INFORMATIONSSIKKERHED

INFORMATIONS-SIKKERHEDS-AKTIVITETER

– KOMMUNALT ARBEJDE MED ØGET INFORMATIONSSIKKERHED

Informationssikkerhedsaktiviteter
– Kommunalt arbejde med øget informationssikkerhed

1. udgave, 1. oplag 2017

Produktion: Kommuneforlaget A/S
Design: e-Types
Foto: Colourbox

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne
facebook.com/kommunerne

Produktionsnr. 830261
ISBN 978-87-93365-92-6-pdf

INDLEDNING

Afhængigheden af digitale løsninger vokser, og udfordringerne med at fastholde et acceptabelt sikkerhedsniveau øges og forandres med stor hast. Ligesom konsekvenserne af sikkerhedsbrud vokser. Borgernes tillid til den digitalt understøttede kommune afhænger af, at kommunerne kan beskytte data mod misbrug. Borgere og virksomheder skal fortsat have tillid til og være trygge ved kommunernes håndtering, anvendelse og opbevaring af data og informationer. Kommunerne skal således øge og tilpasse indsatsen for informationssikkerhed.

I den fælles kommunale digitaliseringsstrategi er det derfor aftalt, at der i fællesskab gøres en indsats ift. sikkerhedsarbejdet, herunder, at kommunerne vil arbejde aktivt med risikobaseret håndtering af udfordringerne med informationssikkerhed med inspiration fra ISO27001 standarden. Det er ligeledes aftalt i den fællesoffentlige digitaliseringsstrategi 2016-2020, at alle myndigheder skal øge fokus på sikkerhed og at kommunerne skal følge principperne i standard for informationssikkerhed, ISO27001. Ligesom det er aftalt, at der skal følges op på myndighedernes arbejde med informationssikkerhed.

ISO27001 er en sikkerhedsstandard, der arbejder med en risikobaseret tilgang til informationssikkerhed ud fra en række områder eller principper for, hvad der skal være fokus på, for at en organisation kan gennemføre et kvalificeret arbejde med informationssikkerhed. Denne tilgang passer godt med de nye regler i databeskyttelsesforordningen, da der også her lægges der op til en risikobaseret tilgang.

Med udgangspunkt i den risikobaserede tilgang, principperne for ISO27001 samt erfaringer fra kommuner, har KL udarbejdet denne opsamling, kaldet en drejebog, der kan anvendes i arbejdet med at øge informationssikkerheden i den enkelte kommune.

Drejebogen er bygget op med afsæt i de seks fælleskommunale indsatsområder, der arbejdes med i det fælles kommunale sikkerhedsprogram. Projektet har særligt fokus på elementerne:

- Forretningsoverblik og ledelsens styring af informationssikkerhed
- Politik for informationssikkerhed
- Risikovurdering og håndtering, herunder dokumentation af kontroller

Der arbejdes derudover videre med elementerne leverandørstyring, hændelseshåndtering og beredskabsplan. Drejebogen vil blive opdateret ultimo 2017 med disse emner.

I denne drejebog angives forslag til en måde at håndtere indsatsområderne på. Alle kommuner er forskellige i størrelse, kompleksitet og organisering, og derfor må hver kommune forholde sig konkret til egne forhold. Ledelsesmæssig styring af informationssikkerhed afhænger alene af den enkelte organisation, dens kultur og informationer og skal planlægges, tilrettelægges og udvikles herefter. Det er derfor vigtigt, at den enkelte kommune selv prioriteter og forholder sig til, hvorledes man ønsker at anvende drejebogen.

I drejebogen henvises der til en række hjælpeværktøjer og skabeloner, der kan være en støtte i arbejdet med den risikobaserede tilgang. Disse kan frit benyttes i kommunen og kan hentes i Sikkerhedsprogrammets Yammer-portal, som kommunens kontaktperson til Sikkerhedsprogrammet har adgang til. I Yammer er der ligeledes mulighed for at dele konkret erfaringer med andre kommuner og der findes eksempler på de forskellige produkter, som kommuner har lagt op.

Målgruppe
Drejebogen er henvendt til kommunens informationssikkerhedskoordinator og øvrige kommunale ansatte, der har ansvaret for informationssikkerhed.

01 / FORRETNINGS-OVERBLIK

Fundamentet for arbejdet med informationssikkerhed er, at der er skabt et godt overblik over forretningen, dvs. at der findes et klart billede af hvilke informationer, der er de mest kritiske for forretningen.

Det kræver et kendskab til interne og eksterne forhold, som kan bidrage med at bestemme de primære forretningsområder og tilhørende processer.

Output
Overblik over forretningsprocesser, arbejdsområder, interessenter og systemer m.v., som er essentielle for kommunen, herunder de ansvarlige for forretningsområderne (system- og risikoejere). Dette udgør endvidere grundlaget for risikovurderingen.

I det omfang dette overblik allerede findes, anbefales det at dette anvendes.

Anbefaling
Overblik over forretningen kan fx skabes gennem workshops med fagchefer og andre interne interessenter, som vil kunne bidrage med det forretningsmæssige indblik og medvirke til at skabe en fælles forståelse af vigtige prioriteringer.

Det er vigtigt, at der fokuseres bredt på informationer, og at det ikke kun kommer til at handle om "it-systemer".

Man skal kort sagt gå fra at have fokus på it-sikkerhed til at have fokus på informationssikkerhed.

Som et led i arbejdet med databeskyttelsesforordningen har KL påtaget sig opgaven med at udarbejde fællesfortegnelser, der er dækkende for alle kommunale behandlingsaktiviteter.

Fortegnelserne indeholder bl.a. oplysninger om hvilke typer oplysninger der behandles, formålene med behandlingen, sikkerhedsforanstaltninger og overførsel til tredje lande. Fortegnelserne kan derfor anvendes til at skabe et overblik over kommunale behandlingsaktiviteter og dermed bidrage til forretningsoverblikket.

Titlerne på KL's fællesfortegnelser (som de ser ud pr. 1. august 2017):

- Beredskab
- Beskæftigelse
- Borgerbetjening
- Borgerlige forhold (se KLE-hovedgruppe nr. 23)
- Børne- og voksenforanstaltninger
- Dag- og uddannelsestilbud
- Flygtninge og integration
- Infrastruktur, forsyning, affald og spildevand
- Kultur- og idrætstilbud, fonde og samarbejder
- Ledelsesinformation og tværgående projekter
- Løn- og personaleadministration samt arbejdsmiljø
- Natur- og miljøbeskyttelse
- Omsorgs- og sundhedsydelser
- Planlægning, byggeri og erhvervsforhold
- Regulering af private erhverv
- Sekretariatsbetjening og kommunikation
- Social service og behandlingstilbud samt sociale ydelser
- Økonomiadministration og kontante ydelser

Deler man kommunen op efter ovenstående, skal man være opmærksom på, at de tilknyttede behandlinger af personoplysninger til de enkelte fortegnelser kan foregå flere steder i kommunen. Der er således behov for at afdække den organisatoriske forankring af behandlingerne og ansvaret for sikkerheden af disse behandlinger.

02 / LEDELSENS STYRING AF INFORMATIONS-SIKKERHEDEN

Informationssikkerhed er et ledelsesansvar ligesom det er tilfældet for økonomistyring, håndtering af arbejdsmiljøet, serviceniveauet eller borgerbetjening.

Den ledelsesforankring, der er nødvendig på informationssikkerhedsområdet, skal konkret komme til udtryk i:

- Målfastsættelse
  Den øverste ledelse fastlægger niveauet for sikkerhed i organisationen, herunder accepterer risici, idet den træffer de overordnede beslutninger vedrørende informationssikkerhed og forholder sig til økonomiske, ressourcemæssige og organisatoriske konsekvenser.

- Organisering
  Der skal tages stilling til organiseringen internt i kommunen
  - Ressourceallokering
  - Definering af politikker og strategier
  - Definering af roller og ansvar
  - Aktiv opfølgning på den løbende rapportering

Output
Beskrivelse af organisering, navne, opgaver, roller og ansvar i forhold til kommunens behov og prioritering af arbejdet med informationssikkerhed.

Det gælder fx udpegning af informationssikkerhedskoordinator, informationssikkerhedsudvalg og formandskab, systemejere, brugernes ansvar mv.

Organiseringen skal godkendes af topledelsen

Anbefaling
Den risikobaserede og ledelsesforankrede tilgang er grundlaget for arbejdet med informationssikkerheden. En tilgang, hvor arbejdet med informationssikkerhed vurderes i forhold til betydningen for forretningen og borgerne, og hvor prioriteringen af indsatsen derfor flyttes ud af it-afdelingen og fra it-leverandøren og over til forretningen.

Styringen af informationssikkerhed bør tilpasses og integreres i den eksisterende organisation, så der tages hensyn til eksisterende arbejdsgange, organiseringer og ansvarsfordelinger m.v.

Den øverste ledelse bør etablere en organisation til koordinering af informationssikkerhedsarbejdet. Organisationen igangsætter aktiviteter, følger op på implementering af politikker og retningslinjer, måler effekt og rapporterer tilbage til ledelsen.

