere risici. Det er ikke nødvendigvis risikoejeren, der skal håndtere risici, men det er risikoejerens ansvar, at der bliver taget hånd om en risiko. Når de konkrete risici identificeres senere i processen, vil der eventuelt være behov for at udpege flere risikoejere. Risikoejerbegrebet bliver gennemgået yderligere i afsnit 3.2 om risikoidentifikation.

Et metodevalg vil typisk som minimum indeholde følgende:

- Fastsættelse af niveauer for konsekvens og sandsynlighed og hvad de betyder. Fx kunne 'middel konsekvens' betyde et tab på mellem 100.000 kr. og 500.000 kr. eller mellem 1 % og 5 % af virksomhedens omsætning.
- Hvordan beregnes risiko? Fx niveau for konsekvens x sandsynlighed (se figur 3).
- Hvornår kan en risiko accepteres? Fx 'Risici accepteres, når de er under værdien X'.
- Definition af kriterier for risikoejer. Fx 'Ansvaret for risici under værdi X ligger hos afdelingsledere' eller 'Ansvaret for risici over værdi X ligger hos den administrerende direktør'.

EKSEMPLER PÅ ETABLERING AF KONTEKST

Konteksten for **virksomhed A** (autoværkstedet) kan se ud som følger: Virksomheden vurderer, at størstedelen af kunderne kommer ind fra gaden, og kun ca. 30 % laver en forudgående tidsbestilling på virksomhedens hjemmeside. Værkstedet bruger primært IT til regnskab og tidsbestilling, men har også et par computere med specialprogrammer, som bruges af mekanikerne. Disse computere er dog ikke internetopkoblede. Værkstedet behandler ikke følsomme (person-)data, udover kontaktinformation til kunder, lønsedler og lignende. Der skal derfor ikke tages hensyn til følsomme persondata. Den primære bekymring er derfor tab af omsætning, idet læk af data ikke vurderes som særlig relevant, og virksomheden ikke er underlagt særlig lovgivning som fx NIS-direktivet[6].

Da virksomheden er forholdsvis lille, vil etablering af konteksten kunne udføres af ejeren af værkstedet sammen med værkstedets bogholder. Det kan foregå som et uformelt møde på en halv time, hvor strategi og mission italesættes, og hvor interessentlandskabet kortlægges. Deltagerne behøver ikke medbringe noget særligt forarbejde udover deres baggrundsviden. Selve processen kan dokumenteres som et referat af beslutningerne.

På baggrund af ovenstående og virksomhedens størrelse vælger virksomheden, at risikovurderingen skal foregå med tre niveauer for konsekvens (lav, middel og høj) afhængigt af størrelsen på det forventede tab (0-25.000 kr., 25.001-200.000 kr. og 200.001+ kr.). Se tabel A1.

Sandsynlighed opdeles ligeledes på tre niveauer (lav, middel og høj) afhængigt af intervallet; ('forventer ikke, at det kan ske', 'kan ske inden for 2 år' og 'forventer, det sker mindst årligt'): Se tabel A2.

Risikovurderingen gentages en gang om året og er relativt uformel. I forbindelse med vurderingen sparres der med IT-leverandøren og revisoren. Da ejeren af værkstedet har al kontakt med IT-leverandøren, er det samtidig ejeren, der er risikoejer for alle risici. Det besluttes, at alle høj/høj (rød) risici skal udbedres hurtigst muligt, mens lav/middel (grøn) risici accepteres. Middel/middel og middel/høj (gul) risici skal vurderes løbende. Se tabel A3.

Tabel A1

KONSEKVENS	Lav	Middel	Høj
BELØB	0-25.000 kr.	25.001-200.000 kr.	200.001+ kr.

Tabel A2

SANDSYNLIGHED	Lav	Middel	Høj
INTERVAL	'Forventer ikke, at det kan ske'	'Kan ske inden for 2 år'	'Forventer, det sker mindst årligt'

Tabel A3

		SANDSYNLIGHED		
		Lav	Middel	Høj
KONSEKVENS	Lav	Lav/Lav	Middel/Lav	Høj/Lav
	Middel	Lav/Middel	Middel/Middel	Høj/Middel
	Høj	Lav/Høj	Middel/Høj	Høj/Høj

[6] Direktivet om net- og informationssystemers sikkerhed (NIS-direktivet) (EU) (2022/2555) har fokus på at beskytte EU's kritiske infrastruktur og økonomier.

For **virksomhed B** (produktionsvirksomheden, der installerer og udvikler løsninger til videoovervågning), kunne konteksten se sådan ud: IT bruges til regnskab, projektstyring og en række andre administrative funktioner. Det anvendes derudover også i forbindelse med installation af løsninger hos kunder. Virksomhedens løsninger har en funktionalitet, der løbende sender vedligeholdelsesdata hjem til virksomheden, ligesom virksomheden har mulighed for at koble sig på løsninger via internettet for at foretage fjernsupport. Virksomhedens kunder er primært private hjem, men den har også en række produkter målrettet virksomheder og større organisationer. På grund af ovenstående skal der i sikkerhedsarbejdet tages højde for, at der kan forekomme persondata i virksomhedens systemer. Samtidig kræver nogle af de større kunder, at der er styr på informationssikkerheden og ønsker dokumentation herfor.

For at sikre en høj grad af dokumentation bliver alle beslutninger dokumenteret og gemt i virksomhedens ledelsessystem baseret på standarden ISO/IEC 27001. Beslutningerne inkluderer en liste over interessenter (både interne og eksterne), der skal inddrages i processen, krav, der skal leves op til (GDPR og ISO/IEC 27001), samt hvor ofte risikovurderingsprocessen gentages, af hvilke dele af virksomheden og af hvem. Det besluttes at arbejde med fem niveauer af konsekvens (forventede tab: 0-50.000 kr., 50.001-125.000 kr., 125.001-500.000 kr., 500.001-2.500.000 kr. og 2.500.001+ kr.): Se tabel B1. Og på samme måde fem niveauer for sandsynlighed (dagligt, ugentligt, kvartalsvist, årligt, 10-års hændelse): Se tabel B2.

Niveauerne skal dog justeres løbende, når virksomheden har fået mere erfaring med processen. Risiko beregnes som produktet af konsekvensscore x sandsynlighed og kan derfor ligge på mellem 1 og 25. Se tabel B3.

Hændelser med risiko på under 10 accepteres (grøn), og alt derover skal så vidt muligt nedbringes. Dog kan produktejer acceptere risici på op til og med 16 (gul), mens højere risici (rød) skal accepteres på direktionsniveau.

Tabel B1

KONSEKVENS	1	2	3	4	5
BELØB	0-50.000 kr.	50.001-125.000 kr.	125.001-500.000 kr.	500.001-2.500.000 kr.	2.500.001+ kr.

Tabel B2

SANDSYNLIGHED	1	2	3	4	5
INTERVAL	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt

Tabel B3

		SANDSYNLIGHED				
		10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
KONSEKVENS	0-50.000 kr.	1	2	3	4	5
	50.001-125.000 kr.	2	4	6	8	10
	125.001-500.000 kr.	3	6	9	12	15
	500.001-2.500.000 kr.	4	8	12	16	20
	2.500.001+ kr.	5	10	15	20	25

Virksomhed C (webshoppen) startede som en enkeltmandsvirksomhed, der importerer vin, men er siden vokset og beskæftiger nu fire personer. Virksomheden er mere eller mindre 100 % baseret på virksomhedens webshop, hvor alle ordrer bliver modtaget. Da webshoppen er omdrejningspunktet for virksomheden, indsamles der så meget data som muligt med henblik på marketing og viden om kunderne. Disse data er persondata og derfor underlagt GDPR-lovgivning. De ansatte i virksomheden er ikke specielt IT-kyndige, og al IT er derfor cloudbaserede løsninger, ligesom et eksternt webbureau har ansvaret for driften af webshoppen.

Selve kontekstbeskrivelsen for virksomhed C minder meget om beskrivelsen fra virksomhed A. Dette skyldes, at virksomhederne anvender samme (uformelle) tilgang til processen med tre niveauer for konsekvens og sandsynlighed (se tabel C1 og C2). På samme måde besluttes det, at alle 'høj/høj' (rød) risici skal udbedres hurtigst muligt, mens 'lav/middel' (grøn) risici accepteres. 'Middel/middel' og 'middel/høj' (gul) risici skal vurderes løbende. Se tabel C3.

Virksomhed C adskiller sig dog fra virksomhed A ved at have et større fokus på GDPR og flere dele udliciteret til leverandører, hvilket er relevant i de efterfølgende trin.

Tabel C1

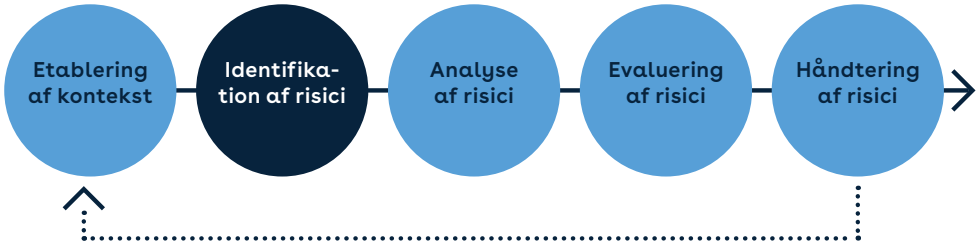
KONSEKVENS	Lav	Middel	Høj
BELØB	0-25.000 kr.	25.001-200.000 kr.	200.001+ kr.

