SMV anvendelsesguide for risikostyring i forhold til cyber- og informationssikkerhed

Forord

Denne guide er udarbejdet af Alexandra Instituttet og Dansk Standard. Guiden er udviklet i samarbejde med SMV'er og fageksperter, der har haft mulighed for at give input til guiden via workshops og en offentlig kommenteringsrunde. Guiden er støttet af henholdsvis Cyber Hub og Erhvervsstyrelsen.

Introduktion

Cyberangreb og læk af følsomme personoplysninger fylder meget i medierne, og ifølge Center for Cybersikkerheds trusselvurdering, vurderes truslen fra cyberkriminalitet at være meget høj. Derudover er der også andre faktorer som medarbejdernes digitale adfærd, tekniske nedbrud, brand eller naturkatastrofer, der i lige så høj grad udgør en stor risiko for organisationers cyber- og informationssikkerhed. Samtidigt demonstrerer tiltag som Cyber Security Act, Cyber Resilience Act, NIS2 og Radioudstyrsdirektivet at myndighederne begynder at stille krav til cybersikkerheden i forbindelse med nye love.

En analyse fra Erhvervsstyrelsen viser, at 40% af de danske smv'er har et for lavt digitalt sikkerhedsniveau set i forhold til deres risikoprofil. Dertil kommer at 24% af smv'erne ikke anvender de mest basale sikkerhedsforanstaltninger som opdateringer og backup[1] . Og manglen på opdateringer eller backup kan koste dyrt for danske SMV'er. Et eksempel er Roskilde Teltudlejning, der i 2015 var tæt på konkurs, da de via en phishingmail blev ramt af et ransomware angreb, og netop ikke havde styr på deres backup[2].

Det er derfor vigtigt, at man som organisation er bevidst om og arbejder systematisk med sine risici for at kunne bevare kontrollen og opretholde sine forretningsmål selv om der skulle komme bump på vejen. Et godt udgangspunkt for at højne sikkerhedsniveauet hos danske smv'er er, at hjælpe dem med at kortlægge deres risikoprofil og give dem nogle redskaber til at arbejde konkret med håndteringen af disse risici. Derfor er formålet med denne guide også at samle råd og vejledninger om, hvordan man kan arbejde konkret med risikostyring i forhold til cyber- og informationssikkerhed. Guiden vil være orienteret mod danske smv'er og vil med udgangspunkt i eksempler give inspiration til, hvordan smv'er kan systematisere deres arbejde med

[1] Digital sikkerhed i danske SMV'er 2021

[2] https://sikkerdigital.dk/virksomhed/casehistorier-om-cyberangreb/roskilde-teltudlejning

risici – også selv om man ikke har den store forhåndsviden om risikostyring. Større virksomheder vil dog også kunne finde inspiration i guiden.

Guiden skal fungere som et supplement til Erhvervsstyrelsens IT-risikovurderingsværktøj, men dækker bredere ved at kigge på andre parametre udover virksomhedernes IT-sikkerhed og de tekniske risici, da udefrakommende hændelser, adfærdsmæssige og organisatoriske risici også kan spille en væsentlig rolle ift. adgangen til vigtige informationer for den enkelte organisation.

Ambitionen er, at denne guide bliver et værdifuldt værktøj for danske smv'er og organisationer i deres arbejde med risici inden for cyber- og informationssikkerhed. Målet er at få flere danske smv'er til at sætte fokus på risikostyring og dermed bidrage til at højne sikkerhedsniveauet generelt i dansk erhvervsliv.

1. Introduktion til risikostyring – sådan kommer du 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 organisations potentielle risici. Risici kan bestå af såvel interne som udefrakommende faktorer. Risikostyring er helt centralt for en organisation og er nødvendigt for at sikre organisationens fremtidige overlevelse. Selv om man som organisation arbejder med risikostyring, vil man aldrig kunne fjerne risici fuldstændig. Men ved at have en systematisk tilgang til risici, øger man muligheden for potentielt at reducere sandsynligheden for, at der sker uforudsete hændelser. Risikostyring kan potentielt også minimere konsekvensen af risici.

Langt de fleste organisationer arbejder med risikostyring i et eller andet omfang. Der er som regel styr på de økonomiske risici, og det er også de færreste virksomheder med et fysisk kontor, hvor der for eksempel ikke er en lås på hoveddøren. Men det er langt fra alle virksomheder, der arbejder systematisk med risikostyring, og især når det handler om risikostyring i forhold til cyber- og informationssikkerhed.

Arbejdet med risikostyring ift. cyber- og informationssikkerhed er primært relevant for virksomheder og organisationer, der i en eller anden grad er digitaliserede; for eksempel organisationer med et digitalt faktureringssystem, mailsystem eller netbutik. Og det er efterhånden de færreste virksomheder og organisationer der kan sige, at de på ingen måde er digitaliserede. For selv om det digitale måske ikke er kerneforretningen, er det digitale i mange organisationer blevet et essentielt understøttende værktøj, der potentielt kan have stor indvirkning på kerneforretningen. Der er derfor et stort behov for at adressere cyber- og informationssikkerhed og systematisere arbejdet med risikostyring på linje med f.eks. økonomiske risici.

