FREDENSBORG
KOMMUNE

Risikostyring

Fredensborg Kommune

Indhold

Baggrund

Risikovurderingerne er et praktisk værktøj til at identificere hvilke forhold og sårbarheder ved et system/aktiv/proces, der kræver overvågning eller handling og derved et beslutningsgrundlag for styring og prioritering af informationssikkerhedsarbejdet ud fra et risikobaseret grundlag.

Ifølge databeskyttelsesforordningens artikel 32 skal den dataansvarlige etablere passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der imødegår de risici, som behandlingen måtte medføre for de registrerede (borgere eller medarbejdere).

Risikoen måles ved at bedømme, hvor stor sandsynligheden er for, at en trussel vil kunne påvirke en sårbarhed, og hvor store konsekvenser det kan have. Der skelnes mellem konsekvenser for kommunen og for den registrerede (GDPR).

Risikovurderingen bør ikke kun omfatte it-systemer, men alle aktiver som f.eks. processer, netværksudstyr (routere, switche, firewalls mv.), papirarkiver, medarbejdere, immaterielle aktiver mv. Aktiverne kan med fordel grupperes efter deres type.

Fortrolighed, integritet og tilgængelighed (FIT)
Brud på *fortrolighed* handler om at data mister sin beskyttelse, og fremmede/uvedkommende får adgang til data, som de ikke burde have adgang til. Eksempler på brud:

- En bruger for ved en fejl adgang til en mappe på et fildrev, en sag eller et system, som personen ikke burde have adgang til, og dermed til data som personen ikke burde have 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.

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:

- Der bliver indlæst gamle (ugyldige data ind i et system, således at data ikke længere er de seneste nye - og der dermed træffes beslutninger på et forkert grundlag.
- Udefrakommende hacker sig ind på kommunens pc'er og foretager ændringer i it-systemer med personoplysninger eller i dokumenter indeholdende personoplysninger lagret på eksempelvis et drev på en PC.
- Et regneark bliver overskrevet med en gammel version, og er dermed ikke længere er korrekt.

Tilgængelighed (tilgængelighed er nede i ½ dag, 1 dag, 3 dage, en uge eller mere) handler om, at man kan få adgang til data. Eksempler på brud:

- Systemer er brudt ned, og data er dermed ikke tilgængelige.
- Der er journaliseret forkert - dvs. at dokumenter er lagt på en forkert sag, og dermed ikke tilgængelige.
- 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.

Risikostyringsprocessen

Etablering af kontekst

Hvem er vi? Hvad er kerneforretningen og prioriteter? Hvilken samfundskontekst opererer vi i?

I denne fase skal den organisatoriske, fysiske og tekniske afgrænsning af risikovurderingerne fastsættes. Der udpeges roller og ressourcer, defineres kriterier for risikotolerence og beskrives en metode for risikovurderingen.

Risikovurdering

Risikovurderingen er omdrejningspunktet i risikostyringen. Her identificeres, analyseres og evalueres risici med udgangspunkt i den definerede kontekst. Resultatet af risikovurderingen er en liste over risici, som er prioriteret i forhold til de foruddefinerede kriterier (fx organisationens strategi eller systemets eller datas kritikalitet).

Der skal altid laves en vurdering af risikoen for tab af fortrolighed, integritet og tilfældighed (FIT).

Risikohåndtering

Der er fire muligheder for at håndtere risici: 1. Kontrollér (risikoen styres ved at indføre kontroller eller foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne). 2. Acceptér (risikoen accepteres, og der foretages ikke yderligere). 3. Undgå (risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen). 4. Flyt (risikoen overføres til en tredjepart, fx ved hjælp af forsikring, outsourcing eller lignende).

Som en del af risikohåndteringen udarbejdes en risikohåndteringsplan, som ud fra ovennævnte muligheder beskriver, hvordan de identificerede risici skal håndteres.