Tabel C2

SANDSYNLIGHED	Lav	Middel	Høj
INTERVAL	'Forventer ikke, at det kan ske'	'Kan ske inden for 2 år'	'Forventer, det sker mindst årligt'

Tabel C3

		SANDSYNLIGHED		
		Lav	Middel	Høj
KONSEKVENS	Lav	Lav/Lav	Middel/Lav	Høj/Lav
	Middel	Lav/Middel	Middel/Middel	Høj/Middel
	Høj	Lav/Høj	Middel/Høj	Høj/Høj



3.2 Identifikation af risici

Det andet trin i risikostyringsprocessen er identifikation af risici. Det er en vigtig proces, da den danner baggrund for den videre analyse, evaluering og håndtering af risici. Det er kun de risici, I identificerer i denne proces, I arbejder videre med. Det er derfor vigtigt, at I ikke overser potentielle risici. Identifikation af risici kan inddeles yderligere i to processer; identifikation og beskrivelse af informationssikkerhedsrisici samt identifikation af risikoejere.

Identifikation og beskrivelse af informationssikkerhedsrisici
Den første proces handler om at lokalisere, identificere og beskrive potentielle risici ved at se på kilder til risici og potentielle hændelser. Formålet er at udarbejde en liste over alle de risici, der kan hindre, påvirke eller forsinke opfyldelsen af jeres mål eller true jeres forretningsgrundlag. Når I skal udarbejde jeres risikoidentifikation, er der to tilgange, I kan benytte jer af:

- Den hændelsesbaserede tilgang
- Den aktivbaserede tilgang.

Fælles for tilgangene er, at de giver samme output, nemlig en liste over identificerede risici. Listen indeholder beskrivelser af og antagelser om de enkelte risici, så man efterfølgende kan foretage risikoanalysen. Selvom resultatet er det samme for begge tilgange, kræver de forskelligt input. Den hændelsesbaserede tilgang forudsætter, at I har et overblik over potentielle hændelser, der kan ramme virksomheden, og har særligt fokus på konsekvenserne. Den aktivbaserede tilgang forudsætter, at I har en oversigt over virksomhedens væsentlige aktiver (fx data), og vil have særligt fokus på sandsynligheden.

Den hændelsesbaserede tilgang
Denne tilgang tager udgangspunkt i hændelser og deres konsekvenser – altså hvilke typer af cyberangreb kan vi forestille os, og hvilke konsekvenser vil det have? Ved denne tilgang vurderes sandsynligheden for, at en hændelse sker, og hvilke konsekvenser den har. Ofte kan hændelser og deres konsekvenser bestemmes ved at identificere de bekymringer, den øverste ledelse eller andre risikoejere måtte have. Det kunne fx være en frygt for ikke at kunne modtage ordrer pga. et phishing-/ransomwareangreb.

Fordelen ved den hændelsesbaserede tilgang er, at den er rimelig let forståelig. "Hvad sker der, hvis vi bliver ramt af ransomware?" er et forholdsvis veldefineret spørgsmål, man kan undersøge. Hvis I vælger den hændelsesbaserede tilgang, vil I dog kun få undersøgt de hændelser, I har fantasi til at forestille jer. Der kan hentes inspiration i lister over mulige hændelser, men det vil dog ofte være nødvendigt at rette til, så det passer til jeres kontekst. Eksempler på lister kan findes i henholdsvis Tabel E-2 i NIST SP-800-30[7] eller Tabel A.10 i anneks A i standarden ISO/IEC 27005[8], men man kan også bruge mindre formelle lister, som fx det overblik over potentielle trusler mod virksomheder, man kan finde på sikkerdigital.dk[9].

[7] NIST SP-800-30 Guide for conducting Risk Assessments
[8] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks
[9] https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed

Trusselskatalog fra sikkerdigital.dk:

- Ransomware (online afpresning)
- Phishing
- CEO-fraud (direktørsvindel)
- Fakturabedrageri
- DDoS-angreb (overbelastningsangreb)
- Bevidste insidere
- Cyberspionage
- Virus og malware

Læs mere om de enkelte trusler på sikkerdigital.dk

Udfordringen ved brugen af trusselskataloger er at finde (eller tilrette) et katalog, som vil passe med jeres virksomheds modenhed og målet for risikovurderingen.

Den aktivbaserede tilgang

Denne tilgang tager udgangspunkt i de aktiver, dvs. data, enheder eller funktioner, der ligger i jeres virksomhed, og vurderer de sårbarheder og trusler, der er mod aktiverne. Et aktiv er alt, hvad der har værdi for jeres virksomhed og derfor kræver beskyttelse. Det kan fx være de data, som ligger i jeres faktureringssystem, idet fraværet (eller ændring) af disse vil forhindre fakturering af kunderne og medføre tab. Et andet eksempel kan være designdokumenterne/planerne, der anvendes i en produktionsvirksomhed, da en konkurrent ville kunne kopiere produktet, hvis de fik adgang til aktivet. Efter at I har identificeret jeres aktiver, kan I derefter se på, hvad der kan påvirke aktiverne, og hvad der derfor er en potentiel trussel.

Fordelen ved den aktivbaserede tilgang er, at I tager udgangspunkt i noget velkendt. Det kan gøre det lettere at starte arbejdet, da I skal se ind i virksomheden og identificere det, som har værdi for jer. I kan derefter se på mulige sårbarheder og trusler og derudfra beskrive nogle risikoscenarier. Ligesom i den hændelsesbaserede tilgang kan det være en fordel at bruge et register over kendte sårbarheder og trusler, fx CVE-databasen[10], så man ikke overser noget. ISO/IEC 27005[11] indeholder også lister over både trusler og sårbarheder, og ENISA[12] har også udarbejdet et trusselskatalog, man kan lade sig inspirere af til risikoidentifikationen.

Hvis man har et godt overblik over vigtige data og systemer, kan det derfor være en god idé at tage udgangspunkt i den aktivbaserede tilgang. Hvis man mangler det overblik, kan den hændelsesbaserede tilgang være et godt sted at starte. I forbindelse med risikoidentifikationen, vil man ofte ende med at få en (for) lang liste over risici. Selvom det kan virke uoverskueligt med de mange risici, vil analysen og evalueringen ofte afsløre, at de fleste risici er så små, at de kan accepteres.

Identifikation af risikoejere

Risikoejere har ansvaret for og beføjelsen til at forvalte de risici, de er ansvarlige for. Det er ikke nødvendigvis risikoejeren, der skal nedbringe risici, men det vil være risikoejeren, der står på mål for risici. Hvis en risiko ikke har nogen ejer, er der en sandsynlighed for, at ingen tager sig af det potentielle problem. Risikoejerne skal have en position i virksomheden, der gør dem i stand til at udføre denne opgave, og træffe informerede beslutninger (fx om, hvordan risiciene skal håndteres). Hvor højt i hierarkiet risikoejeren skal findes, vil ofte afhænge af den konkrete risiko. Risici med høj konsekvens vil ofte skulle placeres højere oppe i hierarkiet end risici med lav konsekvens.

Processen med at udpege risikoejere er en del af risikoidentifikationen. I kan enten gøre det samtidig med, at de enkelte risici identificeres, så en ejer bliver tilknyttet øjeblikkeligt, eller I kan gennemgå listen over identificerede risici og tilknytte ejere efterfølgende. Uanset hvilken tilgang I vælger, vil resultatet af processen være, at I har en liste over identificerede risici med ejere tilknyttet.

[10] CVE står for Common Vulnerabilities and Exposures: https://cve.mitre.org/

[11] Tabel A.10 og A.11 i anneks A i ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks

[12] https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

EKSEMPLER PÅ IDENTIFIKATION AF RISICI

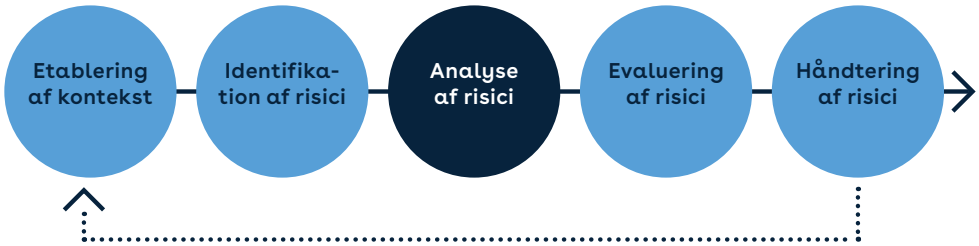
I **virksomhed A** vælger man at anvende en hændelsesbaseret tilgang. Værkstedsejeren beslutter at anvende sikkerdigital.dk's liste over trusler mod virksomheder[13] som udgangspunkt for deres liste. Efter gennemgangen af listen på sikkerdigital.dk gør bogholderen værkstedsejeren opmærksom på, at både CEO-fraud (hvor en angriber forsøger at udgive sig for at være en chef og beder bogholderen om at foretage en bankoverførsel) og fakturabedrageri er noget, der er blevet forsøgt på. Derfor er det en reel risiko, som virksomheden bør forholde sig til. Cyberspionage bliver dog ikke vurderet som værende et stort problem.

I **virksomhed B** vælger man i stedet en aktivbaseret tilgang. Under en række workshops identificerer produktejerne, servicechefer, regnskabschefen og salgschefen, hvilke systemer og data der er kritiske for deres ansvarsområder. Denne liste behandles derefter af produktdesignere/arkitekter, IT-afdeling og andre grupper med teknisk indsigt for at identificere potentielle angrebsscenarier. Som inspiration til arbejdet gennemgår en arbejdsgruppe trusselskataloger fra bl.a. ISO/IEC 27005 og NIST SP-800-30 og samler derved et skræddersyet trusselskatalog til virksomheden. De identificerede risici får derefter tilknyttet en relevant ejer, der som udgangspunkt er IT-chefen, hvis en risiko berører de administrative systemer som fx intranettet eller netværksinfrastrukturen, og en produktejer, hvis kun et enkelt produkt er berørt, fx en sårbarhed i et overvågningskamera. Ligesom under definitionen af konteksten bliver der taget referat af samtlige møder, så begrundelser for valg er dokumenteret. Vigtige beslutninger indføres i ledelsessystemet.

Et af virksomhedens aktiver er de data, som overvågningssystemerne sender ind til virksomheden. Dette aktiv giver anledning til en række potentielle risici, fx kan data lækkes af en ondsindet medarbejder, data kan blive manipuleret af en hacker, der har adgang til overvågningskameraet (eller den netværksforbindelse, som benyttes), ligesom en hacker i princippet også kunne hacke backend'en og derved lække data eller installere ransomware.

I **virksomhed C** vil det igen være samme tilgang som virksomhed A, hvor man anvender trusselskataloget fra sikkerdigital.dk. Særligt truslen fra DDoS-angreb (overbelastningsangreb) finder virksomheden særligt relevant. Derudover får gennemgangen af trusler virksomheden til at tænke over måden, de behandler persondata på.

[13] https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed



3.3 Analyse af risici

Når I har identificeret risici, er det næste skridt at analysere disse risici. Formålet med en risikoanalyse er at fastsætte en risikoværdi, ofte ved hjælp af sandsynlighed og konsekvens, og dermed beregne hvor store risiciene er.

I arbejdet med cyber- og informationssikkerhed anvender man begreberne fortrolighed, integritet og tilgængelighed i forhold til informationer. Fortrolighed handler om, at kun autoriserede personer skal have adgang til information og ingen andre. Ved tab af fortrolighed vil det betyde, at uønskede personer har adgang til informationen. Integritet handler om, at informationer er fuldstændige og korrekte. Ved tab af integritet vil det betyde, at informationer ikke er korrekte eller fuldstændige, som de burde være. Tilgængelighed handler om, at personer, som skal have adgang til information, også har adgangen. Ved tab af tilgængelighed vil det betyde, at autoriserede personer ikke kan tilgå de informationer, som de skal kunne tilgå. Tab af fortrolighed, integritet og fortrolighed er konsekvenser, man ser nærmere på i risikoanalysen.

Når I skal vurdere sandsynligheden, er det vigtigt at skelne mellem forsøg på angreb og at angreb faktisk sker. Fx bliver mange virksomheder udsat for forsøg på CEO-fraud, men kun et fåtal af forsøgene lykkes, da medarbejdere er opmærksomme på risikoen.

Det betyder, at I gerne må tage højde for eventuelle forebyggende foranstaltninger i forbindelse med vurderingen[14]; dog skal I huske at være konsekvente og bruge samme metode for alle risici.

Når I har forholdt jer til sandsynligheden og konsekvensen ved de potentielle trusler, som kan ramme jeres forretningskritiske processer og informationer, og dermed har analyseret jer frem til hvilke risici, I står overfor, kan I danne jer et billede af, hvor udsatte I er i forhold til de enkelte risici.

Hvis I arbejder med personoplysninger, er det vigtigt at have fokus på overholdelsen af persondataforordningen (GDPR). I den forbindelse kan det ved behandling af personoplysninger være nødvendigt, at I udarbejder en risikovurdering, hvor I udregner konsekvensen ved en hændelse for den eller de personer, hvis oplysninger det handler om, i stedet for fra jeres synspunkt. Dette kan standarden ISO/IEC 29134[15] hjælpe med. Der er også hjælp at hente i Datatilsynets vejledning "Vejledende tekst om risikovurdering", hvor der er et særskilt afsnit om risikovurdering set fra de registreredes perspektiv[16].

[14] Inden for risikovurdering bruger man ofte udtrykkene 'inherent risk' og 'residual risk' om risikoen før og efter sikkerhedsforanstaltninger. Den skelnen er vigtig, når man begynder at arbejde mere formelt med risikostyring.
[15] Se kort beskrivelse af ISO/IEC 29134 i anneks A.
[16] https://www.datatilsynet.dk/media/7697/vejledende-tekst-om-risikovurdering.pdf

EKSEMPLER PÅ ANALYSE AF RISICI

I **virksomhed A** gør bogholderen opmærksom på, at de i virksomheden jævnligt bliver udsat for forsøg på såkaldt CEO-fraud. Risikoen for CEO-fraud bliver derfor vurderet til at ske med 'middel' sandsynlighed, da de jævnligt bliver modtaget, men opdaget, da bogholderen fatter mistanke og derfor ikke reagerer på dem. Konsekvensen er ligeledes 'middel', da beløbene, der anmodes om, som regel er i omegnen af 50.000 kr.

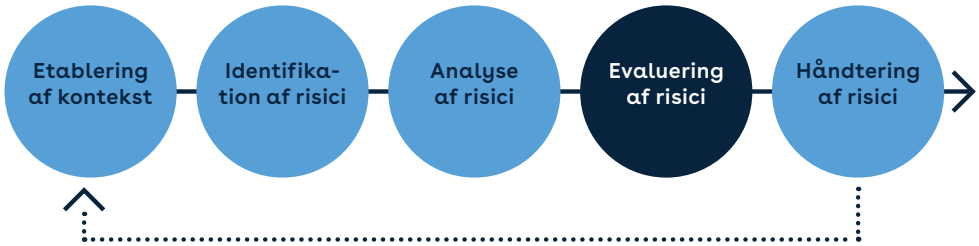
Virksomhed A analyserer også på risikoen for cyberspionage. Det står hurtigt klart, at virksomheden ikke ligger inde med forretningshemmeligheder af betydning, ligesom det i princippet kun er værkstedsejeren og betroede medarbejdere, som har adgang til IT-systemerne. Både konsekvens og sandsynlighed bliver derfor vurderet til 'lav'.

I forbindelse med risikoidentifikationen bliver **virksomhed B** opmærksom på, at det ikke bliver valideret, hvor data (videooptagelser) stammer fra, og at det derfor er muligt for en angriber at "overskrive" videoen fra et bestemt kamera. På en workshop, hvor tre teknikere samt produktejeren deltager, vurderes det, at angrebet forholdsvis nemt kan gennemføres, og det får derfor en sandsynlighed på 4 (svarende til ét angreb om ugen), med en konsekvens på 5 (firmaets jurist vurderer, at virksomheden kan blive stævnet for forholdsvis høje beløb i forbindelse med eventuelle indbrud hos kunderne).

En anden risiko er manglen på ekspertise i tilfælde af et cyberangreb. IT-afdelingen kan sagtens håndtere den almindelige drift, men IT-chefen mener ikke, at personalet vil være i stand til at håndtere de udfordringer, der vil opstå ved fx et ransomwareangreb. Det betyder, at det vil tage længere tid at komme op at køre igen, hvilket bliver vurderet til at kunne blive meget dyrt – dvs. konsekvens 5, selvom sandsynligheden for et angreb er forholdsvis lille; 2.

Virksomhed C er meget afhængige af deres webshop, idet alle salg foregår herigennem. Hvis webshoppen bliver utilgængelig i forbindelse med et DDoS-angreb, vurderer virksomheden, at det vil koste omkring 25.000 kr. om dagen i tabt omsætning. Samtidig har virksomheden ikke nogen foranstaltninger til forebyggelse af DDoS-angreb, og virksomheden vurderer derfor, at sandsynligheden for et angreb er høj, selvom de ikke ved, hvem der kunne finde på at angribe.

Som led i deres markedsføring indsamler virksomhed C en del persondata, som bliver analyseret af en tredjepart. Selvom et læk vurderes til at være usandsynligt, mener ejeren, at det måske kan være på kant med GDPR-lovgivningen. Ejeren forventer ikke, at det er noget, Datatilsynet vil reagere på (sandsynlighed: lav), ligesom ejeren heller ikke forventer en stor bøde, hvis virksomhedens praksis skulle vise sig at være ulovlig (konsekvens: lav).



3.4 Evaluering af risici

På baggrund af de tidligere trin har I nu identificeret og analyseret jer frem til nogle risici, der kan sammenholdes med jeres sikkerhedspolitikker og målsætninger, som I identificerede i forbindelse med etableringen af konteksten. Formålet med dette trin er, at I skal forholde jer til, om den enkelte risiko er en risiko, I kan og vil leve med i forhold til forretningens målsætninger og politikker, eller om det er noget, I skal forsøge at ændre på. I den forbindelse er det vigtigt, at ledelsen er med til at beslutte risikovilligheden. I denne fase handler det således om at prioritere mellem alle de identificerede risici og træffe beslutninger om, hvorvidt alle risici skal håndteres, eller om der er risici, der er mindre vigtige at håndtere. Der vil nok ikke som det første være behov for at se på de risici, hvor både sandsynligheden og konsekvensen er meget små.

EKSEMPLER PÅ EVALUERING AF RISICI

I **virksomhed A** viste risikoanalysen, at risikoen for CEO-fraud er 'middel/middel', dvs. at risikoen er i kategorien af risici, der løbende skal adresseres. Risikoen for cyberspionage er 'lav/lav' og derfor ikke noget, der umiddelbart skal reageres på. Se tabel A4.

Tabel A4

KONSEKVENS	SANDSYNLIGHED: Lav	Middel	Høj
Lav	**Lav/Lav**	Middel/Lav	Høj/Lav
Middel	Lav/Middel	**Middel/Middel**	Høj/Middel
Høj	Lav/Høj	Middel/Høj	Høj/Høj

Cyber-spionage

CEO-fraud

I **virksomhed B** viste risikoanalysen, at risikoen ved den manglende validering, er 4 x 5, dvs. en risikoværdi på 20, der skal reageres på af direktionen. Risikoen relateret til manglende ekspertise i forbindelse med et cyberangreb bliver vurderet til 2 x 5, dvs. 10, og de vil drøfte det med en afdelingsleder. Se tabel B4.

