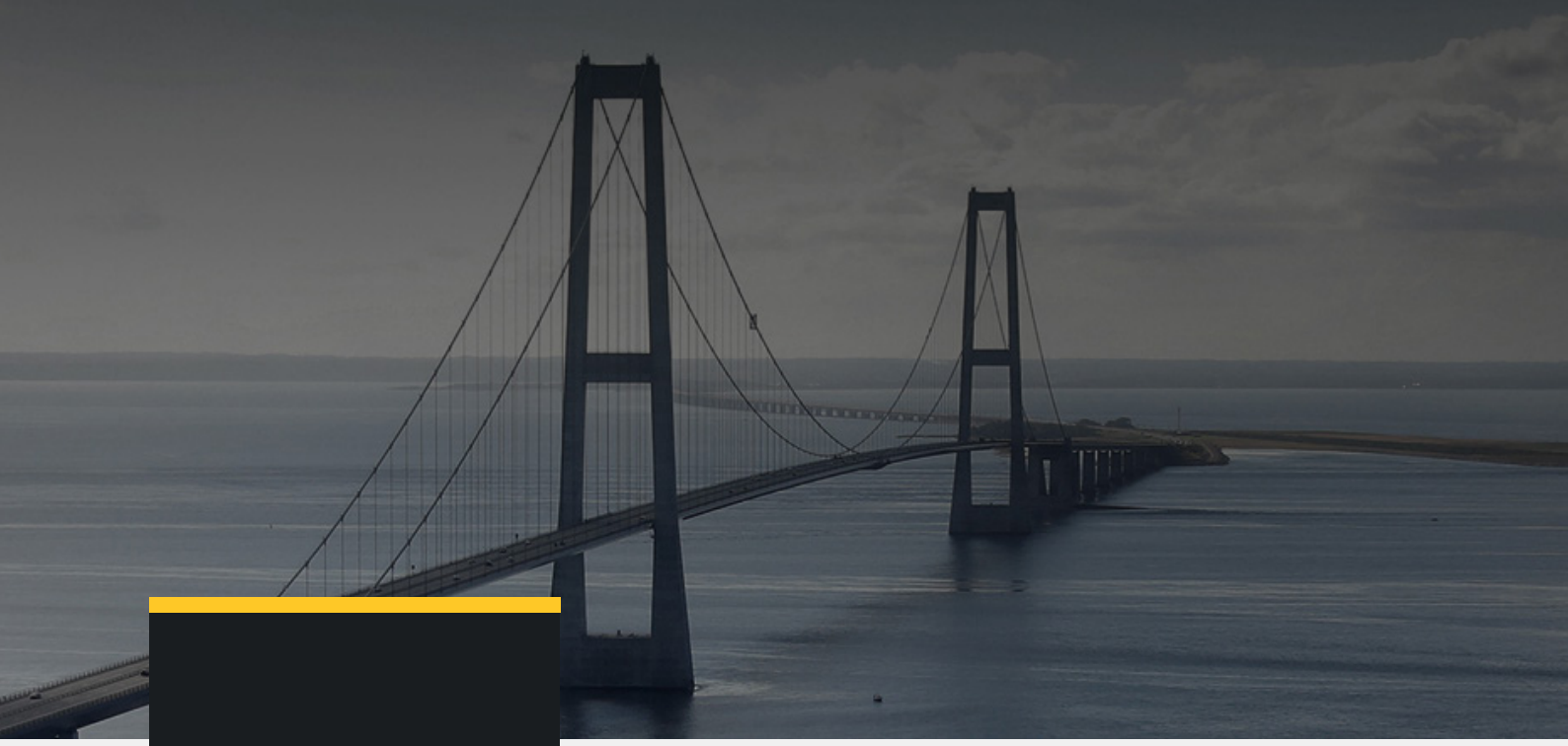


Strategi for Erhvervsstyrelsens cyber- og informationssikkerhed 2022-2025

6. december 2022

Erhvervsstyrelsen

Strategi for Erhvervsstyrelsens cyber- og informationssikkerhed 2022-2025

1. Indledning

Som følge af den Nationale Cyber- og Informationssikkerhedsstrategi (NCIS) for 2022-2024 igangsættes der en række indsatser for at styrke sikkerheden i og omkring de samfundsvigtige funktioner. Strategien bygger videre på den forrige strategi for 2018-2021 og sigter efter at løfte den digitale sikkerhed på tværs af samfundet. Initiativerne skal løfte beskyttelsen af den kritiske infrastruktur og statens it-systemer samt sikre, at myndigheder har et tilstrækkeligt sikkerhedsniveau. Med NCIS 2022-2024 forpligtes ministerområder med ansvar for samfundsvigtige funktioner, der i væsentlig grad er it-understøttet, til at udarbejde strategier for cyber- og informationssikkerheden samt oprette en decentral cyber- og informationssikkerhedsenhed (DCIS).

I forbindelse med Digitaliseringsstyrelsens nationale kortlægning af Danmarks kritiske infrastruktur i april 2021, har Erhvervsstyrelsen – med afsæt i vejledning fra Digitaliseringsstyrelsen[1] – vurderet, at Erhvervsstyrelsen udfører en samfundsvigtig funktion, som er vurderet til at være samfundskritisk og har særlig betydning for den digitale infrastruktur i Danmark. Erhvervsstyrelsen har derfor udarbejdet Strategi for Erhvervsstyrelsens cyber- og informationssikkerhed med det primære formål at sikre, at der foreligger en klar plan for arbejdet med cyber- og informationssikkerhed for det samfundskritiske it-system.