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

Risikoaccept

For kritiske aktiver bør risikoaccepten altid foretages af den øverste ledelse.
Selvom risici kontrolleres ved at indføre yderligere kontroller, vil der i de fleste tilfælde altid være en restrisiko. Det er vigtigt, at der i risikohåndteringsplanen foretages en vurdering af de valgte kontrollers effekt på risikoen, og at den tilbageværende risiko vurderes og beskrives.

Opfølgning på risici

Der bør løbende foretages opfølgning på risici. Det bør sikres, at de kontroller og tiltag, der indføres som en del af risikohåndteringen rent faktisk også bliver implementeret og fungerer efter hensigten. Der bør løbende følges op på de forudsætninger, som ligger til grund for risikovurderingen. Aktiver, trusler, sårbarheder og konsekvenser kan hurtigt ændres og medfører tilsvarende ændringer i risikobilledet.

Risikovurderinger i Fredensborg Kommune

Roller og ansvar
Ansvaret for gennemførsel af risikovurderingen er placeret hos det fagcenter, der har ansvaret for det aktiv, der risikovurderes (fx systemejeren). Det er således fagcentrets ansvar at inddrage GDPR-teamet ved bl.a. it- nyanskaffelser eller opstart af nye processer. GDPR-nøgleperson(er) i fagcentret faciliterer arbejdet med risikovurderinger i det konkrete center, og sikrer at alle relevante parter bliver involveret. GDPR-teamet bistår med rådgivning og sparring til arbejdet med risikovurderinger.

Fagcentret spiller en central rolle i vurderingen, da det er repræsentanter herfra, der skal foretage vurderingerne og sørge for, at der er tilstrækkelig information om systemet til at anbefale sikkerhedsforanstaltninger.

Beslutningen om, hvilke af anbefalingerne der skal følges og implementeres, ligger hos systemejer/risikoejeren. Risikoejeren er typisk den person, som en risikohændelse vil have en direkte konsekvens for, og dermed har ansvaret for at risikoen håndteres. Risikoejeren indstiller til ledelsen om en risiko bør accepteres eller nedbringes/reduceres. Ansvaret for udarbejdelse af risikohåndteringsplan ligger dermed også hos risikoejer. Risikoejer kan være centerchefen, teamleder, en systemansvarlig, projektejer, direktør mv., afhængigt af risikoen.

Metode

Risikovurderinger udarbejdes i Wired Relations.

Konsekvensvurdering
Konsekvensvurderingen har til formål at afdække, hvilke konsekvenser et brud på hhv. fortroligheden, integriteten og tilgængeligheden (FIT) vil have i relation til en række forskellige konsekvenstyper, f.eks. økonomi, registrerede personer, kommunens evne til at nå strategiske mål mv. FIT er omdrejningspunktet for informationssikkerhedsarbejdet, og er derfor de centrale områder, informationssikkerheden italesættes ud fra.

Der gennemføres både en konsekvensvurdering fra kommunens perspektiv og fra de registreredes perspektiv.

Konsekvenstyper og skala for vurdering af konsekvenser for Fredensborg Kommune:

Konsekvens-beskrivelse	Medfører økonomiske meromkostninger eller tab for kommunen	Medfører administrative belastninger for kommunen	Påvirker kommunen omdømme negativt	Medfører indskrænkninger i kommunens evne til at handle i en periode	Påvirker kommunens forhold til interessenter	Medfører brud på lovgivning, fx forvaltningslov og straffelov
Ubetydelig (uvæsentlig) Score: 1	Ingen særlig påvirkning	Ingen særlige påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning
Begrænset (generende) Score: 2	Meromkostninger og tab i begrænset niveau, som kan kræve mindre budgetændringer	Håndteres inden for rimeligt ekstra administrativt ressourcetræk	Forbigående opmærksomhed fra enkelte grupper	Planlagte aktiviteter kan gennemføres med mindre justeringer	Forringet samarbejde med interessenter i enkeltsager	Manglende overholdelse af administrative procedurer og regler, som ikke er af kritisk karakter
Væsentlig (kritisk) Score: 3	Store økonomiske tab med risiko for at blive sat under administration	Der må trækkes væsentligt på eksisterende og nye administrative ressourcer	Offentligheden fatter generel negativ interesse for organisationen	Medfører revurdering af vigtige aktiviteter	Generelt forringet samarbejde med interessenter	Lovbrud, der er kritiske og kan stille ministeriet i miskredit
Maksimal (uacceptabelt) Score: 4	Væsentlige økonomiske tab. Bliver sat under administration	Eksisterende og nye administrative ressourcer er ikke tilstrækkelige	Væsentlig skade på omdømme. Der vil være personale- og ledelsesmæssige konsekvenser	Bliver ude af stand til at gennemføre vigtige aktiviteter. Der vil være personale- og ledelsesmæssige konsekvenser	Væsentligt nedbrud i det generelle samarbejde med interessenter	Brud på kritisk lovgivning, fx straffeloven brydes. Der vil være personale- og ledelsesmæssige konsekvenser