Der er mange fordele ved at arbejde systematisk med risikostyring i forhold til cyber- og informationssikkerhed. For det første bidrager det til at ruste en organisation, så den er forberedt, hvis den skulle blive udsat for f.eks. it-kriminalitet. Derudover kan en systematisk tilgang til risikostyring i forhold til cyber- og informationssikkerhed også være et konkurrenceparameter og gøre en organisation mere attraktiv over for kunder, samarbejdspartner og eventuelle investorer. At have styr på cyber- og informationssikkerhed bliver også et mere og mere udpræget markedskrav, hvor 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 er forankret hos ledelsen, og der er

afsat ressourcer til arbejdet. Derefter handler det om at få brudt arbejdet op i nogle overkommelige 'bidder'.

Denne guide vil gennemgå processerne i risikostyring trin-for-trin. 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 ift. cyber- og informationssikkerhed[3]. Der findes en række andre forskellige tilgange til risikostyring, og en håndfuld af disse vil kort blive introduceret i annekset.

Tid, kompetencer og ressourcer er nogle af de barrierer, der oftest afholder organisationer 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 er forberedt, og ikke hele tiden skal arbejde med damage control. Hvis man ikke har kompetencerne til at påbegynde en risikostyringsproces, er der hjælp at hente.

Denne guide er et bud på en lettilgængelig gennemgang af en risikostyringsproces, men der er også mulighed for at hente inspiration andre steder, som er beskrevet i annekset. Derudover er der naturligvis mulighed for at få hjælp udefra, selv om det selvfølgelig også kræver noget økonomi. Og endeligt er der ressourcebarrieren, der blandt andet kan dække over økonomi og medarbejdere. Igen handler det om at prioritere. Hvis der er potentiale for at en manglende risikostyring kan have fatale konsekvenser for kerneforretningen, så giver det nok mening at komme i gang.

Endeligt er det vigtigt at huske, at arbejdet med risikostyring er en kontinuerlig proces, da risici løbende ændrer sig i takt med at organisationen og omverden 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 organisation.

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 nogle konkrete eksempler. Eksemplerne er fiktive, men tager udgangspunkt i nogle typiske virksomhedsparametre. De parametre som eksemplerne er bygget op omkring er:

- digitalisering af organisationen
- fortrolighed af data anvendt i organisationen
- organisationens placering i leverandørhierarkiet

Digitalisering af organisationen

Graden af en organisations digitalisering spiller en vigtig rolle i forhold til en organisations risikostyring, og derfor anvendes der i guiden et parameter, der ser på hvor digital organisationen er. I nogle organisationer anvendes IT primært til støttefunktioner som f.eks. bogholderiet. Et IT nedbrud vil derfor få mindre konsekvenser, idet selve forretningen kan fungere mere eller mindre upåvirket i forholdsvis lang tid. I andre organisationer er IT en forudsætning for forretningen (som f.eks. netbutik) og selv et nedbrud på få timer

[3] Standarden er i skrivende stund under opdatering, og der forventes en ny version klar i slutningen af 2022 og en dansk oversættelse forventes at være klar i løbet af 2023.

kan standse al aktivitet indtil problemet er udbedret. Dette kan forekomme tydeligst hvor IT anvendes direkte til at styre produktionen, men kan f.eks. også forekomme i forbindelse med ordrestyring.

Fortrolighed af data anvendt i organisationen

Det andet parameter, som er udvalgt, er omfanget af fortrolig data anvendt i organisationen, da det også har stor indflydelse på, hvordan man tilrettelægger sin risikostyringsproces. Et læk af fortrolige data vil nemlig ikke kun få konsekvenser for den implicerede organisation, men kan også have personlige konsekvenser for medarbejdere, kunder mm. Det er vidt forskelligt hvilke data organisationer behandler. Langt de fleste organisationer behandler fortrolig data i forbindelse med lønningssystemer, men derudover varierer det meget om fortrolig data egentligt behandles. Hvis organisationen f.eks. arbejder indenfor sundhedssektoren eller med mange forretningshemmeligheder, er det naturligvis oplagt at informationers fortrolighed af data skal beskyttes. Modsat er der mange virksomheder, særligt i B2B segmentet, hvor de behandlede data ikke er videre fortrolige.

Organisationens placering i leverandørhierarkiet

Stort set alle organisationer samarbejder med andre organisationer; enten som leverandør eller som aftager af ydelser. Disse relationer er også vigtige at forholde sig til i forbindelse med risikostyring, da potentielle risici også kan have konsekvenser for andre end ens egen organisation. Hvis man f.eks. leverer ydelser til en organisation, som grundet sin natur er særligt udsat for cyberangreb, kan man opleve selv at blive et mål for cyberkriminalitet, selvom ens egen organisation som sådan ikke er så interessant. Ligeledes kan man selv have outsourcet (kritiske) dele af sin forretning til en underleverandør, hvorfor man bør undersøge om underleverandøren har styr på sikkerheden.

Disse tre virksomhedsparametre er udvalgt, da de alle kan have en stor betydning for en organisations tilgang til risikostyring. F.eks. ville en traditionel, mindre murer/tømrer virksomhed sandsynligvis ligge ”lavt” på digitaliserings- og fortrolighedsparametrene, da IT kun bruges af bogholderiet og forretningen mere eller mindre er manuelt baseret. Det kunne dog hurtigt ændre sig, hvis virksomheden har nogle ”interessante” kunder, for eksempel forsvaret, fængsler eller lufthavne og virksomheden i den forbindelse var i besiddelse af plantegninger. Samtidigt er det ikke usandsynligt at virksomhedens IT drift er outsourcet til en anden leverandør, hvilket kunne blive problematisk i tilfælde af problemer hos leverandøren.