Tabel B4

KONSEKVENS \ SANDSYNLIGHED	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	**10**	15	**20**	25

Manglende ekspertise ifm. et cyberangreb

Manglende validering af hvor data stammer fra

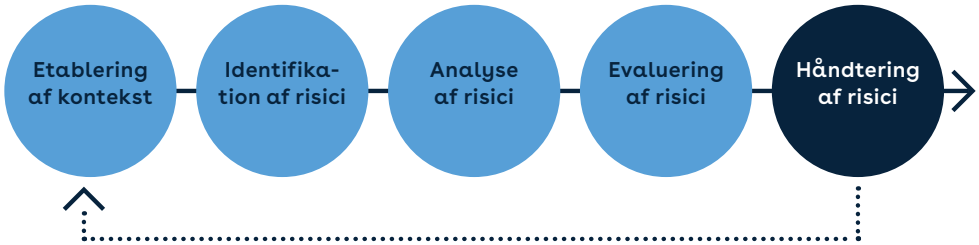
I **virksomhed C** viste risikoanalysen, at risikoen for et DDoS-angreb er 'høj/middel', hvilket dog afhænger af, hvor længe webshoppen er utilgængelig. Brugen af persondata bliver vurderet til at udgøre en 'lav/lav' risiko. Se tabel C4.

Tabel C4

KONSEKVENS \ SANDSYNLIGHED	Lav	Middel	Høj
Lav	**Lav/Lav**	Middel/Lav	Høj/Lav
Middel	Lav/Middel	Middel/Middel	**Høj/Middel**
Høj	Lav/Høj	Middel/Høj	Høj/Høj

Brug af persondata

DDoS-angreb



3.5 Håndtering af risici

Når I har udregnet risici for de relevante, potentielle hændelser og har besluttet jer for et niveau af risikoaccept, er det næste skridt i processen at håndtere de identificerede risici. Her er der igen brug for at prioritere, og det giver derfor god mening at kigge i retning af en cost-benefit-analyse; er omkostningerne ved at undgå risici større end hændelsen, I ønsker at forhindre?

Ved risikohåndtering opereres der med fire valgmuligheder for at håndtere en risiko:

1. **Acceptere risikoen.** Dette er en mulighed, hvis risikoen falder ind under, hvad I vil leve med i forhold til jeres politikker og kriterier for risikoaccept. I kan også vælge at acceptere en risiko, hvis omkostningerne ved at adressere risikoen overstiger risikoens potentielle omkostninger. Der kan også være tale om en risiko, som det ikke er muligt for jer at gøre noget ved (fx naturkatastrofer eller at have aktiviteter i et ustabilt land). Risikoen vil fortsat være der, men sandsynligheden er forholdsvis lav, og I adresserer den først i det øjeblik, den bliver til virkelighed.
2. **Undgå risikoen.** Risikoen undgås ved at stoppe eller ændre den aktivitet, der forårsager risikoen. I kan vælge at undgå risikoen, hvis den er for stor, og der ikke kan findes nogle passende handlinger til at nedbringe den. Et eksempel er at flytte fx serverrum op fra kælderen og dermed undgå risikoen for oversvømmelse.
3. **Flytte/dele risikoen.** Det er en mulighed at flytte risikoen ved fx at outsource en aktivitet til andre, som er bedre i stand til at varetage opgaven med en mindre risiko (fx ved at vælge en cloudløsning til opbevaring af informationer). En anden mulighed er at tegne en forsikring, som nedbringer konsekvensen, hvis uheldet er ude. Det skal dog bemærkes, at det at flytte risikoen kan skabe en ny risiko[17].
4. **Forøge/minimere risikoen.** I kan også vælge at igangsætte nogle aktiviteter eller foranstaltninger, som er med til at mindske sandsynligheden eller konsekvensen og dermed nedbringer risikoen til et niveau, som I kan leve med. I kan fx anvende krypterede mails eller to-faktor-autentifikation. I de tilfælde hvor man vælger at forøge en risiko, vil det oftest være ud fra et forretningsmæssigt synspunkt, hvor man vurderer, at den potentielle gevinst er risikoen værd. Det kan være i forbindelse med lancering af et nyt produkt eller ved at gå ind på et nyt marked.

[17] Det kan fx være svært at udregne, om en forsikring vil dække organisationens tab af informationer tilstrækkeligt. Og selvom man outsourcer aktiviteter til andre, har man stadig selv ansvaret. Rådet for Digital Sikkerhed, Dansk Industri og Forsikring & Pension har udarbejdet en vejledning til smv'er om cyberforsikringer for at give et overblik over, hvad man skal være opmærksom på, hvis man vil købe en cyberforsikring: https://www.digitalsikkerhed.dk/vejledning-til-smv-om-cyberforsikringer/

I kan som virksomhed vælge mellem forskellige foranstaltninger/aktiviteter, der kan bidrage til at nedbringe risici. Disse aktiviteter kan fx være forebyggende, opdagende eller korrigerende. Hvis I ønsker at nedbringe sandsynligheden for, at en hændelse sker, er det ofte forebyggende tiltag, som fx at slå to-faktor-autentifikation til, som er gode at benytte. Er det konsekvensen, I vil nedbringe, er det ofte opdagende og korrigerende tiltag, I skal fokusere på at implementere. Det kan fx være overvågning eller backup.

Standarden ISO/IEC 27002[18] indeholder en lang række sikkerhedsforanstaltninger, der kan anvendes som inspiration til at forebygge og håndtere risici. Ligeledes indeholder sikkerdigital.dk og andre best practices[19] også metoder, der kan bruges i risikohåndteringsfasen.

EKSEMPLER PÅ HÅNDTERING AF RISICI

I **virksomhed A** har ejeren og bogholderen en dialog om, hvordan risikoen for CEO-fraud bedst adresseres. De beslutter, at ved overførsler større end 1.000 kr., skal bogholderen altid have bekræftelse enten telefonisk eller fysisk. Derved har de implementeret en forebyggende foranstaltning, der sænker risikoens sandsynlighed, og derved sænker den samlede risiko til et acceptabelt niveau.

Da risikoen for cyberspionage blev vurderet som lav, vælger ejeren at acceptere risikoen og ikke gøre yderligere ved den.

I **virksomhed B** besluttes det, at der øjeblikkeligt skal igangsættes en mekanisme til at foretage valideringen af datas oprindelse. Al andet udviklingsarbejde bliver derfor sat i bero, indtil det er på plads. Dette vil reducere sandsynligheden for angrebet til 1 (og den samlede risiko til 5). Desværre har virksomheden ikke mulighed for at rulle ændringen ud til en række allerede solgte, ældre systemer. Dette informeres den administrerende direktør om, hvorefter det tages op til diskussion på et bestyrelsesmøde, så de kan beslutte, om den resterende risiko skal accepteres, eller om produkterne skal tilbagekaldes.

For at reducere konsekvensen ved de manglende ressourcer i tilfælde af et cyberangreb har virksomhed B besluttet sig for at tegne en forsikring, der kan hjælpe med ressourcer i tilfælde af et nedbrud og samtidig kan dække noget af det driftstab, der kan forekomme i den forbindelse.

I **virksomhed C** blev der identificeret en risiko omkring læk af de persondata, som indsamles i forbindelse med webshoppen. Nogle data er nødvendige i forbindelse med fakturering og ordrehåndtering, men en række data bliver sendt til tredjeparter i forbindelse med kundeanalyse. Da ejeren ikke kan se en tydelig værdi af de analyser, besluttes det, at virksomheden skal standse indsamlingen af de unødvendige data og derved helt undgå risikoen (selvom den er lav) for et datalæk fra tredjeparter.

For at nedbringe risikoen for et DDoS-angreb kontakter virksomheden sin IT-leverandør og tilkøber en service, der automatisk opskalerer serverkapaciteten i tilfælde af DDoS-angreb. På den måde bliver sandsynligheden for et angreb kraftigt reduceret.

[18] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
[19] Se anneks A for inspiration

Opsamling

Som gennemgået her i guiden kan en risikostyringsproces være et gavnligt redskab for jer, der gerne vil adressere jeres risici og sætte fokus på cyber- og informationssikkerhed. Risikostyring er ikke en enkeltstående opgave, men en løbende proces, der hele tiden skal vedligeholdes. Risikostyringsprocessen bør samtidig være fleksibel, da jeres risikobillede hurtigt kan ændre sig.

En organisation er ikke stærkere end det svageste led, og derfor er det afgørende, at hele virksomheden forstår vigtigheden af at adressere og håndtere risici, og at alle i virksomheden tager et fælles ansvar. Derfor skal cyber- og informationssikkerhedsindsatsen kommunikeres klart ud til hele virksomheden.

Da risikostyring er et kritisk område, er det afgørende, at ledelsen er involveret og dedikerer de nødvendige ressourcer til både udformning og implementering af processen såvel som de efterfølgende foranstaltninger. På samme måde er det vigtigt, at de, der er ansvarlige for risikostyring, har mandat fra ledelsen til at gennemføre ændringerne.

Forhåbentligt har denne guide vist, at en risikostyringsproces ikke er en uoverkommelig opgave, men en proces, der kan sættes i værk med både få ressourcer og begrænset tid.

Anneks A: Præsentation af standarder og øvrige metoder til risikostyring

I dette afsnit præsenteres nogle af de mest anvendte og gennemtestede risikostyringsmetoder. Nogle af disse er internationalt anerkendte standarder, mens andre er mere nationalt funderede værktøjer, der kan være en hjælp til at komme i gang med risikostyring. I dette anneks vil der være en kort gennemgang af følgende standarder, rammeværk og redskaber:

- ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks
- ISO/IEC 29134 Information technology – Security techniques – Guidelines for privacy impact assessment
- OCTAVE Allegro
- NIST SP 800-30, SP 800-37 og SP 800-39
- STRIDE/DREAD
- OWASP Risk Rating Methodology
- Erhvervsstyrelsens IT-risikovurderingsværktøj
- Erhvervsstyrelsens Sikkerhedstjek

ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks
ISO/IEC 27005 er en vejledning i risikostyring og giver inspiration til, hvordan man som organisation kan vurdere og håndtere risici vedrørende organisationens informationer ud fra en vurdering af sandsynligheden for, at en hændelse sker, sammenstillet med den konsekvens, som hændelsen har for organisationen.

ISO/IEC 27005 indeholder en vejledning i, hvordan man kan udarbejde en risikovurdering og dermed få et overblik over organisationens trusler, sårbarheder, og hvordan risici kan håndteres ud fra organisationens risikovillighed. Standarden giver redskaber til at prioritere risici og kan dermed bidrage til at sikre det optimale niveau af foranstaltninger i en organisation i forhold til værdien af den information, som skal beskyttes. Standarden stiller skarpt på konsekvens og sandsynlighed og indeholder information om kriteriefastsættelser og eksempler på risikoscenarier.

ISO/IEC 27005 opstiller en risikostyringsproces for informationssikkerhed med udgangspunkt i kravene fra standarden ISO/IEC 27001 (ISO/IEC 27001 er en ledelsesstandard, der stiller de overordnede krav til en systematisk tilgang til informationssikkerhed). ISO/IEC 27005 kan dog sagtens læses og anvendes selvstændigt, men dens store styrke i forhold til andre risikoværktøjer er dens integration med ISO/IEC 27001.

ISO/IEC 27005 er relevant for alle, der gerne vil arbejde med risikostyring uanset om man 'blot' ønsker inspiration til sit arbejde med risikostyring, eller om man ønsker at opbygge et helt system for processerne. ISO/IEC 27005 er blevet opdateret i 2022, og i den forbindelse har der netop været fokus på at gøre standarden så brugervenlig som muligt, så man nemt forstår indholdet, selvom man ikke tidligere har arbejdet med risikostyring eller standarder.

Denne guide er opbygget med inspiration fra ISO/IEC 27005 og suppleret med konkrete eksempler på, hvordan standardens principper kan anvendes.

ISO/IEC 29134 Information technology – Security techniques – Guidelines for privacy impact assessment
Hvis man arbejder med persondata, kan det være relevant at udføre en 'privacy impact assesment' (PIA). Den internationale standard ISO/IEC 29134 beskriver, hvordan en sådan kan udføres og minder meget om processen i ISO/IEC 27005. De største forskelle ligger primært i etablering af kontekst og hvilke interessenter, der skal underrettes, samt at man i forbindelse med konsekvensanalysen skal tage udgangspunkt i den persons interesser, som data omhandler, i stedet for organisationens interesser.

OCTAVE Allegro
OCTAVE Allegro er en metode til risikovurdering med fokus på data og information. Den oprindelige OCTAVE-metode var et generelt risikovurderingsrammeværk målrettet større virksomheder med over 300 ansatte. Den

oprindelige OCTAVE-metode er sidenhen, i form af Allegro, blevet forenklet lidt og blevet målrettet 'informationsaktiver', og hvor de anvendes. Metoden har mange lighedspunkter med ISO/IEC 27005. Først etableres diverse kriterier (fx hvad betyder 'høj konsekvens'?), hvorefter informationsaktiverne identificeres og beskrives. Efter informationsaktiverne er beskrevet, kigges der på trusler mod aktiverne, og en række trusselsscenarier beskrives, og herefter laves den egentlige risikoanalyse. Metoden afsluttes med en fase omkring nedbringelsen af risici, hvor man vælger, hvordan de identificerede risici skal håndteres.

Metoden adskiller sig primært fra ISO/IEC 27005 ved udelukkende at fokusere på selve risikoanalysen. Metoden indeholder derfor ikke elementer ud over det, fx hvem der skal orienteres eller godkende i de forskellige trin undervejs. Metoden er samtidig mere specifik i forhold til ISO/IEC 27005 og indeholder fx tre faste kategorier for konsekvens. At metoden er så specifik, kan gøre den en smule lettere at anvende direkte, men betyder samtidig, at brugeren skal tage stilling til emner, som måske ikke er relevante i den konkrete case.

NIST SP 800-30, SP 800-37 og SP 800-39
NIST er det amerikanske institut for standarder og teknologi, der udgiver en række standarder og lignende dokumenter vedrørende blandt andet IT-sikkerhed (SP 800-serien). NIST-dokumenter er meget udbredt i USA, hvor mange regulativer læner sig op ad disse. I Danmark og resten af Europa er brugen af NIST-dokumenter ikke så udbredt, udover i nogle tekniske nicher/brancher, hvor det kan være relevant at overholde amerikansk lovgivning. Det kan fx være, hvis man skal levere til de amerikanske myndigheder eller forsvar. NIST SP 800-30, 800-37 og 800-39 arbejder alle med emner inden for risikostyring.

SP 800-30 omhandler selve risikoanalysen, mens SP 800-37 og SP 800-39 handler om de omkringliggende emner, dvs. selve styringen. Selve den beskrevne risikoanalyse i SP 800-30 tager udgangspunkt i trusler mod organisationen og kigger derefter på sandsynligheden for, at de sker, og deres konsekvens. Analysen kommer derfor igennem de samme faser som ISO/IEC 27005 og OCTAVE Allegro, om end rækkefølgen ikke er den samme.

Da NIST-publikationerne udgør et komplet rammeværk (som også omhandler mange andre emner end risikostyring), behandles også en del af de samme emner som i ISO/IEC 27000-serien (standarder for informationssikkerhed). Dele af standarderne (særligt SP 800-37 og 800-39) overlapper derfor med indholdet af ISO/IEC 27001.

STRIDE/DREAD
STRIDE og DREAD er ikke egentlige risikovurderingsmodeller, men bliver ofte anvendt i forbindelse med risikovurdering. Begge modeller er tiltænkt mere eller mindre uformelle workshops/brainstorms.

STRIDE er et akronym for
- **S**poofing – Er det muligt at udgive sig for at være en anden?
- **T**ampering – Er det muligt at foretage en (uautoriseret) ændring af data?
- **R**epudiation – Er det muligt for en bruger at benægte, at vedkommende har udført en handling?
- **I**nformation disclosure – Er der fare for, at fortrolig data bliver lækket?
- **D**enial of service – Er der fare for, at funktionalitet kan standses?
- **E**levation of privilege – Er det muligt for en bruger at foretage ikke-autoriserede handlinger?

STRIDE beskriver forskellige kategorier af trusler og anvendes som regel som en checkliste, man kan gennemgå for de enkelte komponenter eller interfaces i et IT-system. Ved at anvende checklisten sikrer man, at man kommer igennem de gængse typer af trusler for et system.

DREAD er et akronym for
- **D**amage – Hvor alvorlig er truslen?
- **R**eproducibility – Hvor let er det at gentage truslen?
- **E**xploitability – Hvor krævende er det at udføre truslen?
- **A**ffected users – Hvor mange brugere vil blive berørt af truslen?
- **D**iscoverability – Hvor let er det at opdage truslen?

DREAD kan anvendes som et alternativ til den tidligere beskrevne vurderingsmodel (hvor man kigger på konsekvens og sandsynlighed) til at vurdere trusler og kan anvendes som en form for risikoprioritering. Hver kategori gives en score på mellem 0 og 10, hvorefter kategorierne opsummeres og en samlet score opnås. DREAD er forholdsvis enkel at arbejde med, men har den svaghed, at de mange kategorier giver relativt ens vurderinger på forskellige systemer. Fx vil et system, der bruges til kritiske data, maksimalt kunne score 10 point (20 %) højere end et identisk system med trivielle data. Ved at multiplicere kategorierne kan dette dog afhjælpes.

Begge modeller er væsentligt mere teknisk orienteret end risikostyrings-/risikovurderingsværktøjerne fra ISO/IEC 27005 og OCTAVE Allegro og kan anvendes af arkitekter, programmører og systemadministratorer uden involvering af ledelsen. Samtidig er de forholdsvis enkle at arbejde med og kan derfor hurtigt implementeres som en del af virksomhedens udviklingsprocesser.

OWASP Risk Rating Methodology
OWASP er en organisation, der publicerer en lang række best practices inden for IT-sikkerhed og har også udarbejdet guides vedrørende risikovurdering, bl.a. OWASP Risk Rating Methodology.

OWASP Risk Rating Methodology er en forholdsvis enkel og uformel model til risikoanalyse. Den består primært af en beskrivelse af, hvordan man kan beregne sandsynligheden for, at en hændelse sker, og hvor stor konsekvensen af hændelsen er. Dette gøres ved at nedbryde hændelserne til otte underemner, som er lettere at beregne sandsynlighed og konsekvens for.
Metoden er primært tiltænkt teknikere og giver ikke megen vejledning i, hvordan de identificerede risici efterfølgende skal håndteres. Metoden antager samtidig, at de udførende personer ikke nødvendigvis har megen forretningsmæssig indsigt, og det er derfor fuldt acceptabelt at udelade dele af konsekvensanalysen, hvis ikke personen har den nødvendige viden.

Erhvervsstyrelsens IT-risikovurderingsværktøj
Erhvervsstyrelsen lancerede i 2021 et IT-risikovurderingsværktøj, der skal hjælpe danske smv'er med at kortlægge deres sikkerhedsrisici. Risikovurderingsværktøjet lister en række risikoscenarier, som er relevante for virksomheder at forholde sig til. Værktøjet er interaktivt og for hvert risikoscenarie bliver man bedt om at forholde sig til sandsynligheden for, at risikoscenariet sker og hvad konsekvensen i så fald vil være for ens forretning. Både sandsynlighed og konsekvens vurderes ud fra en simpel skala fra 1-5.