Strategien tager udgangspunkt i de krav, der følger af NCIS-initiativ 1.1. om Styrket sikkerhed omkring samfundsvigtige funktioner. Strategien bygger ovenpå og supplerer Erhvervsstyrelsens øvrige arbejde med informationssikkerhed, og strategiperioden er derfor fastlagt, så den følger tidsplanen for arbejdet med styrelsens it-handlingsplan lavet i regi af Statens It-råd. Erhvervsstyrelsens målsætning med strategien for perioden 2022-2025 er at styrke robustheden af det samfundskritiske it-system. Da trusselsbilledet er konstant skiftende, vil Erhvervsstyrelsens cyber- og informationssikkerhedsstrategi blive opdateret løbende eksempelvis ved markante samfundsmæssige ændringer.

Det bemærkes afsluttende, at strategien er skrevet med henblik på offentliggørelse, og derfor ikke beskriver konkrete sårbarheder og styrelsens håndtering af disse. Strategien dækker over perioden 2022-2025.

2. Erhvervsstyrelsens informationssikkerhedslandskab

Strategien for Erhvervsstyrelsens cyber- og informationssikkerhed indgår i styrelsens samlede arbejde med informationssikkerhed. Strategien beskriver konkret, hvordan styrelsen løfter NCIS-initiativ 1.1 Styrket sikkerhed omkring samfundsvigtige funktioner i tæt koordinering med og med øje for det

[1] Vejledning til model for porteføljestyring af statslige it-systemer, Digitaliseringsstyrelsen, juni 2021

eksisterende strategiske arbejde om informationssikkerhed, der pågår i styrelsen. Denne strategi anvender alene udtrykket informationssikkerhed. Cybersikkerhed dækker over beskyttelse af cyberspace såsom netværk, enheder og systemer. Informationssikkerhed har til formål at beskytte alt og alle informationer – strategien henviser til informationssikkerhed, da dette er mest altomfavnende.

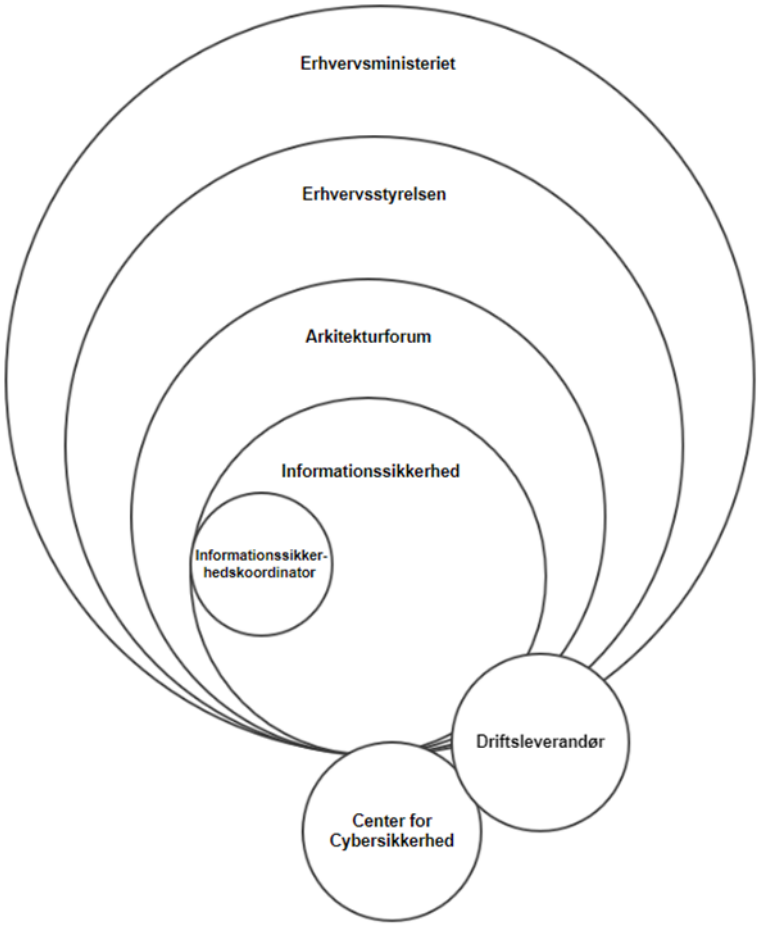
2.1. Ledelsesforankring

Arbejdet med informationssikkerhed har fokus på at etablere de rette rammer for et ledelsessystem for informationssikkerhed (ISMS). Det har medført, at styrelsen har en sikkerhedsorganisation med udnævnelse af en informationssikkerhedskoordinator og et Arkitekturforum, som sammen giver en governance struktur omkring det tværgående arbejde med it-sikkerhed. Informationssikkerhedskoordinatoren agerer som organisationens daglige sikkerhedsansvarlige, og har tværgående koordineringsopgaver. Arkitekturforum er overordnet ansvarlig for prioritering af organisationens informationssikkerhedsarbejde, og fastlægger på baggrund af indstillinger fra informationssikkerhedskoordinatoren sikkerhedsniveauet for organisationen. Mellem informationssikkerhedskoordinatoren og Arkitekturforum indgår en ledelseskæde, som består af kontorchef og vicedirektør, som kvalitetssikrer indstillinger og materiale inden det forelægges den øverste ledelse i Arkitekturforum. Etableringen af Arkitekturforum, som er forankret i topledelsen med direktionsmedlemmer, har medvirket til, at styrelsen løbende kan sikre den rette prioritering af sikkerheden og fastholde en forsat høj bevidsthed om informationssikkerhed i forbindelse med udviklingen af nye systemer samt drift og vedligehold af eksisterende. Erhvervsministeriets departement udgør qua deres rolle som tilsynsmyndighed den overordnede del af sikkerhedsorganisationen som anvist i figur 1.

Informationssikkerhedsorganisationens overordnede formål er at sikre at:

- Informationssikkerheden implementeres i organisationen
- Informationssikkerhedspolitikken og regler i styrelsen er relevante og opdaterede
- Der løbende følges op på sikkerhedsarbejdet i styrelsen
- Fokus på områder, hvor sikkerhedspolitik og regler ikke følges tilfredsstillende

Figur 1: Erhvervsstyrelsens sikkerhedsorganisation



2.1. Ledelsesforankring

Erhvervsstyrelsen udarbejder hvert tredje år en it-handlingsplan i regi af it porteføljestyring under Statens It-råd. Handlingsplanen adresserer forretningsunderstøttelse, it-systemtilstand, informationssikkerhed, kontrakter og sourcing samt forsyningssikkerhed. Erhvervsstyrelsens informationssikkerhedstiltag skal sikre stabilitet i tilgangen til data, fortrolighed ift. persondata samt pålideligheden i datas indhold. Det sikres ved, at Erhvervsstyrelsen lever op til almindeligt anerkendte principper for informationssikkerhed, såsom lovmæssige krav, anerkendte standarder og databeskyttelsesforordningen. Styrelsen anvender ISO 27001:2013 og den interne strategiske it-handlingsplan, der definerer rammen for beskyttelse af styrelsens informationer, særligt at kritiske og personfølsomme informationer bevarer deres fortrolighed, integritet og tilgængelighed. Styrelsen følger et ledelsesgodkendt årshjul for alle relevante sikkerhedsaktiviteter såsom risikovurderinger, SoA-dokumentation med tilhørende kontroller, beredskabsstyring, håndtering af sikkerhedshændelser, udarbejdelse af og vedligeholdelse af sikkerhedsdokumenter samt politikker og træning af medarbejderne i awareness,

hvorfor arbejdet omkring delstrategien vil blive implementeret i samme årshjul. Ovenstående arbejde omkring informationssikkerhed er således ledelsesforankret i styrelsens Arkitekturforum.

2.3. Risikovurderinger

Styrelsen arbejder risikobaseret og risikovurderinger af styrelsens it-aktiver indgår som en fast aktivitet i styrelsens interne årshjul. I arbejdet med at fastsætte strategiske og operative mål anbefaler Center for Cybersikkerhed (CFCS), at der tages afsæt i en risikovurdering af organisationens it-understøttelse. Erhvervsstyrelsen arbejder efter ISO-standarderne:

> *ISO/IEC 27001:2013 Ledelsessystem for informationssikkerhed – krav og vejledning, og*
>
> *ISO 27005:2018 Information technology - Security techniques - Information security risk management.*

I arbejdet med sikkerhed skal styrelsen have de grundlæggende parametre for fortrolighed, integritet og tilgængelighed på plads. Fortrolighed betyder, at informationer skal beskyttes mod uautoriseret adgang eller videregivelse, således at uvedkommende ikke er bekendt med oplysningerne. Integritet betyder, at informationer skal beskyttes mod uautoriseret manipulation. Tilgængelighed betyder, at informationer skal være tilgængelige for retmæssige brugere.

For hvert informationsaktiv fastlægges konsekvensen ved tab af aktivitetens fortrolighed, integritet eller tilgængelighed. Dernæst identificeres trusler, som aktivet står over for og det vurderes, hvad sandsynligheden er for at truslen kan indtræffe på baggrund af de sårbarheder systemet har. Erhvervsstyrelsen trusselskatalog bygger på kendte frameworks og best practice, som anvendes i arbejdet med risikostyring. Erhvervsstyrelsen anvender CFCS' årlige trusselsvurdering for cybertruslen mod Danmark, som det generelle trusselsbillede for Erhvervsstyrelsen. I 2022 var den største trussel cyberspionage og cyberkriminalitet[2].

3. Initiativer til styrket indsats for at styrke cyber- og informationssikkerheden i og omkring samfundskritiske it-systemer

Som følge af NCIS-initiativ 1.1 Styrket sikkerhed omkring samfundsvigtige funktioner tager strategien udgangspunkt i en række krav, der tilsammen skal styrke sikkerheden med samfundsvigtige funktioner, der i væsentlig grad er it-understøttet.

3.1 Udarbejdelse af strategi for cyber- og informationssikkerheden for it-understøttelsen af de samfundsvigtige funktioner

Erhvervsstyrelsen har udarbejdet strategien for Erhvervsstyrelsens cyber- og informationssikkerhed i tråd med den vejledning, der er udarbejdet af CFCS og Digitaliseringsstyrelsen. Erhvervsstyrelsens initiativer på områderne er udarbejdet på baggrund af arbejdet med risiko og risikostyring omkring

[2] Cybertruslen mod Danmark 2022, Center for cybersikkerhed, 2022

styrelsens samfundskritiske it-system. