

Generel inddeling i risikogrupper for alle myndigheder



Indhold

Introduktion	1
Koncept for inddeling i risikogrupper	1
Præsentation og illustration af risikogrupper	2
Inddeling i niveauerne "almindeligt" og "højt"	3
Præsentation af de fire risikogrupper samt grundlæggende krav	4
Risikogruppe A (Høj fortrolighed, høj tilgængelighed):	4
Risikogruppe B (Høj fortrolighed, alm. tilgængelighed):	4
Risikogruppe C (Alm. fortrolighed, høj tilgængelighed):	5
Risikogruppe D (Alm. fortrolighed, alm. tilgængelighed):	5
Vejledning til inddeling i risikogruppe	6
Trin 1: Vurder behovet for høj tilgængelighed	6
Trin 2: Vurder behovet for høj fortrolighed	6
Trin 3: Fastlæg risikogruppen	6

Introduktion

Denne vejledning skal hjælpe offentlige myndigheder med at indplacere sig i en risikogruppe på baggrund af myndighedens vurderede sikkerhedsprofil. Indplaceringen kan indgå som del af myndighedens risikostyring. Risikogrupperne skal anvendes ved brug af nogle af Styrelsen for Samfundssikkerheds vejledninger, hvor sikkerhedsanbefalinger er tilpasset de forskellige risikogrupperes sikkerhedsbehov.

Vejledningen består af følgende dele:

- En beskrivelse af risikogrupperne
- Vejledning i, hvordan myndigheden kan udpege sin risikogruppe

Offentlige myndigheder adskiller sig betydeligt fra hinanden i deres arbejdsopgaver, forretningsbehov og hensyn. Nogle myndigheder behandler for eksempel mere beskyttelsesværdige informationer end andre, og konsekvenserne af et systemnedbrud kan være langt mere kritiske for visse myndigheder end for andre. Da myndigheder ikke har ensartede behov, er det vigtigt, at myndighederne er i stand til at vælge de foranstaltninger, der løfter dem til det nødvendige niveau af sikkerhed for deres organisation.

Formålet med indplacering i risikogruppe er at understøtte myndighederne i at træffe kvalificerede, risikobaserede valg, når de skal træffe sikkerhedsmæssige beslutninger. Indplaceringen er således en guide eller en rettesnor, når organisationens sikkerhedsorganisation skal træffe beslutning om konkrete foranstaltning. Det er dog nødvendigt, at organisationen altid har for øje, at der kan være tilfælde, hvor de har et højere sikkerhedsbehov, end deres umiddelbare indplacering tilsiger.

Koncept for inddeling i risikogrupper

I dette afsnit beskrives det overordnede koncept for inddeling i risikogrupper. Offentlige myndigheder skal vurdere deres sikkerhedsprofil og på den baggrund placere sig i én af fire risikogrupper. Myndigheden bør revurdere indplaceringen, hvis myndighedens behov ændres. Placering bør som udgangspunkt ske på myndighedsniveau, men der kan være forskellige dele af organisationerne fx en særligt forvaltning ol, der tilsiger et andet niveau end det, som gælder for resten af myndigheden.

Vurdering af sikkerhedsprofil

Under konceptet skal en myndigheds sikkerhedsprofil vurderes ud fra to behov – behov for beskyttelse mod uautoriseret adgang (fortrolighed) og behov for sikring af stabil, kontinuerlig og robust drift (tilgængelighed). Det vil sige, at de enkelte myndigheders behov for beskyttelse af fortrolighed og tilgængelighed danner grundlaget for myndigheders sikkerhedsprofil. Der differentieres ikke på baggrund af integritet og autenticitet, da konceptet tager udgangspunkt i, at danske myndigheder vurderes at have det tilnærmelsesvis samme høje behov for, at information ikke manipuleres eller ændres. Dette skyldes bl.a., at et brud på integritet i én myndighed vil kunne skabe mistillid for integriteten af andre myndigheder. Der kan dog være tilfælde, hvor enkelte myndigheder har et særligt behov for integritet eller autenticitet af data. I de tilfælde vil myndigheder skulle lave en risikovurdering af behovet som tillæg til deres anvendelse af ovenstående risikogruppering.

Præsentation og illustration af risikogrupper

Konceptet opdeler myndigheder i fire risikogrupper (A-D) ud fra deres behov for henholdsvis fortrolighed og tilgængelighed. De forskellige risikogrupper tager på den måde højde for forskellige typer af sikkerhedsbehov og -hensyn. Figur 1 nedenfor illustrerer grupperingen.

Figur 1 : Opdeling i risikogrupper ud fra behov for fortrolighed og tilgængelighed.



Den vandrette akse angiver myndighedens behov for tilgængelighed. Placering i forhold til tilgængelighed skal baseres på, om myndigheden har samfundskritiske it-systemer¹ eller varetager samfundskritiske funktioner², som er afhængige af systemunderstøttelse.