Risikovurderingsværktøjet fokuserer særligt på IT-systemer og dækker følgende områder:
- Enheder
- Applikationer og tjenester
- Brugere
- Netværk
- Data.

Når alle risikoscenarier er gennemgået, vil resultatet være en grundlæggende risikovurdering, man efterfølgende kan downloade som regneark. Resultatet indeholder også en vejledning til, hvordan virksomheden kan håndtere de forskellige risikoscenarier.

Sikkerhedstjekket
Erhvervsstyrelsen har ligeledes lanceret Sikkerhedstjekket, der kan hjælpe virksomheder med at undersøge, om niveauet af deres IT-sikkerhed er godt nok. Sikkerhedstjekket er med til at skabe et overblik over virksomhedens svage punkter og sårbarheder. Ved at svare på en række spørgsmål knyttet til IT-sikkerhed genereres der et resultat med konkrete anbefalinger og værktøjer til, hvordan man kan styrke sikkerheden i sin virksomhed.

I Sikkerhedstjekket gennemgås følgende fem temaer:
- Ledelse og risikohåndtering
- Sikkerhedsprocedurer
- Medarbejdere
- Tekniske sikkerhedsløsninger
- Samarbejdspartnere.

Anneks B: Virksomhedseksemplerne

I dette anneks findes en sammenskrivning af virksomhedseksemplerne fra guiden.

VIRKSOMHED A
Autoværkstedet

Mindre autoværksted
Mindre grad af digitalisering. Ingen fortrolige/personfølsomme data. Har private kunder og forskellige leverandører af materialer. Dog ikke kunder med særlige krav. Relativt få brugere.

Etablering af kontekst
Virksomheden vurderer, at størstedelen af kunderne kommer ind fra gaden, og kun ca. 30 % laver en forudgående tidsbestilling på virksomhedens hjemmeside. Værkstedet bruger primært IT til regnskab og tidsbestilling, men har også et par computere med specialprogrammer, som bruges af mekanikerne. Disse computere er dog ikke internetopkoblede. Værkstedet behandler ikke følsomme (person-)data, udover kontaktinformation til kunder, lønsedler og lignende. Der skal derfor ikke tages hensyn til følsomme persondata. Den primære bekymring er derfor tab af omsætning, idet læk af data ikke vurderes som særlig relevant og virksomheden ikke er underlagt særlig lovgivning som fx NIS-direktivet.

Da virksomheden er forholdsvis lille, vil etablering af konteksten kunne udføres af ejeren af værkstedet sammen med værkstedets bogholder. Det kan foregå som et uformelt møde på en halv time, hvor strategi og mission italesættes, og hvor interessentlandskabet kortlægges. Deltagerne behøver ikke medbringe noget særligt forarbejde udover deres baggrundsviden. Selve processen kan dokumenteres som et referat af beslutningerne.

På baggrund af ovenstående og virksomhedens størrelse vælger virksomheden, at risikovurderingen skal foregå med tre niveauer for konsekvens (lav, middel og høj) afhængigt af størrelsen på det forventede tab (0-25.000 kr., 25.001-200.000 kr. og 200.001+ kr.): Se tabel A1.

Sandsynlighed opdeles ligeledes i tre niveauer (lav, middel og høj) afhængigt af intervallet; ('forventer ikke, at det kan ske', 'kan ske inden for 2 år' og 'forventer, det sker mindst årligt'): Se tabel A2.

Tabel A1

KONSEKVENS	Lav	Middel	Høj
BELØB	0-25.000 kr.	25.001-200.000 kr.	200.001+ kr.

Tabel A2

SANDSYNLIGHED	Lav	Middel	Høj
INTERVAL	'Forventer ikke, at det kan ske'	'Kan ske inden for 2 år'	'Forventer, det sker mindst årligt'

Risikovurderingen gentages en gang om året og er relativt uformel. I forbindelse med vurderingen sparres der med IT-leverandøren og revisoren. Da ejeren af værkstedet har al kontakt med IT-leverandøren, er det samtidig ejeren, der er risikoejer for alle risici. Det besluttes, at alle høj/høj (rød) risici skal udbedres hurtigst muligt, mens lav/middel (grøn) risici accepteres. Middel/middel og middel/høj (gul) risici skal vurderes løbende.Se tabel A3.

Identifikation af risici
I virksomhed A vælger man at anvende en hændelsesbaseret tilgang. Værkstedsejeren beslutter at anvende sikkerdigital.dk's liste over trusler mod virksomheder som udgangspunkt for deres liste. Efter gennemgangen af listen på sikkerdigital.dk gør bogholderen værkstedsejeren opmærksom på, at både CEO-fraud (hvor en angriber forsøger at udgive sig for at være en chef og beder bogholderen om at foretage en bankoverførsel) og fakturabedrageri er noget, der er blevet forsøgt på. Derfor er det en reel risiko, som virksomheden bør forholde sig til. Cyberspionage bliver dog ikke vurderet som værende et stort problem.

Analyse af risici
I virksomhed A gør bogholderen opmærksom på, at de i virksomheden jævnligt bliver udsat for forsøg på såkaldt CEO-fraud. Risikoen for CEO-fraud bliver derfor vurderet til at ske med 'middel' sandsynlighed, da de jævnligt bliver modtaget, men opdaget, da bogholderen fatter mistanke og derfor ikke reagerer på dem. Konsekvensen er ligeledes 'middel', da beløbene, der anmodes om, som regel er i omegnen af 50.000 kr.

Virksomhed A analyserer også på risikoen for cyberspionage. Det står hurtigt klart, at virksomheden ikke ligger inde med forretningshemmeligheder af betydning, ligesom det i princippet kun er værkstedsejeren og betroede medarbejdere, som har adgang til IT-systemerne. Både konsekvens og sandsynlighed bliver derfor vurderet til 'lav'.

Evaluering af risici
Risikoen for CEO-fraud er 'middel/middel', dvs. at risikoen er i kategorien af risici, der løbende skal adresseres. Risikoen for cyberspionage er 'lav/lav' og derfor ikke noget, der umiddelbart skal reageres på. Se tabel A4.

Håndtering af risici
I virksomhed A har ejeren og bogholderen en dialog om, hvordan risikoen for CEO-fraud bedst adresseres. De beslutter, at ved overførsler større end 1.000 kr., skal bogholderen altid have bekræftelse enten telefonisk eller fysisk. Derved har de implementeret en forebyggende foranstaltning, der sænker risikoens sandsynlighed, og derved sænker den samlede risiko til et acceptabelt niveau.

Da risikoen for cyberspionage blev vurderet som lav, vælger ejeren at acceptere risikoen og ikke gøre yderligere ved den.

Tabel A3

KONSEKVENS	SANDSYNLIGHED: Lav	Middel	Høj
Lav	Lav/Lav	Middel/Lav	Høj/Lav
Middel	Lav/Middel	Middel/Middel	Høj/Middel
Høj	Lav/Høj	Middel/Høj	Høj/Høj

Tabel A4

KONSEKVENS	SANDSYNLIGHED: Lav	Middel	Høj
Lav	**Lav/Lav**	Middel/Lav	Høj/Lav
Middel	Lav/Middel	**Middel/Middel**	Høj/Middel
Høj	Lav/Høj	Middel/Høj	Høj/Høj

Cyber-spionage

CEO-fraud

VIRKSOMHED B
Produktionsvirksomheden

Mellemstor virksomhed
(omkring 85 ansatte), der producerer og installerer videoovervågningssystemer. Høj grad af digitalisering. Stor mængde fortrolige data. Stor snitflade med mange brugere; kunder, samarbejdspartnere, leverandører mm. Leverer til kritisk infrastruktur.

Etablering af kontekst
IT bruges til regnskab, projektstyring og en række andre administrative funktioner. Det anvendes derudover også i forbindelse med installation af løsninger hos kunder. Virksomhedens løsninger har en funktionalitet, der løbende sender vedligeholdelsesdata hjem til virksomheden, ligesom virksomheden har mulighed for at koble sig på løsninger via internettet for at foretage fjernsupport.

Virksomhedens kunder er primært private hjem, men den har også en række produkter målrettet virksomheder og større organisationer. På grund af ovenstående skal der i sikkerhedsarbejdet tages højde for, at der kan forekomme persondata i virksomhedens systemer. Samtidig kræver nogle af de større kunder, at der er styr på informationssikkerheden og ønsker dokumentation herfor.

For at sikre en høj grad af dokumentation bliver alle beslutninger dokumenteret og gemt i virksomhedens ledelsessystem baseret på standarden ISO/IEC 27001. Beslutningerne inkluderer en liste over interessenter (både interne og eksterne), der skal inddrages i processen, krav, der skal leves op til (GDPR og ISO/IEC 27001), samt hvor ofte risikovurderingsprocessen gentages, af hvilke dele af virksomheden og af hvem. Det besluttes at arbejde med fem niveauer af konsekvens (forventede tab: 0-50.000 kr., 50.001-125.000 kr., 125.001-500.000 kr., 500.001-2.500.000 kr. og 2.500.001+ kr.): Se tabel B1.

Og på samme måde fem niveauer for sandsynlighed (dagligt, ugentligt, kvartalsvist, årligt, 10-års hændelse): Se tabel B2.

Tabel B1

KONSEKVENS	1	2	3	4	5
BELØB	0-50.000 kr.	50.001-125.000 kr.	125.001-500.000 kr.	500.001-2.500.000 kr.	2.500.001+ kr.

Tabel B2

SANDSYNLIGHED	1	2	3	4	5
INTERVAL	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt

Niveauerne skal dog justeres løbende, når virksomheden har fået mere erfaring med processen. Risiko beregnes som produktet af konsekvensscore x sandsynlighed og kan derfor ligge på mellem 1 og 25. Se tabel B3.

Hændelser med risiko på under 10 accepteres (grøn), alt derover skal så vidt muligt nedbringes. Dog kan produktejer acceptere risici på op til og med 16 (gul), mens højere risici (rød) skal accepteres på direktionsniveau.

Identifikation af risici
I virksomhed B vælger man i stedet en aktivbaseret tilgang. Under en række workshops identificerer produktejerne, servicechefer, regnskabschefen og salgschefen, hvilke systemer og data der er kritiske for deres ansvarsområder. Denne liste behandles derefter af produktdesignere/arkitekter, ITafdeling og andre grupper med teknisk indsigt for at identificere potentielle angrebsscenarier. Som inspiration til arbejdet gennemgår en arbejdsgruppe trusselskataloger fra bl.a. ISO/IEC 27005 og NIST SP-800-30 og samler derved et skræddersyet trusselskatalog til virksomheden. De identificerede risici får derefter tilknyttet en relevant ejer, der som udgangspunkt er IT-chefen, hvis en risiko berører de administrative systemer som fx intranettet eller netværksinfrastrukturen, og en produktejer, hvis kun et enkelt produkt er berørt, fx en sårbarhed i et overvågningskamera. Ligesom under definitionen af konteksten bliver der taget referat af samtlige møder, så begrundelser for valg er dokumenteret. Vigtige beslutninger indføres i ledelsessystemet.

Et af virksomhedens aktiver er de data, som overvågningssystemerne sender ind til virksomheden. Dette aktiv giver anledning til en række potentielle risici, fx kan data lækkes af en ondsindet medarbejder, data kan blive manipuleret af en hacker, der har adgang til overvågningskameraet (eller den netværksforbindelse, som benyttes), ligesom en hacker i princippet også kunne hacke backend'en og derved lække data eller installere ransomware.

Analyse af risici
I forbindelse med risikoidentifikationen bliver virksomhed B opmærksom på, at det ikke bliver valideret, hvor data (videooptagelser) stammer fra, og at det derfor er muligt for en angriber at "overskrive" videoen fra et bestemt kamera. På en workshop, hvor tre teknikere samt produktejeren deltager, vurderes det, at angrebet forholdsvis nemt kan gennemføres, og det får derfor en sandsynlighed på 4 (svarende til ét angreb om ugen), med en konsekvens på 5 (firmaets jurist vurderer, at virksomheden kan blive stævnet for forholdsvis høje beløb i forbindelse med eventuelle indbrud hos kunderne).

En anden risiko er manglen på ekspertise i tilfælde af et cyberangreb. IT-afdelingen kan sagtens håndtere den almindelige drift,

Tabel B3

KONSEKVENS	SANDSYNLIGHED				
	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	10	15	20	25

men IT-chefen mener ikke, at personalet vil være i stand til at håndtere de udfordringer, der vil opstå ved fx et ransomwareangreb. Det betyder, at det vil tage længere tid at komme op at køre igen, hvilket bliver vurderet til at kunne blive meget dyrt – dvs. konsekvens 5, selvom sandsynligheden for et angreb er forholdsvis lille; 2.

Evaluering af risici
I virksomhed B viste risikoanalysen, at risikoen ved den manglende validering er 4 x 5, dvs. en risikoværdi på 20, der skal reageres på af direktionen. Risikoen relateret til manglende ekspertise i forbindelse med et cyberangreb bliver vurderet til 2 x 5, dvs. 10, og de vil drøfte det med en afdelingsleder. Se tabel B4.

Håndtering af risici
I virksomhed B besluttes det, at der øjeblikkeligt skal igangsættes en mekanisme til at foretage valideringen af datas oprindelse. Al andet udviklingsarbejde bliver derfor sat i bero, indtil det er på plads. Dette vil reducere sandsynligheden for angrebet til 1 (og den samlede risiko til 5). Desværre har virksomheden ikke mulighed for at rulle ændringen ud til en række allerede solgte, ældre systemer. Dette informeres den administrerende direktør om, hvorefter det tages op til diskussion på et bestyrelsesmøde, så de kan beslutte, om den resterende risiko skal accepteres, eller om produkterne skal tilbagekaldes.

For at reducere konsekvensen ved de manglende ressourcer i tilfælde af et cyberangreb har virksomhed B besluttet sig for at tegne en forsikring, der kan hjælpe med ressourcer i tilfælde af et nedbrud og samtidig kan dække noget af det driftstab, der kan forekomme i den forbindelse.

Tabel B4

KONSEKVENS	SANDSYNLIGHED				
	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	**10**	15	**20**	25

Manglende ekspertise ifm. et cyberangreb

Manglende validering af hvor data stammer fra

VIRKSOMHED C
Webshoppen

Lille virksomhed
(fire ansatte), der importerer vin. Høj grad af digitalisering (100 % webshop). Mange brugere af webshoppen. Nogen grad af fortrolige data. Benytter sig i høj grad af leverandører i forhold til IT-driften.

Etablering af kontekst

Virksomhed C startede som en enkeltmandsvirksomhed, der importerer vin, men er siden vokset og beskæftiger nu fire personer. Virksomheden er mere eller mindre 100 % baseret på virksomhedens webshop, hvor alle ordrer bliver modtaget. Da webshoppen er omdrejningspunktet for virksomheden, indsamles der så meget data som muligt med henblik på marketing og viden om kunderne. Disse data er persondata og derfor underlagt GDPR-lovgivning. De ansatte i virksomheden er ikke specielt IT-kyndige, og al IT er derfor cloudbaserede løsninger, ligesom et eksternt webbureau har ansvaret for driften af webshoppen.

Selve kontekstbeskrivelsen for virksomhed C minder meget om beskrivelsen fra virksomhed A. Dette skyldes, at virksomhederne anvender samme (uformelle) tilgang til processen med tre niveauer for konsekvens og sandsynlighed (se tabel C1 og C2). På samme måde besluttes det, at alle 'høj/høj' (rød) risici skal udbedres hurtigst muligt, mens 'lav/middel' (grøn) risici accepteres. 'Middel/middel' og 'middel/høj' (gul) risici skal vurderes løbende. Se tabel C3.

Virksomhed C adskiller sig dog fra virksomhed A ved at have et større fokus på GDPR og flere dele udliciteret til leverandører, hvilket er relevant i de efterfølgende trin.

Virksomhed C adskiller sig dog fra virksomhed A ved at have et større fokus på GDPR og flere dele udliciteret til leverandører, hvilket er relevant i de efterfølgende trin.

Identifikation af risici

I virksomhed C vil det igen være samme tilgang som virksomhed A, hvor man anvender trusselskataloget fra sikkerdigital.dk. Særligt truslen fra DDoS-angreb (overbelastningsangreb) finder virksomheden særligt relevant. Derudover får gennemgangen af trusler virksomheden til at tænke over måden, de behandler persondata på.

Tabel C1

KONSEKVENS	Lav	Middel	Høj
BELØB	0-25.000 kr.	25.001-200.000 kr.	200.001+ kr.

Tabel C2

SANDSYNLIGHED	Lav	Middel	Høj
INTERVAL	'Forventer ikke, at det kan ske'	'Kan ske inden for 2 år'	'Forventer, det sker mindst årligt'

Tabel C3

		SANDSYNLIGHED		
		Lav	Middel	Høj
KONSEKVENS	Lav	Lav/Lav	Middel/Lav	Høj/Lav
	Middel	Lav/Middel	Middel/Middel	Høj/Middel
	Høj	Lav/Høj	Middel/Høj	Høj/Høj

Analyse af risici
Virksomhed C er meget afhængige af deres webshop, idet alle salg foregår herigennem. Hvis webshoppen bliver utilgængelig i forbindelse med et DDoS-angreb, vurderer virksomheden, at det vil koste omkring 25.000 kr. om dagen i tabt omsætning. Samtidig har virksomheden ikke nogen foranstaltninger til forebyggelse af DDoS-angreb, og virksomheden vurderer derfor, at sandsynligheden for et angreb er høj, selvom de ikke ved, hvem der kunne finde på at angribe.

Som led i deres markedsføring indsamler virksomhed C en del persondata, som bliver analyseret af en tredjepart. Selvom et læk vurderes til at være usandsynligt, mener ejeren, at det måske kan være på kant med GDPR-lovgivningen. Ejeren forventer ikke, at det er noget, Datatilsynet vil reagere på (sandsynlighed: lav), ligesom ejeren heller ikke forventer en stor bøde, hvis virksomhedens praksis skulle vise sig at være ulovlig (konsekvens: lav).

Evaluering af risici
I virksomhed C viste risikoanalysen, at risikoen for et DDoS-angreb er 'høj/middel', hvilket dog afhænger af, hvor længe webshoppen er utilgængelig. Brugen af persondata bliver vurderet til at udgøre en 'lav/lav' risiko. Se tabel C4.

Håndtering af risici
I virksomhed C blev der identificeret en risiko omkring læk af de persondata, som indsamles i forbindelse med webshoppen. Nogle data er nødvendige i forbindelse med fakturering og ordrehåndtering, men en række data bliver sendt til tredjeparter i forbindelse med kundeanalyse. Da ejeren ikke kan se en tydelig værdi af de analyser, besluttes det, at virksomheden skal standse indsamlingen af de unødvendige data og derved helt undgå risikoen (selvom den er lav) for et datalæk fra tredjeparter.

For at nedbringe risikoen for et DDoS-angreb kontakter virksomheden sin IT-leverandør og tilkøber en service, der automatisk opskalerer serverkapaciteten i tilfælde af DDoS-angreb. På den måde bliver sandsynligheden for et angreb kraftigt reduceret.