Konsekvenstyper og skala for vurdering af konsekvenser for de registrerede:

Konsekvens-beskrivelse	Forskelsbehand-ling, Skade på om-dømme, Sociale konsekvenser, Ind-flydelse på privat-liv, Skade på men-neskelig værdighed	Materiel skade, Identitetstyveri, Identitetssvig, Økonomiske kon-sekvenser, Finan-sielle tab, Skade på legitime inte-resser	Immateriel skade, Fysisk skade, Skade på liv, psyke og helbred	Begræns-ning/krænkelse af fundamentale rettigheder og frihedsrettighe-der	Beskyttelsen af børns privatliv forringes
Ubetydelig (uvæsentlig) Score: 1	Ingen særlig på-virkning	Ingen særlig på-virkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig på-virkning
Begrænset (generende) Score: 2	Registreredes ek-sponeres internt for uautoriserede	Registrerede op-lever ingen sær-lige eller mindre materielle tab.	Registrerede udsættes for fysiske og/el-ler psykiske helbredsmæs-sige gener i mindre grad – intet alvorligt	Registreredes fundamentale rettigheder for-ringes. Regi-strerede kan ikke gøre brug af sine rettighe-der i en kortere periode.	Børn eksponeres internt for uauto-riserede. Foræl-dres kontrol over barnets oplysnin-ger forringes. Børn kan udsæt-tes for helbreds-mæssige gener - intet alvorligt.
Væsentlig (kritisk) Score: 3	Registreredes ek-sponeres på en måde, som skader de sociale relatio-ner, såvel internt blandt kollegaer og eksternt uden for organisation. Registreredes fra-tages potentielt retten til at være anonym.	Registrerede op-lever alvorlige materielle tab.	Registrerede fysiske og/el-ler psykiske helbred eller fysiske sikker-hed påvirkes	Registreredes fundamentale rettigheder for-ringes. Regi-strerede kan ikke gøre brug af sine rettighe-der i en læn-gere periode.	Børn eksponeres på en måde, som ikke tjener den registrerede, og kan blive ekskl u-deret fra sociale netværk. Foræl-dres kontrol over barnets person-oplysninger fra-tages. Børns hel-bred påvirkes
Maksimal (uaccepta-belt) Score: 4	Væsentlig skade på registreredes ry/omdømme, der kan føre til store sociale tab. Regi-strerede fratages muligheden for at være anonym, da fortroligheden af data mistes.	Væsentlige mate-rielle tab, der på-virker registrere-des livssituation væsentligt	Registreredes udsættes for fundamental helbredsmæs-sig fare. Regi-streredes fysi-ske sikkerhed er i fare. Men-neskeliv kan stå på spil.	Registrerede mister helt mu-ligheden for at gøre brug af sine rettighe-der.	Børn lider væ-sentlig skade på omdømme, der kan føre til soci-ale tab. Børns helbred er i fun-damental fare.

Trussels-, sårbarheds- og sandsynlighedsvurdering
Trusselvurderingen skal afdække, hvilke relevante trusler der er rettet mod det pågældende system.