2.1 Eksempler anvendt i guiden

Med udgangspunkt i de typiske parametre, er der udarbejdet tre eksempler på organisationer, der er gennemgående i hele guiden. For hvert trin i risikostyringsprocessen, vil det via eksemplerne blive illustreret, hvordan de typiske parametre påvirker processen, og hvad man skal være særligt opmærksom på. Eksemplerne indeholder også en kort beskrivelse af hvordan trinnet kan udføres, herunder hvilke input trinnet kræver og hvad resultatet af trinnet bør være.

Nedenfor en kort beskrivelse af de tre eksempler:

Organisation A:	**Organisation B:**	**Organisation C:**
Mindre autoværksted. Mindre grad af digitalisering. Ingen fortrolige/personfølsomme data. Har private kunder og forskellige leverandører af materialer	Mellem størrelse virksomhed (med omkring 85 ansatte), der producerer og installerer videoovervågnings-systemer.	Lille virksomhed (fire ansatte), der importerer vin. Høj grad af digitalisering (100% webshop)

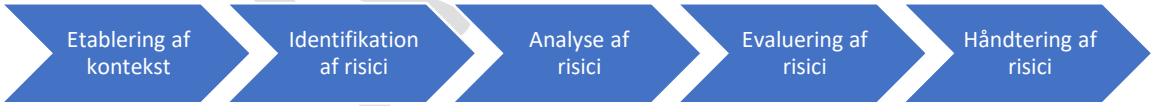
3. Risikostyring trin-for-trin

I dette afsnit gennemgås en risikostyringsproces trin-for-trin og kobles med de tidligere nævnte eksempler og parametre. Denne guides gennemgang af risikostyring er baseret på ISO/IEC 27005's tilgang og operer med fem trin:

- Etablering af kontekst
- 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 benævnes som risikovurdering. Den skelnen kan være relevant at huske, idet nogle standarder og værktøjer udelukkende er beregnet til en del af den samlede risikostyringsproces. F.eks. håndterer ISO/IEC 27005 hele risikostyringsprocessen, mens OCTAVE Allegro[4] arbejder med risikovurdering og derfor ikke omfatter håndtering af identificerede risici.

Figuren nedenfor viser den risikostyringsproces, der er gennemgående i guiden.



3.1 Etablering af kontekst

Det første skridt i en risikostyringsproces er at etablere organisationens kontekst. Formålet med denne fase er at fastsætte rammerne og forberede den videre proces. Dette gøres ved at analysere interne og eksterne forhold og afdække hvad informationssikkerhed betyder for organisationen. Informationssikkerhed handler

4 Se annekset for yderligere beskrivelse.

helt grundlæggende om at sikre data og informationer, og formålet med at etablere konteksten er således også at udvælge de informationer, som er særligt vigtige for organisationen at beskytte.

Det kan nemlig have alvorlige konsekvenser, hvis organisationens informationer bliver ødelagt, stjålet eller på anden vis bliver utilgængelige.

For at vide hvordan man skal vurdere på forskellige risici, er det nødvendigt at se nærmere på de kritiske forretningsprocesser samt de tilhørende informationer som er vigtige at beskytte i sin organisation; de såkaldte primære aktiver[5]. For at kunne udpege de vigtige informationer, skal både interne og eksterne forhold afdækkes:

- Organisationens karakteristika; strategi, mål, vision og mission. Hvad er organisationen sat i verden for at udføre? Hvilke best practices følger organisationen og hvilke lov- og aftalekrav er organisationen underlagt?
- Identifikation af interessentlandskabet. Interessenters forventninger og krav. Hvilke krav stiller interessenter til organisationens informationssikkerhedsindsats? Hvordan skal disse prioriteres?

Både de interne forhold samt interessenters krav og forventninger bidrager til at udpege de risici og muligheder, som skal adresseres, og dermed også danne grundlag for at kunne formulere organisationens formål med informationssikkerhed, som bl.a. kan tælle: Compliance, kulturændring, skabe tillid hos kunder, beskytte kritiske aktiver, sikre business continuity.

Etableringen af kontekst handler også om at fastlægge de næste skridt i risikostyringsprocessen, og her kommer man bl.a. ind på metodevalg for den videre proces. Som organisation kan man selv bestemme hvilken fremgangsmåde man vil følge for den videre risikostyringsproces, men det er vigtigt, at man anvender en metode som muliggør sammenlignelige og reproducerbare resultater. Herefter opstiller man nogle kriterier for den efterfølgende proces med at identificere, analysere og evaluere risici samt at definere ens kriterier for accept af risici. Dette indbefatter bl.a. at man definerer de forskellige niveauer af konsekvens og sandsynlighed (hvad betyder f.eks. "Høj konsekvens" for os?) og spørger sig selv om hvor stor en risiko, der kan accepteres. Ovenstående bør være i overensstemmelse med organisationens politikker, målsætninger og interessenter. Sidst men ikke mindst er der brug for at man træffer beslutninger angående organiseringen af risikostyringsprocessen, hvor der uddelegeres roller og ansvar. Her er det vigtigt, at der udpeges en passende risikoejer, når en risiko er blevet identificeret, og at der fra ledelsens side naturligvis er opbakning til hele processen.