I den forbindelse er informationssikkerhedsudvalget en vigtig del af informationssikkerhedsorganisationen og det skal besidde den nødvendige beslutningskompetence. Det er eksempelvis sikkerhedsudvalget, der sætter mål for sikkerheden og sørger for at informationssikkerheden realiseres og efterleves.

Det anbefales derfor at informationssikkerhedsudvalget bemandes med IT- eller Digitaliseringschefen samt ledelsesrepræsentanter fra de vigtigste fagforvaltninger (set ud fra den risikobaserede tilgang). Formanden for udvalget bør være en repræsentant fra direktionen.

I stedet for at etablere et informationssikkerhedsudvalg kan man vælge at give et eksisterende udvalg, eksempelvis digitaliseringsudvalget, ansvaret som informationssikkerhedsudvalg.

Yderligere beskrivelse af funktioner og roller i arbejdet med informationssikkerhed kan findes i præsentationen: Informationssikkerhed, en rejsefortælling om funktioner, roller og ledelse.

03 / POLITIK FOR INFORMATIONS-SIKKERHED

Alle kommuner har en sikkerhedspolitik. Denne skal transformeres til en informationssikkerhedspolitik. Det er topledelsens ansvar at informationssikkerhedspolitikken passer til kommunens opgavemæssige formål, indeholder målsætninger og rammer for sikkerhedsarbejdet og en forpligtigelse til løbende forbedringer af informationssikkerheden.

Informationssikkerhedspolitikkerne er et strategisk styringsredskab, hvor kommunens målsætning, afgrænsning, ansvarsplacering og rammer for styringen af arbejdet med informationssikkerhed fastsættes. Informationssikkerhedspolitikkerne kan også bidrage til at skabe en fælles forståelse i kommunen for, hvad informationssikkerhed indebærer, og hvilken tilgang man har til det.

Output
En informationssikkerhedspolitik for kommunen, der løbende opdateres. Informationssikkerhedspolitikken skal godkendes af topledelsen og kommunikeres til medarbejderne, så de forstår hvilken betydning politikken har for dem.

Anbefaling
Ledelsen bør involveres i arbejdet med informationssikkerhedspolitikken, så det sikres, at dens vurderinger og beslutninger indgår. Politikken kan evt. skrives ud fra en eksisterende skabelon i kommunen.

Det anbefales at indarbejde afsnit om etablering og vedligeholdelse af Informationssikkerhedsstyring.

Den løbende opdatering vil ofte være informationssikkerhedsudvalgets opgave, hvor der tages udgangspunkt i den aktuelle risikovurdering for kommunen.

04 / RISIKOVURDERING OG -HÅNDTERING

Risikovurdering handler om at identificere og analysere mulige trusler, sårbarheder overfor truslerne og sandsynligheden for de kan opstå. Desuden vurderes konsekvenser i forhold til risikoen for tab af fortrolighed, integritet og tilgængelighed, eksempelvis risiko for at lønsedler ved en fejl sendes til en forkert borger, at data utilsigtet ændres så de ikke er korrekte eller et system bryder ned, så det ikke er tilgængeligt.

Arbejdet med risikovurderingen skal munde ud i en vurdering af, hvilke trusler der synes mest oplagte i forhold til at kunne påvirke forretningens evne til at nå sine mål. Dermed får ledelsen mulighed for at prioritere de indsatser, som giver kommunen et passende og ønsket niveau af informationssikkerhed, ligesom ledelsen kan prioritere ressourcerne i forhold til, hvor de gør mest gavn.

På baggrund af risikovurderingen udarbejdes en handlingsplan, der følger op på de risici, der vurderes som de vigtigste, og som ledelsen skal forholde sig til. Der skal foretages en organisatorisk, fysisk og teknisk afgrænsning af risikostyringens omfang, defineres risikotolerance og beskrives en metode for risikovurderingen.

Output
Beskrivelse af risikovurderingsprocessen. Risikovurdering indeholdende følgende elementer:

- Trusselsidentifikation (trusselskatalog)
- Konsekvensvurdering
- Sandsynlighedsvurdering (sårbarhedsvurdering)
- Overblik over risici (risikobillede)
- Risikohåndtering (prioritering og handlingsplaner)

Risikovurderingen og de aftalte aktiviteter i handlingsplanen skal godkendes af topledelsen.

Anbefaling
I forbindelse med risikovurderingen anbefales det altid at gennemføre en konsekvensvurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed (FIT).

› EKSEMPEL PÅ FORTROLIGHED

Brud på fortroligheden handler om, at data mister sin beskyttelse, og fremmede/uvedkommende dermed får adgang til data, som de ikke burde have adgang til.

Eksempler på brud på fortroligheden er:

› En bruger får ved en fejl adgang til en mappe på et fildrev, en sag eller en system, som personen ikke burde have adgang til, og dermed til data som personen ikke burde havde adgang til

› Et regneark bliver ved en fejl sendt til personer, som ikke skulle have haft det, og dermed får modtagerne adgang til data, som de ikke burde have haft

› Et brev med følsomme personoplysninger sendes ved en fejl til en forkert borger.

› EKSEMPEL PÅ INTEGRITET

Integritet handler om, at man kan stole på data, dvs. at de data som er, f.eks. i et system, er de rigtige, og at man kan/tør træffe beslutninger på baggrund af dette.

Eksempler på brud på integriteten er:

› At der bliver indlæst gamle (ugyldige) data ind i et system, således at data ikke længere er de senest nye – og der dermed træffes beslutninger på et forkert grundlag

› At udefrakommende hacker sig ind på kommunens pc'er og foretager ændringer i it-systemer med personoplysninger eller i dokumenter indeholdende personoplysninger lagret på eksempelvis computerens drev eller fællesdrev

› At et regneark bliver overskrevet med en gammel version, og det dermed ikke længere er korrekt.

› EKSEMPEL PÅ TILGÆNGELIGHED (UNDER ½ DAG, 1 DAGE, 3 DAGE, EN UGE ELLER MERE)

Tilgængelighed handler om, at man kan få adgang til data.

Eksempler på brud på tilgængeligheden er:

› Systemet er brudt ned, og data er dermed ikke tilgængelige

› At der er journaliseret forkert – dvs. at dokumenter er lagt på en forkert sag, og dermed ikke er tilgængelige

› At data er blevet flyttet, eller der er blevet ændret ved muligheden for adgang, og de dermed ikke er tilgængelige

› Angreb af hackere med ransomware, hvor filer låses med krav om løsepenge for at åbne filerne igen.

Risikovurdering bør tage udgangspunkt ide vigtigste aktiver, eksempelvis de vigtigste forretningsprocesser med anvendte it-systemer samt vigtigste tekniske aktiver (it-/digitaliseringsafdelingens ansvarsområde).

De vigtigste aktiver findes ved at inddrage fagforvaltningerne og få deres vurdering af, hvilke kritiske forretningsprocesser de har og er afhængige af. Eksempelvis lægge vægt på processer/arbejdsgange hvor sikkerhedsbrud kan have indvirkning på liv, ære og velfærd eller give økonomiske tab.

Det anbefales at informationssikkerhedsudvalget godkender hvilke aktiver, der skal gennemføres en risikovurdering på, så omfanget bliver styret.

Risikovurderingen bør dog ikke kun omfatte forretningsprocesser, it-systemer og de tekniske aktiver (it-afdelingens ansvarsområde), men alle de aktiver som indgår i et informationssystem. Det inkluderer også fysiske aktiver som fx papirarkiver, medarbejdere, immaterielle aktiver. I mange tilfælde kan de tekniske aktiver grupperes på en måde, hvor antallet begrænses, mens det stadig er muligt at knytte specifikke trusler til dem. For eksempel kan routere, switche, firewalls mv. grupperes som netværksudstyr eller infrastruktur. Aktiverne kan med fordel grupperes efter deres type for at lette identifikationen, eftersom der ofte vil være en sammenhæng med de relevante trusler.

Det anbefales at starte med risikovurderingen indenfor eksempelvis et fagforvaltningsområde for at opnå erfaringer med den valgte metode. Efterfølgende kan metoden tilpasses i.f.t. erfaringer og udbredes til hele kommunen.

Deltagere
Risikovurderingen og risikohåndteringen vil ikke kunne foretages af sikkerhedskoordinatoren alene, men kræver at områdeleder, systemejer, superbruger eller andre medarbejdere, der kan vurdere konsekvenser og sandsynlighed, inddrages.

05 / KOM GODT I GANG MED RISIKOVURDERING

Fastlæggelse af omfang
Inden selve risikovurderingen påbegyndes, skal omfanget og niveauet af den ønskede risikovurdering fastlægges. Der skal besluttes skala for konsekvens- og sandsynlighedsvurdering ligesom trusselskatalog skal beskrives. De primære deltagere i dette arbejde kan være it-sikkerhedsfunktionen og forretningen .

Trusselsvurdering
Identifikationen af relevante trusler er afgørende for, at man ikke overser risici. Derfor bør trusselsvurderingen ske på en systematisk måde. Ved at tage udgangspunkt i et katalog over mulige trusler kan man pejle sig ind på de trusler, der er relevante.

Der findes meget omfattende trusselskataloger, som indeholder enhver tænkelig situation, men man kan også anvende mere generiske kataloger. Ifølge National strategi for cyber- og informationssikkerhed er det et krav, at cyber trusler også indgår i myndighedernes risikovurderinger og risikoledelse fra 2015.