Tabel C4

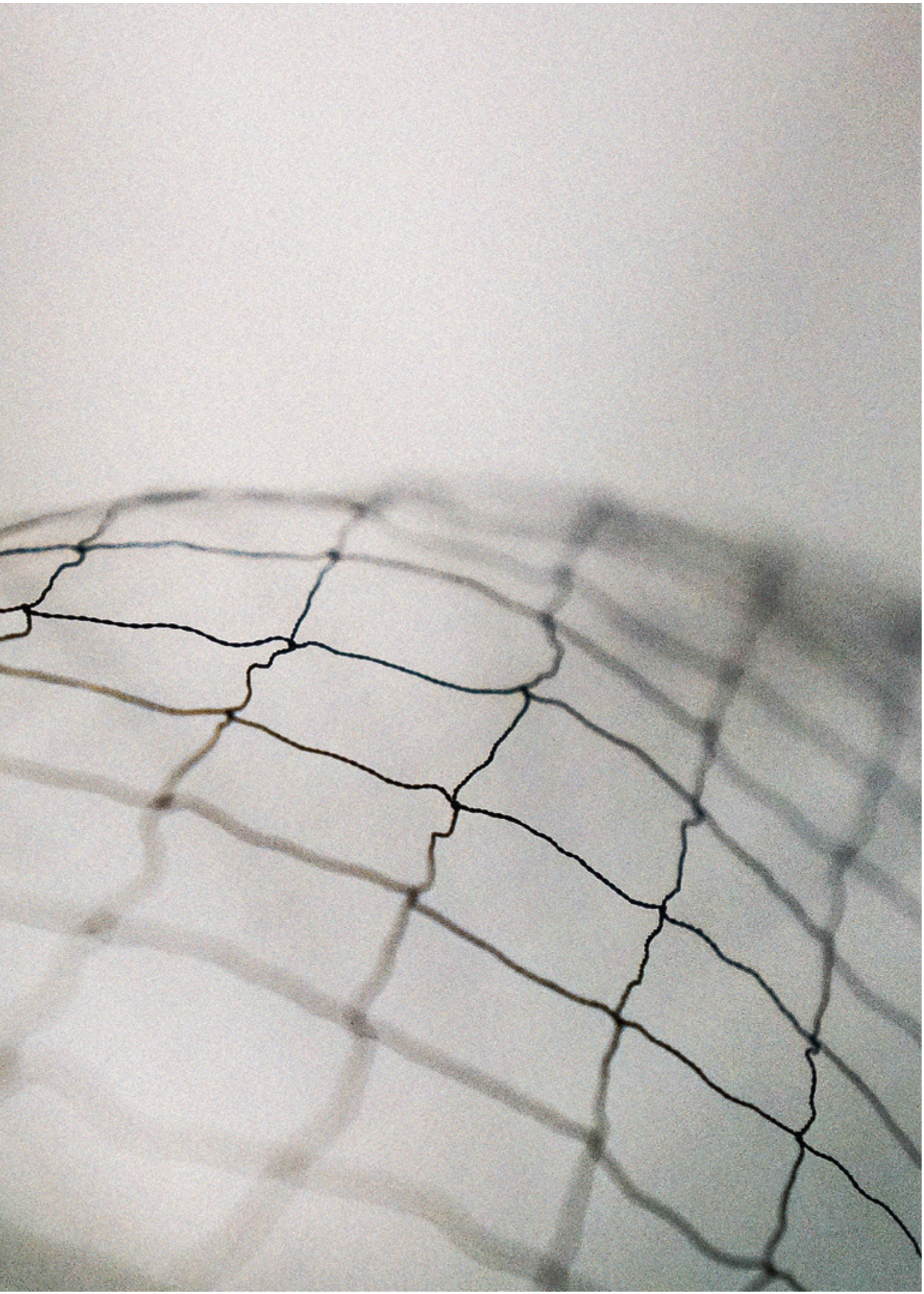
KONSEKVENS \ SANDSYNLIGHED	Lav	Middel	Høj
Lav	**Lav/Lav**	Middel/Lav	Høj/Lav
Middel	Lav/Middel	Middel/Middel	**Høj/Middel**
Høj	Lav/Høj	Middel/Høj	Høj/Høj

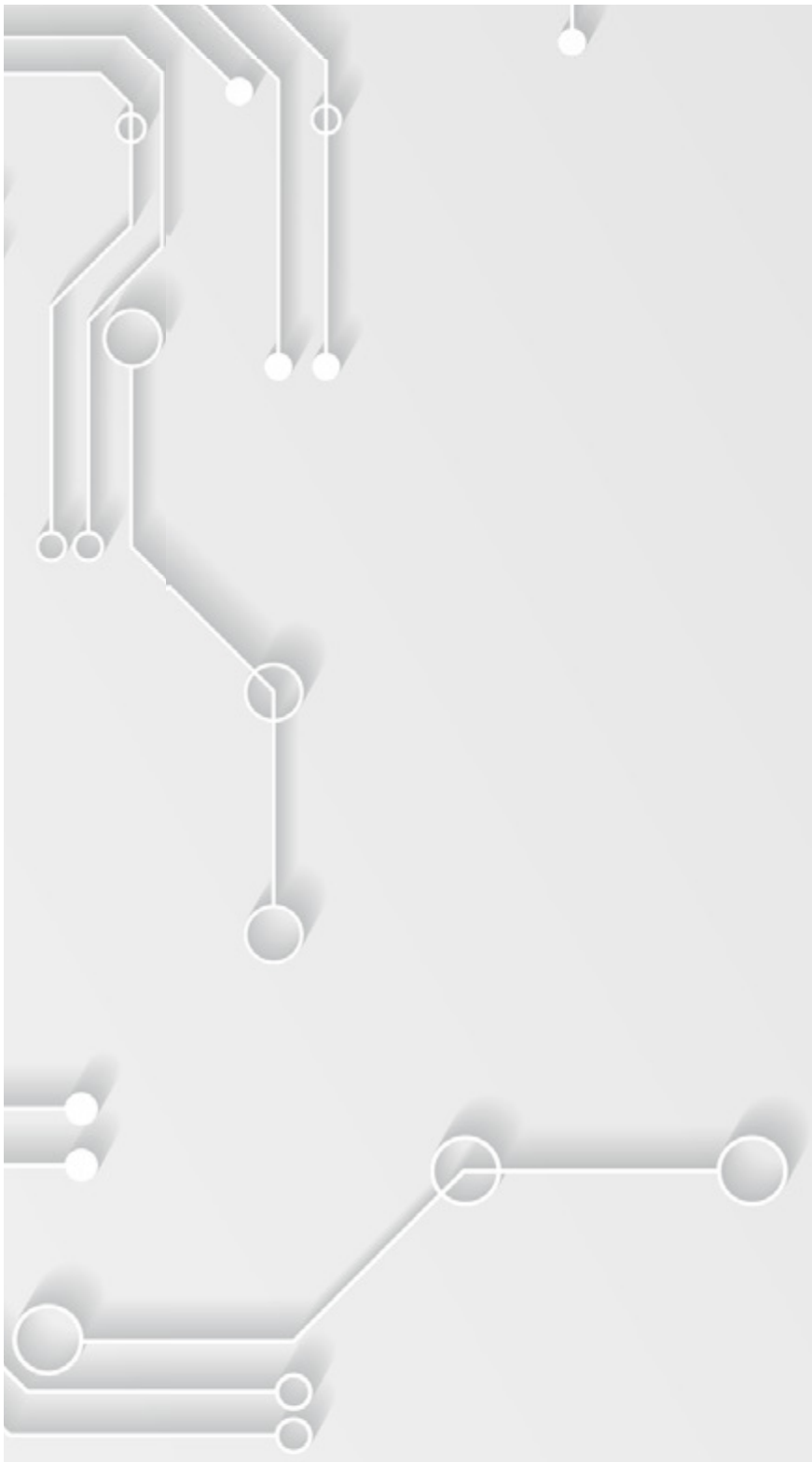
Brug af persondata

DDoS-angreb

Bibliografi og referencer

1. Cybertruslen mod Danmark (Center for Cybersikkerhed, 28. juni 2022): https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/
2. Digital sikkerhed i danske SMV'er 2021: https://erhvervsstyrelsen.dk/digital-sikkerhed-i-danske-smver-2021
3. Erhvervsstyrelsens IT-risikovurderingsværktøj: https://virksomhedsguiden.dk/content/ydelser/it-risikovurderingsvaerktoej/fce38da7-025d-4326-98fe-c198f3ad8316/
4. Erhvervsstyrelsens Sikkerhedstjek: https://virksomhedsguiden.dk/content/ydelser/sikkerhedstjekket/fffe471f-dbad-49a6-ab69-e4d9a01691ab/
5. Exploring the opportunities and limitations of current Threat Intelligence Platforms (ENISA 2018): https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms
6. https://cve.mitre.org/
7. https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed
8. https://www.digitalsikkerhed.dk/vejledning-til-smv-om-cyberforsikringer/
9. https://sikkerdigital.dk/virksomhed/virksomhedscases/pom-industries
10. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements
11. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
12. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks
13. ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment
14. NIS-direktivet: Europaparlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen
15. NIST SP-800-30 Guide for conducting Risk Assessments
16. NIST SP-800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
17. NIST SP-800-39 Managing Information Security Risk: Organization, Mission, and Information System View
18. OCTAVE Allegro: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419
19. OWASP Risk Rating Methodology: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
20. Persondataforordningen (GDPR): Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger
21. STRIDE/DREAD
22. Vejledende tekst om risikovurdering (Datatilsynet og Rådet for Digital Sikkerhed 2019): https://www.datatilsynet.dk/media/7697/vejledende-tekst-om-risikovurdering.pdf





DANSK STANDARD

Fonden Dansk Standard
Göteborg Plads 1
DK-2150 Nordhavn

+45 39 96 61 31
dansk.standard@ds.dk
www.ds.dk