Typisk vil en kontekstbeskrivelse derfor som minimum indeholde:

- Fastsættelse af niveauer for konsekvens og sandsynlighed og hvad de betyder. F.eks. kunne "middel konsekvens" betyde et tab på mellem 100.000 og 500.000 DKK.
- Hvordan beregnes risiko? F.eks. konsekvens niveau x sandsynlighed.
- Hvornår kan en risiko accepteres? F.eks. "Risici accepteres når den er under værdien X".
- Definition af kriterier for risikoejer. F.eks. "Risici under værdi X kan ejes af afdelingsledere" eller "Risici over værdi X skal ejes af adm. direktør".

[5] IT-udstyr, software, personale og fysiske placeringer anses som værende understøttende aktiver. Disse er med til at understøtte forretningsprocesserne og bidrage til at organisationen opbevarer og bearbejder informationer.

Figur på vej om sandsynlighed og konsekvens

3.1.1 Eksempler på etablering af kontekst

Konteksten for **virksomhed A** (et mindre autoværksted) kunne se ud som følgende: 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 laptops med specialprogrammer som bruges af mekanikerne. Disse laptops er dog ikke internetopkoblede. Værkstedet behandler ikke følsomme (person-) data, udover kontaktinformation til kunder, lønsedler og lignende. Den primære bekymring er derfor tab af omsætning, idet læk af data ikke vurderes som særligt relevant og virksomheden ikke er underlagt særlig lovgivning som f.eks. NIS.

Da virksomheden er forholdsvis lille, vil arbejdet i forbindelse med etableringen af konteksten kunne udføres af ejeren af værkstedet sammen med værkstedets bogholder. Selve processen kan foregå som et uformelt møde/brainstorm/workshop 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.

Med ovenstående og virksomhedens størrelse in mente, har virksomheden valgt at risikovurderingen skal foregå med tre niveauer for konsekvens og sandsynlighed (lav, medium og høj) afhængigt af størrelsen på det forventede tab (0-25.000 DKK, 25.000-200.000 DKK og 200.000+ DKK) og sandsynligheden ("har ikke fantasi til at se det ske", "kan ske indenfor 2 år" og "vi forventer det sker mindst årligt"). Risikovurderingen gentages årligt 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 er samtidigt besluttet, at alle høj/høj (konsekvens/sandsynlighed) risici skal udbedres hurtigst muligt, mens lav/medium risici accepteres. Medium/medium og medium/høj risici skal adresseres løbende.

Figur bliver opdateret

Beløb	**Konsekvens**		**Interval**	**Sandsynlighed**
0-25.000 DKK	Lav		"Har ikke fantasi til at se det ske"	Lav
25.000-200.000 DKK	Medium		"Kan ske indenfor 2 år"	Medium
200.000+ DKK	Høj		"Sker mindst årligt"	Høj

For **virksomhed B** (en mellemstørrelse virksomhed, der installerer og udvikler løsninger til videoovervågning) kunne konteksten se ud som følger: IT bruges til regnskab, projektstyring og en række andre administrative funktioner. Det anvendes derudover også i forbindelse med installation af løsninger ved kunder. Virksomhedens løsninger har en funktionalitet, der løbende sender vedligeholdelsesdata hjem til virksomheden, ligesom virksomheden har mulighed for at koble sig på løsninger for at lave fjern-support. Virksomhedens kunder er primært private hjem, men 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. Samtidigt kræver nogle af de større kunder, at der er styr på sikkerheden og ønsker derfor dokumentation herfor.

Da virksomheden ønsker en høj grad af dokumentation, bliver alle beslutninger dokumenteret og gemt i et ledelsessystem. Det inkluderer en liste af interessenter (både interne og eksterne) der skal inddrages i processen, krav der skal leves op til (GDPR og virksomhedens IT sikkerhedssystem baseret på ISO/IEC 27001), 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, 50.000-125.000, 125.000-500.000, 500.000-2.500.000 og 2.500.000+) og sandsynlighed (dagligt, ugentligt, kvartalsvist, årligt, 10-års hændelse), som dog skal revideres 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. Hændelser med risiko på under 10 accepteres, alt derover skal så vidt muligt mitigeres, dog kan produkt-ejer acceptere risici på op til og med 16, mens højere risici skal accepteres på "c-level" ledelse.

Figur bliver opdateret

Beløb	Konsekvens		Definition	Sandsynlighed
0-50.000	**1**		**10-års hændelse**	**1**
50.000-125.000	**2**		**Årligt**	**2**
125.000-500.000	**3**		**Kvartalsvist**	**3**
500.000-2.500.000	**4**		**Ugentligt**	**4**
2.500.000+	**5**		**Dagligt**	**5**

Virksomhed C startede som en enkeltmands virksomhed der importerer vin, men er siden vokset og beskæftiger nu 4 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 klassificeres som persondata og er derfor underlagt GDPR. 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. 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.

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. De risici, der identificeres i denne proces, vil udelukkende være de risici, som man arbejder videre med. Så det er essentielt, at man ikke overser potentielle risici. Identifikation af risici kan yderligere splittes op i to processer; identificering og beskrivelse af informationssikkerhedsrisici og identificering af risikoejere:

Identificering 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 organisationens mål. Når man skal udarbejde sin risikoidentifikation, er der to tilgange, der ofte anvendes:

- Den hændelsesbaserede tilgang
- Den aktivbaserede tilgang

Fælles for tilgangene er, at de begge producerer det samme output, nemlig en liste af de identificerede risici. Listen indeholder beskrivelser af og antagelser omkring de enkelte risici, således man efterfølgende kan foretage risikoanalysen. Selvom resultatet er det samme for begge tilgange, forventer de forskelligt input. Den hændelsesbaserede baserede forudsætter at man har en liste af potentielle hændelser, der kan ramme virksomheden, hvor den aktivbaserede tilgang forudsætter man har en liste af virksomhedens væsentlige aktiver (f.eks. data).

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 forekommer og hvilke konsekvenser den har. Ofte kan hændelser og deres konsekvenser bestemmes ved at identificere de bekymringer, som den øverste ledelse eller andre risikoejere, måtte have. Det kunne f.eks. være en frygt for ikke at kunne modtage ordrer pga. et phishing/ransomware angreb.

Fordelen ved den hændelsesbaserede tilgang er, at den er forholdsvis let forståelig. ”Hvad sker der, hvis vi bliver ramt af ransomware?” er et forholdsvis veldefineret spørgsmål, som man kan undersøge. Ulempen ved den hændelsesbaserede tilgang er, at man kun får undersøgt de hændelser, man har fantasi til at forestille sig. Man kan finde inspiration i lister over mulige hændelser, men det vil dog ofte være nødvendigt at rette til, så det passer til organisationens kontekst. Eksempler på lister kan findes i henholdsvis Tabel E-2 i NIST SP-800-30[6] eller Tabel A.10 i Anneks A i ISO/IEC 27005[7] (nyeste version af 27005), men man kan også bruge mindre formelle lister, som f.eks. det overblik over potentielle trusler mod virksomheder, som man kan finde på sikkerdigital.dk[8]. Udfordringen ved brugen af trusselskataloger er at finde (eller tilrette) et katalog, som passer med organisationens modenhed og scopet for risikovurderingen.

Den aktivbaserede tilgang

Denne tilgang tager udgangspunkt i de aktiver, dvs. data, enheder eller funktioner, der ligger i organisationen og vurderer de trusler og sårbarheder, der er mod aktiverne. Et aktiv er alt, hvad der har værdi for organisationen og derfor kræver beskyttelse. Det kunne f.eks. være de data som ligger i organisationens faktureringssystem, idet fraværet (eller modifikation) af disse ville forhindre fakturering af kunderne og medføre tab for virksomheden. Et andet eksempel kunne være “opskriften”/designdokumenterne/planerne der anvendes i en produktionsvirksomhed, idet en konkurrent

[6] NIST SP-800-30
[7] ISO/IEC 27005:2022
[8] https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed

ville kunne kopiere produktet, hvis de fik adgang til aktivet. Efter organisationens aktiver er identificeret, kan man derefter se på, hvad der kan påvirke aktiverne, og hvad der derfor er en potentiel trussel.

Fordelen ved den aktivbaserede tilgang er, at man tager udgangspunkt i noget velkendt. Det kan gøre det lettere at starte arbejdet, da man skal se ind i organisationen og finde det som, har værdi. Man kan derefter se på mulige sårbarheder og trusler og derudfra definere nogle risikoscenarier. Ligesom i den hændelsesbaserede tilgang, kan det være en fordel at bruge et register over kendte sårbarheder og trusler, f.eks. CVE databasen[9], så man ikke overser noget. ISO/IEC 27005[10] indeholder også lister over både trusler og sårbarheder, og ENISA[11] har også udarbejdet et trusselskatalog, som man kan lade sig inspirere af til risikoidentifikationen.

Identificering af risikoejere

Risikoejere har ansvaret for og beføjelsen til at forvalte de risici, de er ansvarlige for. 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 organisationen, der gør dem i stand til at udøve denne opgave, og træffe informerede beslutninger (f.eks. 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 omkring identificering af risikoejere er en fortsættelse af processen omkring risikoidentifikation. Den kan enten foretages samtidigt med at de enkelte risici identificeres, således en ejer bliver tilknyttet øjeblikkeligt, eller man kan gennemgå listen af identificerede risici og tilknytte ejere efterfølgende. Uanset hvilken tilgang man vælger, vil resultatet af processen være at man har en liste af identificerede risici med ejere tilknyttet.

3.2.2 Eksempler på identifikation af risici og risikoejere

I **virksomhed A** har man valgt at anvende en hændelsesbaseret tilgang. Værkstedsejeren har besluttet at anvende sikkerdigital.dk's liste af trusler mod virksomheder[12] som udgangspunkt for deres liste. Efter gennemgangen af listen på sikkerdigital.dk gør bogholderen værkstedsejeren opmærksom på, at både CEO-fraud og faktura-bedrageri er noget, der er blevet forsøgt på, så derfor er det en reel risici, der skal adresseres.

I **virksomhed B** har man i stedet valgt en aktivbaseret tilgang. I en række workshops har produktejerne, servicechefer, regnskabschefen og salgschefen identificeret hvilke systemer og data, der er kritiske for deres ansvarsområder. Denne liste er derefter blevet behandlet af produktdesignere/arkitekter, IT-afdeling og andre grupper med teknisk indsigt for at identificere potentielle angrebsscenarier. Som inspiration til arbejdet har en arbejdsgruppe gennemgået trusselskataloger fra bl.a. ISO/IEC 27005 og NIST SP-800-30 og derved samlet et skræddersyet trusselskatalog til virksomheden. De identificerede risici har derefter fået tilknyttet en relevant ejer; som udgangspunkt IT-chefen hvis en risiko berører de administrative systemer,

[9] CVE star for "Common Vulnerabilities and Exposures": https://cve.mitre.org/

[10] Tabel A.10 og A.11 i Anneks A i ISO/IEC 27005

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

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

og en produktejer hvis kun et enkelt produkt er berørt. Ligesom under definitionen af konteksten, er der taget referat af samtlige møder, så begrundelser for valg kan dokumenteres. Vigtige beslutninger er derudover indført i ledelsessystemet.