Under skabeloner i Yammer findes et eksempel (Trusselkatalog eksempel) på et mere omfattende trusselskatalog, hvor hver enkelt trussel er vurderet i.f.t.

1. om den udgør en risiko for brud af fortrolighed, integritet og/eller tilgængelighed (FIT).

2. hvor truslen kan være relevant (applikationer, netværk mv.), hvilket giver en indirekte henvisning til, hvem der skal vurdere truslen.

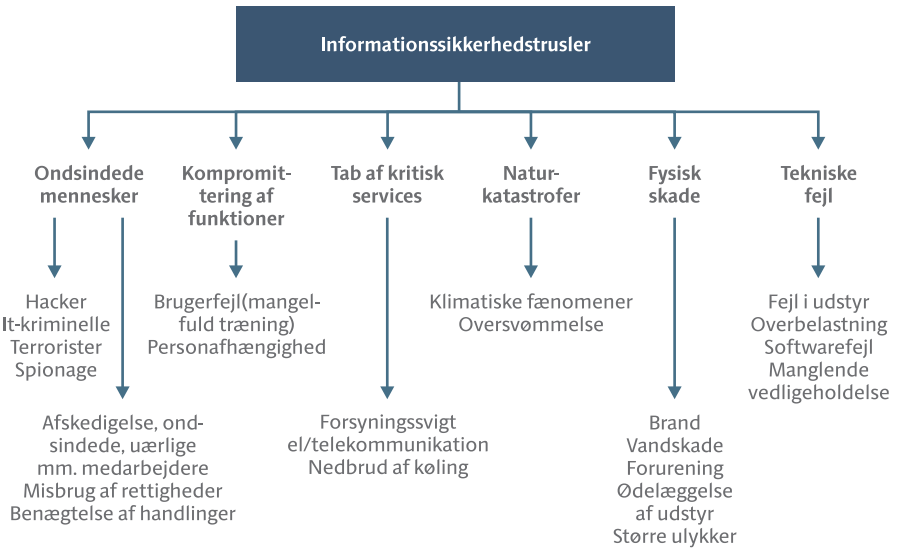
Når man har lagt sig fast på, hvilke trusler der er relevante for kommunen, kan arbejdet med risikovurdering og -håndtering starte.

Dokumentation af risikovurdering og -håndtering
Arbejdet med risikovurdering kan dokumenteres på flere måder.

Man kan vælge at lave spørgeskemaer til brug for konsekvensanalysen og sandsynlighedsanalysen og sende dem til de relevante kontaktpersoner til besvarelse. Har man ikke tidligere arbejdet med risikovurdering anbefales det at lave konsekvens- og sandsynlighedsanalyser via workshops med relevante deltagere.

Uanset hvordan risikovurderingen udføres, vil der være et behov for at dokumentere trusler, sårbarheder, konsekvens, sandsynligheder og handlinger.

› Figur. Eksempel på det trusselsbillede ISO27005 tager udgangspunkt i



Konsekvensanalyse
En del af risikoanalysen er en identifikation af de konsekvenser, som et tab af fortrolighed, integritet og/eller tilgængelighed (FIT) vil medføre for et aktiv, eksempelvis for en forretningsproces. Det er vigtigt at tage udgangspunkt i de forretningsmæssige konsekvenser, dvs. hvilken betydning det vil have for kommunen og borgere som helhed og ikke kun for et afgrænset område. Konsekvenserne kan opdeles i forskellige indvirkninger. Der kan være direkte økonomiske tab, tab af omdømme, indflydelse på serviceniveau mv.

Hvis konsekvensvurderingen resulterer i, at konsekvensen ved sikkerhedsbrud ikke vurderes højere end 2 (mindre alvorlig/generende), kan man overveje ikke at risikovurdere dette aktiv yderligere, da risikoniveauet aldrig vil blive højere end moderat.

Hvis et sikkerhedsbrud har forskellig indvirkning, kan man ligeledes overveje kun at medtage de indvirkninger, der har en konsekvens højere end 2.

Under skabeloner findes et eksempel på en skabelon "Konsekvensanalyse", der kan bruges til konsekvensanalyse i.f.t. FIT. Skabelonen indeholder beskrivelser og vejledning.

Primære deltagere i afdækning af konsekvenser vil typisk være systemejere/sagsbehandlere.

Sandsynlighed (sårbarhed)
Når konsekvensen ved et sikkerhedsbrud er vurderet, skal sandsynligheden for at aktivet rammes vurderes.

Hvis der er lavet konsekvensanalyse på en forretningsproces, vil sandsynlighedsvurderingen ske på de aktiver (eksempelvis it-systemer), som forretningsprocessen anvender.

