

VEJLEDNING

Mindsk risikoen for spionage og kompromittering ved indkøb af off-the-shelf-teknologi

Oktober 2026



Styrelsen for
Samfundssikkerhed

Indhold

Formålet med vejledningen	3
Målgruppe.....	3
Afgrænsning for vejledningen	3
Inddeling i risikogrupper	4
De fire risikomarkører	4
Kobling af risikogruppe og risikomarkører	6
Værktøj: Fastsættelse af grundlæggende sikkerhedsbehov ved indkøb.....	6
Værktøj til risici ved indkøb af produkter.....	7
Løbende opfølgning og monitorering	9

Formålet med vejledningen

Der er en generel spionagetrussel forbundet med danske myndigheder og virksomheders brug af digitale standardprodukter¹, såsom telefoner, routere og pc'er købt direkte fra markedet. Truslen varierer og afhænger bl.a. af, hvem der anvender produktet, hvor teknologien anvendes, og hvilken data, teknologien får adgang til. Teknologierne kan udnyttes til spionage, men også til forberedelse af sabotage mod kritisk infrastruktur, kritiske samfunksfunktioner og myndighedskommunikation. Det skaber et komplekst trusselsbillede, som sammen med digital afhængighed øger behovet for at tænke sikkerhed ind i indkøbsfasen.

Denne vejledning skal hjælpe offentlige myndigheder med at identificere sikkerhedsbehov og reducere risikoen for spionage og kompromittering gennem digitale standardprodukter i indkøbsfasen ved indkøb via Staten og Kommunernes Indkøbsservice (SKI) ePortal og og Statens Indkøbssystem, Statens Digitale Indkøb (SDI). Vejledningen indeholder en række trin, som hjælper myndigheder med at sikre, at sikkerhed tænkes ind gennem hele indkøbsprocessen – og hjælper myndighederne med at mindske risikoen for spionage og kompromittering. Målet er at styrke sikkerheden i indkøbet og reducere risikoen for, at teknologi bliver en sårbarhed for statens samlede sikkerhed. Vejledningen er baseret på de risikomarkører, der anvendes af SKI på en række hardwareaftaler.

Målgruppe

Vejledningen henvender sig til både sikkerhedsansvarlige og indkøbsansvarlige i offentlige myndigheder. De to funktioner er centrale, når det kommer til sikkerhed i indkøb for offentlige myndigheder. De spiller begge en afgørende rolle i at beskytte myndigheden, men arbejder ikke altid ud fra de samme succeskriterier.

Sikkerhedsfunktionen har naturligt et fokus på sikkerhed, mens indkøbsfunktionen har et bredere perspektiv på målet med anskaffelsen. Vejledningen skal give de to funktioner et fælles sprog for sikkerhed.

Afgrænsning for vejledningen

Vejledningen omfatter fysiske produkter, der kan lagre, behandle eller overføre data. Det inkluderer klassisk digitale standardprodukter, herunder alle databærende enheder, som indgår i myndighedens drift (fx mobiltelefon, computer, printer, USB-drev m.m.).

Vejledningen omfatter ikke selvstændige softwareprodukter eller samlede systemanskaffelser. For produkter, hvor hardware leveres med indlejret software, bør sikkerhedsvurderingen dog altid tage højde for begge dele. Styrelsen for Samfundssikkerhed (SAMSIK) har på hjemmesiden sikkerdigital.dk² en række værktøjer og vejledninger til risikovurdering af IT-systemer³. Vejledningen behandler ikke udstyr til at håndtere klassificeret materiale. Kontakt SAMSIK eller din sikkerhedsorganisation for mere information om indkøb af udstyr til klassificeret materiale.

¹ Kaldet Commercial Off-The-Shelf (COTS) teknologi

² Sikkerdigital.dk

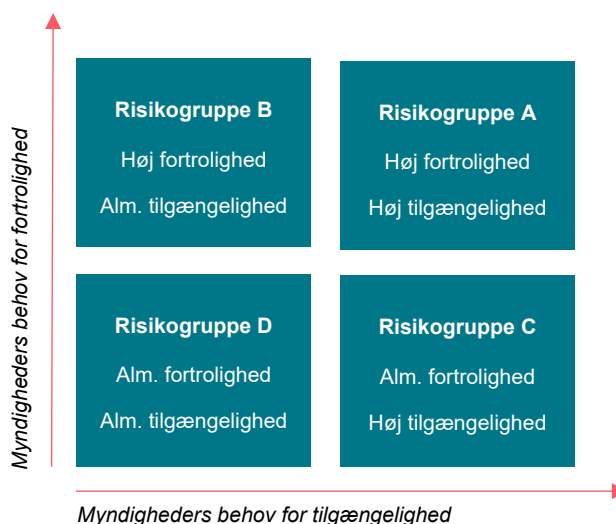
³ Se [UDSYN 2025](#) og [Cybertruslen mod Danmark 2025](#) for mere vejledning.

Inddeling i risikogrupper

For at identificere en myndigheds sikkerhedsbehov, bør myndighedens overordnede risikoprofil afdækkes. Til brug for vurderingen arbejdes der med fire forskellige risikogrupper (A-D). De beskriver de enkelte myndigheders behov for beskyttelse mod uautoriseret adgang (fortrolighed) og behov for sikring af stabil, kontinuerlig og robust drift (tilgængelighed). Sammen danner de to behov grundlag for myndighedens placering i sikkerhedsgruppen. Behovene bliver kategoriseret i almindeligt og højt.

Hvis der er tvivl om, hvilken risikogruppe myndigheden tilhører, henvises der til vejledning for risikogruppeinddeling⁴ for hjælp til indplacering af myndigheden. Denne metode kan også benyttes af andre typer myndigheder, eller enheder i myndigheder.

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



De fire risikomarkører

Risikomarkørerne fremgår som produktinformation i SKIs indkøbskataloger og i SDI. De bruges til at skabe et struktureret overblik over forhold ved et produkt og dets producent, som kan have betydning for informationssikkerheden. De fire markører (præsenteres nedenfor) giver tilsammen et billede af både teknisk risiko, leverandørmæssig påvirkning og geopolitisk kontekst. Risikomarkørerne bør altid sammenholdes med den aktuelle politik for sikkerhed i myndigheden.

Risikomarkørerne fremkommer ved søgning på de enkelte produkter, hvor de vil være synlige som mærkater på søgesiden, samt under produktbeskrivelsen ved information og sikkerhed. Vær derfor opmærksom på, hvor og hvilke markører der giver udslag.

⁴ Se vejledning for inddeling i risikogrupper (bilag)

Risikomarkør	Forklaring af risikomarkør	Forklaring af risiko
 Risiko for eksponering	Produktet kan opbevare, behandle, indsamle eller transmittere data over internettet og kan derfor potentielt være eksponeret for truslen fra cyberspionage.	Generel risiko for, at uvedkommende kan få adgang til data via produktets tekniske forbindelser som cloud eller remote access.
 Kontrol- og sanktionslister	Angiver, at producenten og/eller dennes tilknyttede organisationer eller moderselskab er underlagt udenlandsk regulering, kontrol eller restriktioner ift. national sikkerhed eller cybersikkerhed.	Risiko opstår ved, at producenten er omfattet af statslige sanktioner, underlagt eksportkontrol ift. Uhensigtsmæssig videns-overførsel eller national lovgivning om at give myndigheder adgang til teknologi.
 Produktets oprindelsesland	Angiver, hvor den sidste væsentlige bearbejdning af produktet har fundet sted, fx endelig samling og pakning inden levering til grossist.	Risiko for udnyttelse af forsyningskæden til at manipulere produktet til brug for spionage. Sammenholdes med trusselsvurderinger fra FE, PET og SAMSIK.
 Producentens hjemsted	Angiver, hvor producenten er juridisk hjemmehørende eller etableret, samt hvilken national lovgivning de kan være underlagt.	Risiko for, at producenten er underlagt national lovgivning, som kan tvinge dem til at udlevere data eller give myndigheder adgang til teknologi. Sammenholdes med trusselsvurderinger fra FE, PET og SAMSIK.

Risikomarkørerne vises på 10 rammeaftaler, der alle indeholder kommerciel, internet-forbundet, off-the-shelf-teknologi

02.02 Computere 02.08 Tele og data 50.46 Datakommunikation/WAN 50.03 Servere og storage 50.07 Kommunikationsprodukter	50.10 Kopi og print 50.40 Computere og it-tilbehør 50.43 Tablets, 50.48 Tele og data 50.70 AV-udstyr
---	--

Læs mere på SKIs hjemmeside omkring de enkelte risikomarkører. Det anbefales samtidig løbende at følge opdateringer om både kommende og eksisterende SKI-aftaler.

Kobling af risikogruppe og risikomarkører

Risikomarkører og risikogrupper bør indgå som en fast del af indkøbs- og kontraktprocessen og tilpasses det enkelte indkøbs karakter og kritikalitet. Det forudsætter en klar indkøbspolitik og en fastlagt risikoprofil, som tilsammen danner rammen for myndighedens arbejde med sikkerhed i indkøb. Det bør samtidig tydeliggøres, hvordan risikomarkørerne skal indgå i den konkrete risikovurdering, herunder hvilke kriterier der afgør, om et produkt kan købes, kan købes med kompenserende tiltag eller bør fravælges. Kravene bør så vidt muligt indarbejdes i myndighedernes eksisterende informationssikkerheds- og leverandørstyring.

Myndigheder i risikogruppe A, B og C bør være særligt opmærksomme på produkter og producenter, der kan indebære risiko for brud på fortrolighed eller tilgængelighed, mens myndigheder i risikogruppe D som udgangspunkt kan basere sig på de almindeligt gældende krav til informationssikkerhed. At en myndighed tilhører en risikogruppe med et højt behov for tilgængelighed, betyder ikke i sig selv, at alle produkter skal leve op til skærpede tilgængelighedskrav. Det afgørende er den konkrete risiko ved det enkelte produkt, vurderet på baggrund af de kendte risikomarkører. Der skal derfor foretages en konkret risikovurdering af hvert produkt med udgangspunkt i de risikomarkører, der gør sig gældende for det pågældende produkt

Værktøj: Fastsættelse af grundlæggende sikkerhedsbehov ved indkøb

Dette værktøj skal tænkes som et grundlag for en politik, som skal genbesøges årligt for opdatering. Det er myndighedens ledelse, der har ansvaret for fastlæggelsen af risikogruppen og opdateringen af politikken for sikkerhed.

Trin 1: Fast årlig opdatering af myndighedens risikogruppe

Inden produktet vurderes, skal myndighedens samlede risikoprofil overvejes. Formålet er at sikre, at vurderingen tager højde for myndighedens behov for fortrolighed og tilgængelighed. Her tages bl.a. udgangspunkt i de aktuelle trusselvurderinger fra PET, FE eller SAMSIK.

A: Høj fortrolighed + høj tilgængelighed

B: Høj fortrolighed + alm. tilgængelighed

C: Høj tilgængelighed + alm. fortrolighed

D: Almindeligt behov

Trin 2: Fast årlig opdatering af myndighedens interne politik for sikkerhed

Opdater de overordnede sikkerhedskrav ved indkøb på baggrund af myndighedens politik for sikkerhed.

- Er der særlige interne eller lovgivningsmæssige krav, der skal tages højde for ved indkøb, og er det skrevet med i organisationens sikkerhedspolitik?
- Er der specifikke trusler, der skal tænkes ind i de sikkerhedskrav der skal stilles ved indkøb?

Overvej på baggrund af dette, hvad det stiller af krav til organisationens risikovurdering af risikomarkører ved indkøb af produkter.

- Er der lande/producenter, som myndigheden vurderer udgør en forhøjet risiko?
- Er der kontrol-/sanktionslister, som myndigheden bør være særlig opmærksom på?
- Er der særlige forhold ved produktets forbindelser (fx cloud eller fjernadgang), som myndigheden bør være opmærksom på?

Husk løbende at have dialog omkring politik for sikkerhed og risikovurdering mellem myndighedens sikkerheds- og indkøbsansvarlige, så indkøb kender til myndighedens overordnede sikkerhedskrav til produkter.

Værktøj til risici ved indkøb af produkter

Nedenfor gennemgås, hvordan risikomarkører anvendes i praksis, herunder hvilke forhold der bør indgå i vurderingen af køb af et produkt. Trinene bør bruges som inspiration til myndighedens arbejde, der kan understøtte de konkrete vurderinger.

Bemærk at der er indskrevet en rollefordeling i de nedenstående trin, som er variende mellem den indkøbsansvarlige, den sikkerhedsansvarlige og ledelsen. Det er en fordeling, der er gældende for myndigheder omfattet af NIS 2-loven, da ledelsen har ansvaret for styringen af cybersikkerhed og skal godkende og føre tilsyn med sikkerhedsforanstaltninger. Ligeledes er det gældende, hvis myndigheden arbejder efter sikkerheds-standard ISO 27001, hvor risikostyring er et centralt krav.

Trin 1: Indkøb bliver bedt om at indkøbe et specifikt produkt

Slå produktet op i e-handelssystemet og kontrollér, om én eller flere af de fire sikkerhedsmarkører angiver en risiko ved produktet:

Risiko for eksponering	Kontrol-/sanktionsliste
Produktets oprindelsesland	Producentens hjemsted

Ved udslag af risikomarkører skal myndighedens indkøbsansvarlige vurdere, om personen kan tage stilling til køb af et produkt på baggrund af den interne politik for sikkerhed. I risikovurderingen af de specifikke indkøb kan der tages udgangspunkt i følgende overvejelser:

1. Hvor i myndigheden, og af hvem, skal produktet anvendes?
2. Skal produktet bruges til at behandle følsomme eller klassificerede data?
3. Kan produktet påvirke kritiske funktioner eller drift?

Hvis de indkøbsansvarlig ikke kan vurdere risikoen, bør de tage fat i de sikkerhedsansvarlige.

Trin 2: Beslut handling inden køb af det enkelte produkt

På baggrund af trin 1 vurderes det, hvilken håndtering produktet kræver, og om der er et behov for særlige sikkerhedsforanstaltninger. Det er ledelsen, der står til ansvar for beslutningen. Overvej derfor den samlede sum af de forudgående trin:

- Myndighedens risikogruppe
- Produktets funktion og adgang
- Typen af data produktet giver adgang til
- Det aktuelle trusselsbillede ud fra PET, FE og SAMSIK's vurderinger

Kan købes Ingen yderligere handling er nødvendig.	Kan købes med tiltag Ét eller flere mitigerende sikkerhedstiltag skal implementeres.	Bør ikke købes Risikoen vurderes for høj til at købe.
---	--	---

Hvis et produkt vurderes for risikabelt at indkøbe, vil der være muligheder for at købe alternative produkter via SKI.

Løbende opfølgning og monitorering

Opfølgning og løbende monitorering af spionagetruslen er nødvendig for at holde risikovurderingen opdateret. Risikoen for spionage gennem digitale standardprodukter ændrer sig over tid, og det er derfor nødvendigt, at der følges op på risikoen, når der sker væsentlige ændringer fx i trusselsbilledet, opdatering af produktet, ændring i brug eller ved udrulning af nye funktioner. Selvom foranstaltninger typisk implementeres i driftsfasen, bør I løbende sikre, at de stadig virker efter hensigten. Gennemgå derfor risikovurderingen mindst én gang om året for at sikre, at den stadig er retvisende.

Best practice er, at:

- arbejdet med risikomarkører og risikogrupper understøttes af en løbende dialog mellem indkøb og sikkerhed gennem hele livscyklussen.
- der bør anvendes en ISMS (Information Security Management System)⁵, i form af en ensartet metode, på tværs af organisationen, så vurderinger kan sammenlignes og genbruges, og alle væsentlige beslutninger bør dokumenteres, også når risikoen vurderes som lav.
- der særligt bør være opmærksomhed på produkter med høj eksponering eller stor betydning for organisationens drift, hvor selv mindre ændringer kan have væsentlig effekt på risikoniveauet.

Opdatering og monitorering af eksisterende såvel som kommende risikomarkører foretages løbende i dialog mellem SKI og SAMSIK. Det samme gælder for nye produkter, der løbende indarbejdes i indkøbsaftalerne.

NIS 2 og risikostyring

I myndigheder omfattet af NIS 2-loven skærpes ledelsens ansvar i arbejdet med risikostyring. Det betyder bl.a., at ledelsen har ansvaret for styringen af cybersikkerhed og skal godkende og føre tilsyn med sikkerhedsforanstaltninger. Se NIS 2-vejledningen [Ledelsens rolle og opgaver](#) på samsik.dk. Arbejder din organisation efter sikkerhedsstandarden ISO 27001, er risikostyring et centralt krav.



Datavej 20
3460 Birkerød
+45 45 16 16 66

Rådgivning

Kontakt til Styrelsen for Samfundssikkerhed angående rådgivning om sikkerhed, cybersikkerhed, beredskabsplanlægning og forsyningssikkerhed: raadgivning@samsik.dk