Et af virksomhedens aktiver er de data som overvågningssystemerne sender ind til organisationen. Dette aktiv gav anledning til en række potentielle risici, f.eks. 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** anvender igen samme tilgang som virksomhed A og anvender trusselskataloget fra sikkerdigital.dk.

3.3 Analyse af risici

Når organisationen har identificeret risici, er det næste skridt at analysere disse risici. Formålet med en risikoanalyse er at fastsætte en risikoværdi. I den sammenhæng opererer man ofte med begreberne sandsynlighed og konsekvens. Sandsynlighed dækker over sandsynligheden for at en hændelse indtræffer, og her ser vi på de tidligere identificerede trusler og sårbarheder. Konsekvensen dækker over hvilken konsekvens, som det vil få for vores organisation.

Når man arbejder med informationssikkerhed anvender man ofte begreber som tab af fortrolighed, integritet og tilgængelighed. Fortrolighed handler om at kun autoriserede personer skal have adgang til informationen 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.

Der er flere måder at udregne en risiko på, når man skal forholde sig til sandsynlighed og konsekvens. Er man en lille virksomhed, vil det oftest være nemmest at gøre det simpelt ved en kvalitativ tilgang. Det kan f.eks. være ved 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. Disse skal være beskrevet for både sandsynlighed og konsekvens, hvor sandsynligheden på en skala fra 1-4 vil spænde fra "meget lidt sandsynligt" til "meget sandsynligt" og hvor konsekvensen på en skala fra 1-4 vil spænde fra "mindre konsekvenser" til "katastrofale konsekvenser". Det kan være udfordrende at lave en skala for konsekvens, men man kan med fordel udarbejde en konsekvensskala, der tager udgangspunkt i tab af fortrolighed, integritet og tilgængelighed.

Ved at bruge en skala fra 1-4 i stedet for 1-5 bliver man tvunget til at tage stilling og kan ikke blot vælge den "nemme" løsning ved at vælge værdien 3. Tendensen til at vælge 3 ses særligt, når man ikke helt er sikker på, hvilken score der er den korrekte.

En anden tilgang er den kvantitative metode. Ved denne metode udregner man sandsynlighed ud fra f.eks. procentsatser og konsekvens ud fra tab i omkostninger, hvis en hændelse indtræffer. Det kan være tidskrævende at gøre og samtidigt svært at skaffe sig de data, der gør, at man er i stand til at benytte en kvantitativ metode, hvorfor de fleste vælger den kvalitative metode.

Når vi har forholdt os til sandsynligheden og konsekvensen ved de potentielle trusler, som kan ramme vores kritiske forretningsprocesser og informationer, og dermed analyseret os frem til hvilke risici, vi står over for, kan vi danne os et billede af, hvor udsatte vi er ift. de enkelte risici.

Når man 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 lave en risikovurdering, hvor man udregner konsekvensen ved en hændelse for den registreredes synspunkt i stedet for forretningens synspunkt. Dette kan standarden ISO/IEC 29134[13] hjælpe med.

3.3.1 Eksempler på analyse af risici

I **virksomhed A** gjorde bogholderen opmærksom på at de i virksomheden jævnligt blev udsat for såkaldte CEO fraud forsøg, hvor en angriber forsøger at udgive sig for at være en chef og beder bogholderen om at foretage en bankoverførsel. Risikoen for CEO fraud bliver derfor vurderet til at ske med "medium" sandsynlighed, da de jævnligt bliver modtaget, men opdaget da bogholderen fatter mistanke og derfor reagerer på dem. Konsekvensen er ligeledes "medium", da beløbene der anmodes om som regel er i omegnen af 50.000 DKK.

I forbindelse med risikoidentifikationen blev **virksomhed B** opmærksom på, at det ikke bliver valideret hvor data (videooptagelser) stammer fra, og det derved vil gøre det muligt for en angriber at "overskrive" videoen fra et bestemt kamera. På en workshop, hvor tre teknikere samt produktejeren deltog, blev det vurderet at angrebet forholdsvis nemt kunne gennemføres og det derfor fik en sandsynlighed på '4' (svarende til et angreb om ugen), med en konsekvens på 5 (Firmaets jurist vurderer at virksomheden kan blive stævnet for forholdsvis høje beløb i forbindelse med evt. indbrud hos kunderne).

Virksomhed C er meget afhængige af deres webshop, idet alle salg foregår herigennem. Hvis webshoppen blev utilgængelig i forbindelse med et DDoS angreb, vurderer virksomheden at det vil koste omkring 25.000 om dagen i manglende omsætning. Samtidigt har virksomheden ikke implementeret nogle foranstaltninger til forebyggelse af DDoS angreb og virksomheden vurderer derfor at sandsynligheden for et angreb er høj, selvom de ikke ved hvem som skulle være motiveret for et angreb.

3.4 Evaluering af risici

På baggrund af de tidligere trin, har organisationen nu identificeret og analyseret sig frem til nogle risici, som kan sammenholdes med organisationens politikker og målsætninger, som blev identificeret i forbindelse med etableringen af konteksten. Formålet med dette trin er at forholde sig til om den enkelte risiko er en man kan og vil leve med ift. forretningens målsætninger og politikker, eller om det er noget, man skal forsøge at ændre på. I den forbindelse er det vigtigt at ledelsen er med til at definere 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. De risici hvor både sandsynligheden og konsekvensen er meget lille, er nok heller ikke dem, der er brug for at adressere som det første.