Den lodrette akse angiver myndighedens behov for fortrolighed. Placering i forhold til fortrolighed skal bygge på, om:

- myndigheden håndterer informationer klassificeret FORTROLIGT eller højere
- myndigheden er særligt udsat for spionage³
- myndigheden behandler følsomme, fortrolige eller kritiske informationer, og hvor uautoriseret adgang kan skade enkeltpersoner, myndighedens funktion, eller nationale interesser

¹ Se evt. definition for samfundskritiske it-systemer fra Økonomistyrelsens "Vejledning til model for porteføljestyring af statslige it-systemer"

² For overblik over samfundsvigtige funktioner læs "Bilag 1 – Samfundsvigtige funktioner", fra "Strategi for forsyningssikkerhed"

³ Myndigheder kan tage udgangspunkt i "Spionagetruslen mod Danmark, Færøerne og Grønland" fra PET, samt Cybertruslen mod Danmark 2025. SAMSIK udgiver også løbende sektorspecifikke trusselsvurderinger af cybertruslen mod Danmark – læs mere på samsik.dk/kategori/trusselsvurderinger/

Inddeling i niveauerne "almindeligt" og "højt"

Placering i risikogrupper er baseret på opdeling af myndigheders behov for fortrolighed og tilgængelighed (sikkerhedsprofil) i to niveauer hhv. "almindeligt" og "højt". De to niveauer skal forstås ud fra følgende kriterier:

Tilgængelighed:

- *Almindeligt behov:*
 - Systemer og funktioner kan tåle afbrydelser uden væsentlig påvirkning af samfundets funktioner
 - Fejl og nedbrud medfører primært interne driftsforstyrrelser, men truer ikke samfundskritiske funktioner
- *Højt behov:*
 - Systemer og funktioner er nødvendige for samfundets videreførelse, borgernes sikkerhed eller opretholdelse af kritiske offentlige ydelser
 - Nedbrud kan påvirke liv, sundhed, væsentlig infrastruktur eller finansiell stabilitet

Fortrolighed:

- *Almindeligt behov:*
 - Uautoriseret adgang medfører ikke væsentlig skade for borgere, myndighedens funktioner eller nationale interesser
 - Informationer kan omfatte almindelige personoplysninger, herunder GDPR, interne dokumenter og ikke-følsomme systemdata
- *Højt behov:*
 - Uautoriseret adgang kan medføre væsentlig skade for enkeltpersoner, myndighedens funktion eller nationale interesser
 - Informationer omfatter både store mængder personoplysninger og/eller følsomme personoplysninger samt sikkerheds- eller beredskabsrelevante informationer, eksempelvis klassificeret materiale

Præsentation af de fire risikogrupper samt grundlæggende krav

De statslige myndigheder har – uanset indplacering – krav om at efterleve de tekniske minimumskrav til statslige myndigheders it-sikkerhed. Disse krav har til formål at sikre et fælles højt it-sikkerhedsniveau i staten. Disse krav vurderes løbende således, at kravene følger med den teknologiske udvikling og udviklingen i trusselsbilledet. Dertil kommer krav om at arbejde efter ISO 27001 og for nogle myndigheder kravene i NIS 2-loven.

Det gælder for alle myndigheder, at man skal anlægge en risikobaseret tilgang til sikkerhedsarbejdet. Det vil for NIS2-loven sige, at der skal implementeres de foranstaltninger (tekniske, operationelle og organisatoriske), der vurderes nødvendige for at opnå et passende sikkerhedsniveau. Foranstaltningerne skal dog som minimum omfatte de foranstaltninger, der er beskrevet i NIS 2-loven.

Risikogruppe A (Høj fortrolighed, høj tilgængelighed):

Gruppe A omfatter myndigheder, der har en sikkerhedsprofil med særlige krav til både fortrolighed og tilgængelighed. Det vil sige, at denne placering anvendes, hvor behovet for fortrolighed og tilgængelighed er omfattet af kriterier for "højt behov".

Myndigheder i denne kategori håndterer særligt beskyttelsesværdige informationer, herunder fx informationer vedrørende udenrigs- og sikkerhedspolitik, og det har store konsekvenser, hvis myndighedens systemer eller data bliver utilgængelige eller lækkes – selv i kortere perioder og i mindre omfang.

Eksempelvis kan det være organisationer med ét eller flere (samfunds)kritiske it-systemer, der derudover håndterer store mængder klassificeret materiale, og hvor truslen mod organisationen fra f.eks. cyberkriminalitet og spionage vurderes at være særligt høj. Disse myndigheders vigtigste sikkerhedsbehov ligger derfor i at beskytte data mod uautoriseret adgang samt sikre stabil, kontinuerlig og robust drift af systemer.

Risikogruppe B (Høj fortrolighed, alm. tilgængelighed):

Gruppe B omfatter myndigheder, der har en sikkerhedsprofil med særlige krav til fortrolighed. Det vil sige, at denne placering anvendes, hvor behovet for fortrolighed er højt, men hvor behovet for tilgængelighed som udgangspunktet er omfattet af kriterier for "almindeligt behov".

Myndigheder i denne kategori håndterer primært beskyttelsesværdige informationer, herunder fx informationer vedrørende udenrigs- og sikkerhedspolitik. Her er behov for høje beskyttelseskrav, men systemer kan tåle driftsafbrydelser uden at true samfundskritiske funktioner. Disse myndigheders vigtigste sikkerhedsbehov ligger derfor i at beskytte data mod uautoriseret adgang.

Risikogruppe C (Alm. fortrolighed, høj tilgængelighed):

Gruppe C omfatter myndigheder, der har en sikkerhedsprofil med særlige krav til tilgængelighed. Det vil sige, at denne placering anvendes, hvor behovet for tilgængelighed er højt, men hvor informationer hos myndigheden som udgangspunkt er dækket af kriterier for "almindeligt behov".

Myndigheder i denne kategori håndterer primært ikke-beskyttelsesværdige informationer, men har systemer, som varetager samfundskritiske funktioner, der ikke tåler nedbrud. Disse myndigheders vigtigste sikkerhedsbehov ligger derfor i at sikre stabil, kontinuerlig og robust drift.

Risikogruppe D (Alm. fortrolighed, alm. tilgængelighed):

Gruppe D omfatter myndigheder, der har en sikkerhedsprofil, som – ud over de grundlæggende krav – ikke stiller særlige krav til fortrolighed eller tilgængelighed.

Myndighederne i denne gruppe behandler primært informationer, hvor brud på fortrolighed ikke medfører væsentlig skade for borgere, myndigheders opgaver eller statens interesser.

Systemer og funktioner kan tåle afbrydelser uden væsentlig påvirkning af samfundskritiske funktioner. Nedbrud og fejl medfører primært interne driftsforstyrrelser, men truer ikke samfundskritiske funktioner.

Krav til beskyttelse er baseret på myndighedens almindelige sikkerhedsforanstaltninger, herunder krav om at leve op til ISO 27001, de tekniske minimumskrav samt de foranstaltninger, der som minimum følger af NIS 2-loven.

Vejledning til inddeling i risikogruppe

For at fastlægge, hvilken risikogruppe en myndighed tilhører, bør myndigheden vurdere sit behov for tilgængelighed og fortrolighed. Nedenstående trin og spørgsmål kan bruges som støtte i vurderingen.

Trin 1: Vurder behovet for høj tilgængelighed

En myndighed har behov for høj tilgængelighed, hvis driftsforstyrrelser eller nedbrud kan have væsentlige konsekvenser. Overvej følgende:

- Drifter myndigheden samfundskritiske it-systemer⁴ eller varetager myndigheden funktioner⁵, som samfundet er afhængigt af, og som kræver systemunderstøttelse?
- Er myndighedens funktioner nødvendige for samfundets videreførelse, borgernes sikkerhed eller opretholdelsen af kritiske offentlige ydelser?
- Kan nedbrud påvirke liv, sundhed, væsentlig kritisk infrastruktur eller finansiell stabilitet?

Hvis én eller flere af ovenstående besvares med ja, peger det på et højt behov for tilgængelighed.

Trin 2: Vurder behovet for høj fortrolighed

En myndighed har behov for høj fortrolighed, hvis uautoriseret adgang til informationer kan medføre skade. Overvej følgende:

- Håndterer myndigheden jævnligt informationer klassificeret *FORTROLIGT* eller højere?
- Er myndigheden særligt udsat for spionage, fx på grund af arbejdsområde, data eller placering i staten ⁶?
- Behandler myndigheden følsomme, fortrolige eller kritiske informationer, hvor uautoriseret adgang kan skade enkeltpersoner, myndighedens opgavevaretagelse eller nationale interesser?

Hvis én eller flere af disse spørgsmål besvares med ja, indikerer det et højt behov for fortrolighed.

Trin 3: Fastlæg risikogruppen

Fastlæg risikogruppe ud fra vurderingerne fra trin 1 og 2.

- *Højt behov for tilgængelighed og højt behov for fortrolighed* → *Risikogruppe A*
- *Almindeligt behov for tilgængelighed og højt behov for fortrolighed* → *Risikogruppe B*
- *Højt behov for tilgængelighed og almindeligt behov for fortrolighed* → *Risikogruppe C*
- *Almindeligt behov for tilgængelighed og almindeligt behov for fortrolighed* → *Risikogruppe D*

⁴ I tråd med definition for samfundskritiske it-systemer fra Økonomitstyrelsens "[Vejledning til model for porteføljestyring af statslige it-systemer](#)"

⁵ For overblik over samfundsvigtige funktioner læs "Bilag 1 – Samfundsvigtige funktioner", fra "[Strategi for forsyningsikkerhed](#)"

⁶ Myndigheder kan som hjælp tage udgangspunkt i "[Spionagetruslen mod Danmark, Færøerne og Grønland](#)" fra PET, samt [Cybertruslen mod Danmark 2025](#). SAMSİK udgiver også løbende sektorspecifikke trusselvurderinger af cybertruslen mod Danmark – læse mere på samsik.dk/kategori/trusselvurderinger/



Datavej 20
3460 Birkerød
+45 45 16 16 66

Myndigheder kan få hjælp til risikovurdering, vurdering af sikkerhedsprofil og inddeling i risikogrupper, af SAMSIK's rådgivning, der kan kontaktes på raadgivning@samsik.dk.