Ud fra trusselskataloget findes de trusler, der er relevante for aktiverne. Pr. aktiv vurderes sandsynlighed for, at truslerne udnytter en sårbarhed hos aktivet og dermed giver brud på fortrolighed, integritet og/eller tilgængelighed.

En trussel kræver en sårbarhed for at kunne resultere i en risiko og omvendt. Sårbarheder kan for eksempel være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb. En god måde at få afdækket sårbarhederne på er ved at gennemgå de implementerede kontroller og vurdere deres effektivitet. Primære deltagere i afdækning af sårbarheder vil typisk være systemejere.

Når sandsynlighed vurderes kan værdierne fra nedenstående tabel anvendes.

Sandsynlighed	Eksempelbeskrivelse
1. Usandsynligt	Det anset for næsten udelukket, at hændelsen nogensinde kan forekomme › Ingen erfaring med hændelsen › Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark
2. Mindre sandsynligt	Hændelsen forventes ikke at komme › Ingen erfaring med hændelsen › Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark
3. Sandsynligt	Det er sansynligt at hændelsen vil forekomme › Man har erfaring med hændelsen, men ikke indenfor de sidste 12 måneder › Kendes fra andre offentlige og private virksomheder i Danmark (omtales i pressen)
4. Forventet	Det forventes at hændelsen vil forekomme › Man har erfaring med hændelsen, indenfor de sidste 12 måneder › Hænder jævnligt i andre offentlige og private virksomheder i Danmark (omtales ofte i pressen)

Risikolog
Under skabeloner i Yammer findes et eksempel på en "Risikolog", som kan bruges til at dokumentere relevante trusler, sårbarheder, deres indvirkning samt konsekvenser ved et sikkerhedsbrud og sandsynligheden for at det sker.

Primære deltagere i beskrivelse af sandsynlighed vil typisk være systemejere/superbruger

Risikovurdering
Når konsekvens og sandsynlighed for, at en trussel udnytter en sårbarhed, er skrevet ind i risikologgen, beregner risikologgen selv risikoværdien. Risikoværdien vil ligge i intervallet 1-16, hvor værdierne 1-3 vurderes som acceptable, værdierne 4-8 som moderate og værdierne 9-16 som kritiske (nedenstående tabel).

Kan accepteres	Overveje tiltag	Kritisk (der bør ageres)
Risici i det grønne område: Kan accepteres, ingen handlinger er nødvendige	Risici i det gule område: Ledelsen kan beslutte at acceptere risikoen eller overveje at implementere tiltag, der kan reducere risikoen.	Risici i det røde område: Ledelsen bør ikke acceptere risikoen. Skal der lukkes for services, sættes tiltag i værk, eller kan risikoen overføres til tredje part via forsikring?

Håndtering af risici
Sidste skridt i risikovurderingen er en håndtering af de fundne risici i forhold til de kriterier, som er fastlagt af ledelsen.

Håndtering af risici kan ske efter følgende principper (ovenstående tabel):

- Risici i det grønne område: Kan accepteres, ingen handlinger er nødvendige
- Risici i det gule område: Ledelsen kan beslutte at acceptere risikoen eller overveje at implementere tiltag, der kan reducere risikoen.
- Risici i det røde område: Ledelsen bør ikke acceptere risikoen. Skal der lukkes for services, sættes tiltag i værk, eller kan risikoen overføres til tredje part via forsikring?

Den enkelte risikos håndtering opdateres i risikologgen med en beskrivelse af den valgte håndtering:

1. Acceptér (risikoen accepteres, og der foretages ikke yderligere).
2. Flyt (risikoen overføres til en tredjepart, fx ved hjælp af forsikring, outsourcing eller lignende).
3. Undgå (risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen).
4. Kontroller (risikoen kontrolleres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne).

Ligeledes beskrives eventuelle handlinger/kontroller for at minimere risikoen.

Når der udvælges handlinger/kontroller til reducering af risici, skal det ske ud fra en cost/benefitvurdering, så kontrollernes effekt på risikoen vurderes i forhold til omkostningerne.

I forlængelse af risikohåndteringen bør SoA-dokumentet konsulteres. Dækkes eventuelle nye kontroller allerede af de kontroller, der er beskrevet i SoA-dokumentet eller skal der tilføjes nye kontroller?