[13] Se kort beskrivelse af ISO/IEC 29134 i annekset

3.4.1 Eksempler på risikoevaluering

I **virksomhed A** viste risikoanalysen at risikoen for CEO fraud var "medium/medium", dvs. at risikoen falder i kategorien af risici der løbende skal adresseres.

I **virksomhed B** viste risikoanalysen at risikoen ved den manglende validering, var 4 x 5, dvs. 20.

I **virksomhed C** viste risikoanalysen at risikoen for et DDoS angreb var "Medium/Høj", hvilket dog afhænger af hvor længe webshoppen er utilgængelig.

Figur bliver opdateret.

	Sandsynlighed		
Konsekvens	Lav / Lav	Medium / Lav	Høj / Lav
	Lav / Medium	Medium / Medium	Høj / Medium
	Lav / Høj	Medium / Høj	Høj / Høj

3.5 Håndtering af risici

Når organisationen har udregnet risici for de relevante potentielle hændelser og besluttet sig 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 i den forbindelse god mening at kigge på en cost-benefit analyse; er omkostningerne ved at undgå risici større end hændelsen man ønsker at forhindre?

Ved risikohåndtering er der fire valgmuligheder for, hvordan man vælger at håndtere en risiko:

1. **Acceptere risikoen.** Dette er en mulighed, hvis risikoen falder ind under hvad organisationen vil leve med ift. deres politikker og kriterier for risikoaccept. Eller at omkostningerne ved at adressere risikoen er så høj, at det ikke giver mening. Der kan også være tale om en risiko, som det slet ikke er muligt for en organisation at gøre noget ved (f.eks. naturkatastrofer) Risikoen vil fortsat være der, men organisationen adresserer den først i det øjeblik, at den udmønter sig.
2. **Undgå risikoen.** Risikoen undgås ved at stoppe eller ændre den aktivitet, der forårsager risikoen. En organisation kan vælge at undgå risikoen, hvis konsekvensen af en hændelse falder uden for ens risikoaccept. Man vil også forsøge at undgå risikoen, hvis denne er for stor, og der ikke kan findes nogle passende handlinger til at nedbringe den.
3. **Flytte/dele risikoen.** Det er en mulighed at flytte risikoen ved f.eks. at outsource en aktivitet til andre, som er bedre i stand til at varetage opgaven med en mindre risiko. Et andet eksempel er at tegne en forsikring som nedbringer konsekvensen, hvis uheldet er ude. Det skal dog bemærkes, at det at flytte risikoen skaber en ny risiko[14].
4. **Forøge/minimere risikoen.** Organisationer kan vælge at implementere nogle foranstaltninger/igangsætte nogle aktiviteter, som er med til at nedbringe/fjerne sandsynligheden eller konsekvensen og dermed nedbringe risikoen til et niveau, som organisationen kan leve med.

[14] Det kan være svært at udregne, om en forsikring vil dække organisationens tab af informationer tilstrækkeligt. Derudover er det også vigtigt at pointere, at selvom man outsourcer aktiviteter til andre, står man stadig med ansvaret (NETS sagen). 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/

Som organisation kan man vælge mellem forskellige foranstaltninger/aktiviteter, der kan bidrage til at nedbringe risici. Disse aktiviteter kan have forskellige egenskaber; de kan være forebyggende, opdagende eller korrigerende. Hvis man gerne vil nedbringe sandsynligheden for at en hændelse indtræffer, er det ofte forebyggende tiltag, som man særligt skal benytte. Er det konsekvensen man gerne vil nedbringe, er det ofte opdagende og korrigerende tiltag, som man skal fokusere på at implementere.

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

3.5.1 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 DKK, 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.

I **virksomhed B** besluttes det, at der øjeblikkeligt skal implementeres en mekanisme til at foretage valideringen. Al andet udviklingsarbejde bliver derfor sat i bero indtil det er på plads. Dette vil sænke 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 han tager emnet op til diskussion ved et bestyrelsesmøde, således de kan bestemme om den resterende risiko skal accepteres eller om produkterne skal tilbagekaldes.

Virksomhed B identificerede en risiko omkring manglende kompetencer i forbindelse med IT nedbrud (f.eks. i tilfælde af et ransomware angreb). Selvom virksomheden råder over en kompetent IT-afdeling er det IT-chefens vurdering, at virksomheden ikke har ressourcerne til hurtigt at få gendannet systemerne. Virksomhed B beslutter derfor at tegne en forsikring, der kan hjælpe med ressourcer i tilfælde af et nedbrud og samtidigt dækker noget af det driftstab, der kan forekomme i forbindelse med evt. nedbrud.

Virksomhed C identificerede en risiko omkring læk af de persondata som blev indsamlet 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 for et datalæk fra tredjeparter.

Opsamling

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

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

Som tidligere nævnt er selve organiseringen af risikostyringsprocessen ret central for at den skal give mening. Da risikostyring er et kritisk område, er det afgørende, at ledelsen er involveret og dedikerer de nødvendige ressourcer til både udformning og implementeringen af processen, såvel som de efterfølgende mitigerende foranstaltninger. På samme måde er det vigtigt at de, der er ansvarlige for risikostyring, har mandat fra ledelsen til at gennemføre implementeringen.

En risikostyringsproces er ikke en uoverskuelig opgave, men kan sættes i værk med både knappe ressourcer og begrænset tid.