Vurderingen tager udgangspunkt i Fredensborg Kommunens trusselskatalog (se nederst i dokumentet, findes også i Wired Relations) og deltagernes eventuelle input til relevante trusler. Truslerne kan bl.a. være cyberangreb, leverandørsvigt, tilsigtet læk, mv.
Trusselskataloget er et dynamisk dokument, som ændrer sig løbende, i takt med at nye trusler identificeres. Det er ikke et udtømmende dokument, men skal betragtes som inspiration og forslag til en udvælgelse af relevante trusler. Truslerne kan variere fra system til system.

Når de relevante trusler er identificeret, vurderes det dernæst om systemet eller kommunen er sårbar over for disse. Trusler udnytter sårbarheder, og bliver dermed først realiseret, såfremt omstændighederne tillader det.

Sårbarhederne og truslerne kan dog ikke stå alene, da det er nødvendigt at vurdere, hvorvidt det er sandsynligt, at sårbarheden udnyttes og truslen dermed realiseres. Sandsynligheden for at en hændelse indtræffer kan være svær at vurdere, da det er en hypotetisk vurdering. I vurderingen kan man dog medtage faktorer såsom konkret erfaring med hændelsen (om hændelsen er indtruffet før, eller at systemet ofte udsættes for en bestemt type angreb), det nationale trusselsbillede (udgives af Center for Cybersikkerhed), hvori der gives en indikator på, hvor høj truslen er for fx cyberangreb for offentlige myndigheder. Endelig kan man ud fra typen af data i systemet vurdere om det er sandsynligt, at der skulle indtræffe en hændelse. Har data værdi for fx fremmede magter, andre virksomheder eller hackere, er sandsynligheden for et angreb formentlig højere end ellers. Hvis der tillige er en sårbarhed tilstede, der gør det muligt at få succes med angrebet, er sandsynligheden for at hændelsen indtræffer dermed høj.

Sandsynlighed	Eksempelbeskrivelse
Meget usandsynligt Score: 1	Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme - Ingen erfaring med hændelsen - Kendes kun få tilfælde fra offentlige og private virksomheder
Ret sandsynligt Score: 2	Hændelsen forventes ikke at komme - Mindre erfaring med hændelsen - Kendes til tilfælde fra offentlige og private virksomheder
Sandsynligt Score: 3	Det er sandsynligt, at hændelsen vil forekomme - Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder - Kendes fra offentlige og private virksomheder (omtales årligt i pressen)
Neget sandsynligt Score: 4	Det forventes, at hændelsen vil forekomme - Man har erfaring med hændelsen inden for de sidste 12 måneder - Hænder jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen)

Risikoscore og -villighed

		Konsekvens			
		Ubetydelig (1)	Begrænset (2)	Væsentlig (3)	Maksimal (4)
Sandsynlighed	Meget sandsynligt (4)	Under middel Score: 4	Middel Score: 8	Høj Score: 12	Høj Score 16
	Sandsynligt (3)	Lav Score: 3	Middel Score: 6	Middel Score: 9	Høj Score: 12
	Ret sandsynligt (2)	Lav Score: 2	Under middel Score: 4	Middel Score: 6	Middel Score: 8
	Meget usandsyn-ligt (1)	Lav Score: 1	Lav Score: 2	Lav Score: 3	Under middel Score: 4

Lav – under middel: Bør ikke give anledning til yderligere behandling
Middel: Bør give anledning til overvågning eller håndtering
Høj: Bør håndteres med det samme

Trusselskatalog

Trussel
Trusler mod de fysiske omstændigheder
Brandskade, brand i tilstødende omgivelser, brand forårsaget af forsømmelse
Vandskade, skybrud der fører til oversvømmelse, sprinklersystemfejl, rørskade
Elektromagnetisk beskadigelse, lynnedslag, solstorm, statisk elektricitet
Skade ved naturhændelse, kraftig storm, jordskælv, frost, tørke,
Skade ved katastrofal ulykke. Fly-, tog- eller køretøjsulykke, eksplosion
Forurening af faciliteter, radioaktivt udslip fra atomulykke, biologisk eller kemisk udslip, gasudslip, luftbårne partikler, vulkansk nedfald
Fejl i fysisk miljøstyring
Kølingsfejl, luftfiltreringsfejl, opvarmningsfejl
Vandforsyningssvigt
El-forsyningsfejl
Strømsvigt, el-forsyningslinjebrud
Strømfluktuation, sag, surge, spike, brownout
Forsyningsudstyrssvigt, UPS-fejl, generatorfejl
Elforsyningsoverbelastning
Brugerfejl
Uforsætlige brugerhandlinger, fejlbehandling af medier, mangel på brugeruddannelse
Drifts- eller vedligeholdelsesfejl
Fejl i forbindelse med drifts-, support- eller vedligeholdelsesprocesser.
Angreb med skadelig kode
Virus, malware, ransomware, rootkits, ondsindende links og trojanske heste
Cyberangreb
Destruktiv hacking, hacktivisme
DDoS- eller SPAM-angreb
Statsfinansierede angreb (State-sponsored attacks = APT)
Forfalskning af informationer, ødelæggelse af websites

Hacking, industrispionage, aflytning, opsnapning af information
Kapacitetsfejl
Kapacitetsmangel for systemer eller storage
Softwarefejl
Softwarenedbrud, bugs, databasekorruption
Uautoriseret eller ikke-testet kode
Hardwarefejl
Kommunikationslinjenedbrud
Udstyrsnedbrud eller -defekt, slid, korrosion, henfald af lagringsmedier
Misbrug
Forfalskning, svindel, underslæb
Uautoriseret brug, misbrug af rettigheder
Brud på ophavsrettigheder
Tilsigtet informationslæk eller -tyveri
Hacking, industrispionage, aflytning, opsnapning af information
Tyveri af datamedier eller fysiske dokumenter
Politisk eller økonomisk motiveret informationslæk
Utilsigtet informationslæk
For vidtgående brugerrettigheder/adgangsprivilegier
Forkert konfigureret adgangskontrol
Fejlagtig publicering af data, der indeholder følsomme oplysninger
Tab af datamedier eller fysiske dokumenter
Bevidst ødelæggelse af aktiver
Brandstiftelse, hærværk
Terrorbombning
Sabotage begået af hævngerrige medarbejdere
Tyveri af fysiske aktiver
Indbrud, røveri
Tyveri, tricktyveri
Tyveri begået af ansatte
Manglende overholdelse af lovkrav og aftaler
Brud på ophavsrettigheder
Virksomheden opfylder ikke de gældende compliance-krav
Forkert offentliggørelse af personlige oplysninger

Videnstab
Afskedigelse, opsigelse, rekruttering fra konkurrenter
Manglende vidensoverførsel
Personafhængighed
Tab af personale (ressourcetab)
Vold, bortførelse, mord
Dødsulykke eller alvorlige skader
Sygdom, epidemi, pandemi
Arbejdsafbrydelse
Lokale arbejdskonflikter, strejke, lockout
Leverancesvigt
Konkurs, nedlæggelse
Serviceleverandørfejl, hostingleverandørfejl
Afvigelse fra aftalt serviceniveau/leverede ydelser
Ændringer af servicen, en ny strategi fra leverandøren
Fejl hos underleverandører, dårlig håndtering af underleverandører
Sikkerhedsbrud fra leverandørens side
Utilstrækkelig sikkerhed fra leverandørens side
Leverandørafhængighed
Ikke-standardløsninger, afhængighed af leverandørs infrastruktur, dårlige muligheder for dataeksport
Lange kontraktsperioder, høj pris for at afbryde samarbejdet
Leverandør mangler compliance- eller governance-procedurer
Leverandøren opfylder ikke egen sikkerhedspolitik og -regler
Leverandøren opfylder ikke compliance-krav jf. kontrakten
Nye og ubehandlede sikkerhedstrusler
Nye angrebsformer
Nye former for misbrug af it-systemer