Sandsynlighed	Risikoværdi			
4. Forventet	4	8	12	16
3. Sandsynligt	3	6	9	12
2. Mindre sandsynligt	2	4	6	8
1. Usandsynligt	1	2	3	4
Konsekvens	1. Ubetydelig	2. Mindre alvorlig	3. Meget alvorlig	4. Graverende/ødelæggende

Grøn = Acceptabel risiko	Gul = Moderat risiko	Rød = Kritisk risiko

06 / TIL- OG FRAVALG – UDARBEJDELSE AF SOA-DOKUMENT

SoA-dokumentet (Statement of Applicability, en formel beskrivelse af udvalgte sikkerhedstiltag) er et lån fra ISO27001, hvor man taler om det i forbindelse med Anneks A.

Arbejdet med SoA-dokumentet er et led i håndteringen af risici. SoA'en, som også kaldes beslutningsdokumentet, bruges til at træffe en række til- og fravalg til håndtering af de risici, der er identificeret gennem risikovurderingen.

Et SoA-dokument består således af en liste med kontroller, der kan være relevante for en kommunen at udføre som led i håndtering af risici. Beskrivelsen skal indeholde begrundelser for, hvorfor visse kontroller evt. er blevet valgt fra.

Det eneste krav til udfyldelsen af SoA er, at det skal indeholde alle nødvendige kontroller til at håndtere risici.

Resultatet af arbejdet med SoA-dokumentet skal godkendes af topledelsen.

Output
SoA-dokument, der indeholder en beskrivelse af de foranstaltninger/kontroller, der skal gennemføres. Beskrivelsen skal indeholde begrundelser for, hvorfor visse kontroller evt. er blevet valgt fra.

Anbefaling
Udarbejdelse af SoA-dokumentet kan foregå enten i workshop- eller interviewform.

Arbejdet ligger i forlængelse af de risici, man har identificeret under risikovurderingen. På baggrund af risikovurderingen besluttes det, hvilke muligheder man har for at håndtere de fundne risici, samt hvilke foranstaltninger man vil implementere.

Det er vigtigt, at en organisation identificerer sine sikkerhedskrav. Der er tre hovedkilder til sikkerhedskrav, som kan give anledning til at etablere kontroller:

- Vurdering af risici i organisationen, idet der tages højde for organisationens overordnede forretningsstrategi og målsætninger.
- Lov-, myndigheds- og kontraktkrav, som en organisation, dens handelspartnere, leverandører og serviceudbydere skal opfylde.
- Best Practice – Sæt af principper, målsætninger og forretningskrav til informationshåndtering, -behandling, -lagring, -kommunikation og -arkivering, som en organisation har udviklet for at understøtte driften.

Anneks A i ISO27001 indeholder 114 sikkerhedskontroller, der kan bruges som inspiration eller anvendes som tjekliste, for at sikre at relevante sikkerhedskrav er taget med.

Husk at Anneks A ikke er udtømmende. Der kan være andre sikringsforanstaltninger og kontroller, som er relevante at få med i SoA-dokumentet.

Anneks A kontrollerne kan med fordel gennemgås inden risikovurderingen starter, for at vurdere compliance i.f.t. disse og dermed finde områder, der bør prioriteres.

Valg af kontroller afhænger også af den måde, hvorpå kontrollerne supplerer hinanden og derved samlet udgør et solidt værn til beskyttelse af organisationens informationssikkerhed.

En kontrol kan fravælges ud fra den begrundelse, at den ikke er relevant eller at risikoen ved at fravælge den accepteres, undgås eller overføres til en tredje part.

Det udarbejdede SoA-dokuments tilvalg indgår som grundlag for handlingsplaner for konkrete aktiviteter, der skal implementere sikkerhedsforanstaltningerne.

I SoA skabelonen findes der to ark med hver sit eksempel på et SoA-dokument:

- SoA Radardiagram
  Her kan implementeringsgrad og ønsket implementeringsgrad i.f.t. Anneks A's 114 kontroller samt eventuelle egne kontroller kan angives. Skabelonen kan generere et radardiagram som viser implementeringsgraden i forhold til den ønskede implementeringsgrad.

- SoA Status
  Her kan status i.f.t. implementeringen af Anneks A's 114 kontroller angives. Status vises med farvemarkeringer.

Begge skabeloner kan bruges hvis man ønsker at controllere compliance i.f.t. Anneks A's 114 kontroller inden arbejdet med risikovurdering startes samt til løbende status.

07 / HVORDAN UNDERSTØTTER ISO27001 EFTERLEVELSEN AF DATABESKYTTELSESFORORDNINGEN?

Med de nye regler i databeskyttelsesforordningen lægges der op til en risikobaseret tilgang til kommunernes sikkerhedsarbejde. Udgangspunktet er, at behandling af personoplysninger er forbundet med risici for fysiske personers rettigheder og frihedsrettigheder, og der skal derfor etableres et sikkerhedsniveau, der passer til de risici, som behandlingen udgør.

Her ses navnlig på risici som hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Når Justitsministeriets vejledninger til databeskyttelsesforordningen kommer, vil afsnittet blive udbygget.

Dette sker når version 2 af dette materiale frigives ultimo 2017.

ORDBOG

Aktiv
Ordet aktiver anvendes, som et fælles begreb for forretningsprocesser, it-systemer, teknisk infrastruktur, servere, pc'er etc. (Udtrykket stammer fra ISO27001).

Anneks A
Anneks A er en del af ISO27001 og indeholder 114 sikkerhedskontroller, der kan bruges som inspiration eller anvendes som tjekliste, for at sikre at relevante sikkerhedskrav er taget med i betragtning. Anneks A omtales ofte som SoA-dokumentet.

Dataejer
En chef/leder som har dispositionsret til data og ansvar for behandling af data. Dataejer kan også være systemejer. Se desuden "En rejsefortælling om funktioner, roller og ledelse" hvor roller og opgaver for en data/systemejer er beskrevet.

FIT
Der bør altid gennemføres en konsekvensvurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed (FIT). Med fortrolighed menes, at uvedkommende får adgang til data, som de ikke burde have adgang til. Med integritet menes, at data, f.eks. i et system, er de rigtige, og at man kan træffe beslutninger på baggrund af dette. Med tilgængelighed menes, at man i organisationen kan tilgå nødvendige data.

Fællesfortegnelser
Som et led i arbejdet med databeskyttelsesforordningen har KL påtaget sig opgaven med at udarbejde fællesfortegnelser, der er dækkende for alle kommunale behandlingsaktiviteter.

ISO27001
ISO27001 standarden er udarbejdet med det formål at opstille krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS).

Konsekvens
En del af risikoanalysen er en identifikation af de konsekvenser, som et tab af fortrolighed, integritet og/eller tilgængelighed vil medføre for et aktiv. Der kan være direkte økonomiske tab, tab af omdømme, indflydelse på serviceniveau mv.

Risiko
En risiko kan opstå, hvis en trussel udnytter en sårbarhed, eksempelvis en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb.

Risikoejer
Risikoejer vil ofte være den, der har det økonomiske ansvar for risikoen. Kan eksempelvis være systemejer eller kontraktansvarlig.

Risikologgen
I risikologgen kan relevante trusler, sårbarheder, deres indvirkning samt konsekvenser ved et sikkerhedsbrud beskrives. Ligeledes beskrives hvordan risikoen håndteres/kontrolleres, hvis risikoniveauet er højere end den grænse der er fastlagt.

Risikoprofil
Det fastlagte niveau for hvornår risici er acceptable. Niveauet i accept af risici kan hos informationssikkerhedsudvalget lægges forskelligt for eksempelvis økonomiske risici i forhold til risici på liv/ære/velfærd området. Det samlede billede af risikovillighed udgør organisationens risikoprofil.

Risikovurdering
Risikovurdering handler om at identificere og analysere mulige trusler, sårbarheder overfor truslerne og sandsynligheden for de kan opstå samt tilhørende konsekvenser i forhold til risikoen for tab af fortrolighed, integritet og tilgængelighed.

Sandsynlighed
Når en trussel vurderes, vurderes sandsynligheden for at truslen udnytter en sårbarhed og dermed giver brud på fortrolighed, integritet og/eller tilgængelighed.

SoA
SoA står for 'Statement of Applicability'. SoA-dokumentet er en formel beskrivelse af udvalgte sikkerhedstiltag der udføres som et led i håndteringen af risici. SoA'en kaldes også beslutningsdokumentet og består konkret af en liste med kontroller.

Systemejer
En chef/leder, der er ansvarlig for et eller flere systemer. Se desuden "En rejsefortælling om funktioner, roller og ledelse" hvor roller og opgaver for en systemejer er beskrevet.

Sårbarhed
En trussel kræver en sårbarhed for at kunne resultere i en risiko og omvendt. Sårbarheder kan være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb.

Trusler
Identifikationen af relevante trusler er afgørende for, at man ikke overser risici. Derfor bør trusselsvurderingen ske på en systematisk måde. Der findes meget omfattende trusselskataloger, som indeholder enhver tænkelig situation, men man kan også anvende mere generiske kataloger. Ifølge National strategi for cyber- og informationssikkerhed er det et krav, at cyber trusler også indgår i myndighedernes risikovurderinger og risikoledelse. Eksempler på trusler kan være hackerangreb, oversvømmelse, menneskelige fejl eks. deling af fortrolige oplysninger via mail, servernedbrud, spionage etc.

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne
facebook.com/kommunerne

Produktionsnr. 830261
ISBN 978-87-93365-92-6-pdf