Anneks: 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.

- ISO/IEC 27005 Vejledning i risikostyring for informationssikkerhed
- OCTAVE Allegro
- NIST SP 800-30, SP 800-37 og SP 800-39
- STRIDE/DREAD
- OWASP Risk Rating Methodology
- Erhvervsstyrelsens IT-risikovurderingsværktøj
- Sikkerhedstjekket

ISO/IEC 27005 Vejledning i risikostyring for informationssikkerhed

Denne guides trin-for-trin gennemgang af risikostyring er baseret på ISO/IEC 27005's tilgang.

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 nogle redskaber til at prioritere risici, og kan dermed bidrage til at sikre det optimale niveau af foranstaltninger i en organisation ift. værdien af den information, som skal beskyttes. Standarden stiller skarpt på konsekvenser 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 (ISMS), der stiller de overordnede krav til en systematisk tilgang til informationssikkerhed. Men ISO/IEC 27005 kan sagtens læses og anvendes selvstændigt.

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 novicer på området også forstår indholdet.

Udgangspunktet for denne guide er baseret på principperne fra ISO/IEC 27005-standarden som er suppleret med konkrete eksempler på, hvordan den kan anvendes.

ISO/IEC 29134 Guideline for privacy impact assessment

Hvis man arbejder med persondata, kan det være relevant at udføre en Privacy Impact Assesment (PIA). 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 datasubjektets (den person som data omhandler) interesser 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 generel risikovurderings rammeværk, målrettet større virksomheder med over 300 ansatte. Den originale OCTAVE metode er sidenhen, i form af Allegro, blevet forenklet lidt og blevet målrettet "informations-aktiver"og hvor de anvendes. Metoden har mange lighedspunkter med ISO/IEC 27005. Først etableres diverse kriterier (f.eks. hvad betyder "høj konsekvens"), hvorefter informationsaktiverne identificeres og beskrives. Efter en beskrivelse af informationsaktiverne er udarbejdet , kigges der på trusler mod aktiverne og en række trusselsscenarier beskrives og den egentlige risikoanalyse kan foretages. Metoden afsluttes med en fase omkring risikomitigering, hvor man vælger hvorledes 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 , f.eks. omkring hvem der skal orienteres eller godkende i de forskellige trin undervejs. Metoden er samtidig mere specifik i forhold til ISO/IEC 27005 og fastlåser dermed brugeren til f.eks. tre kategorier for konsekvens. At metoden er, så specifik kan gøre den en smule lettere at anvende direkte, men betyder samtidigt 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 dog ikke så udbredt, udover i nogle tekniske nicher/brancher, hvor det kan være relevant at overholde amerikansk lovgivning. Det kan f.eks. være hvis man skal levere til de amerikanske myndigheder eller forsvar. NIST SP 800-30, 800-37 og 800-39 arbejder alle med emner indenfor risikostyring. Da NIST publikationerne udgør et komplet rammeværk (som også omhandler mange andre emner end risikostyring), behandles dermed også en del af de samme emner som 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, da en del af risikostyringen i NIST regi, er beskrevet som en del af IT-sikkerheds styringen i ISO/IEC regi.

I forbindelse med de tre beskrevne publikationer, omhandler SP 800-30 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 hvormed det sker, ikke er den samme.

STRIDE/DREAD

STRIDE og DREAD er ikke egentlige risikovurderingsmodeller, men er ofte anvendt i forbindelse med risikovurdering. Begge modeller er tiltænkt at blive anvendt i 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 gennemgår for de enkelte komponenter eller interfaces i et system. Ved at anvende checklisten sikrer man, at man kommer igennem de gængse typer af trusler for et system og derved sikrer en højere grad af reproducerbarhed i analysen.

DREAD er et akronym for:

- **D**amage – Hvor slem 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 den ikke tager højde for at de individuelle kategorier kan vægte forskelligt i det enkelte cases.

Begge modeller er væsentligt mere teknisk orienteret end risikostyrings/risikovurderings værktøjerne fra ISO/IEC 27005 og OCTAVE Allegro og kan anvendes af arkitekter, programmører og systemadministratorer uden involvering af ledelsen. Samtidigt 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 indenfor IT sikkerhed og har derfor udarbejdet guides vedrørende risikovurdering. OWASP har i den forbindelse to projekter, OWASP Risk Assessment framework, som består af nogle værktøjer til statistisk analyse og OWASP Risk Rating Methodology, som er beskrevet her.

OWASP Risk Rating Methodology er en forholdsvis enkel og uformel model til risikoanalyse. Den består primært af en beskrivelse af, hvordan man kan estimere sandsynlighed for at en hændelse sker, og hvor stor konsekvensen af hændelsen er. Dette gøres ved at nedbryde sandsynlighed og konsekvens estimaterne til otte underemner, som er lettere at estimere.

Metodikken er primært tiltænkt teknikere og giver ikke megen vejledning i hvordan de identificerede risici efterfølgende skal håndteres. Dele af konsekvensanalysen kan ligeledes udelades, hvis personerne der udfører analysen, ikke har forretningsmæssig indsigt.

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 risikoscenarier bliver man bedt om at forholde sig til sandsynligheden for at risikoscenariet indtræffer og hvad konsekvensen i så fald vil være for ens forretning. Både sandsynlighed og konsekvens selvvurderes ud fra en simpel 1-5 skala.

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, som 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 sikkerhedsløsning
- Samarbejdspartnere.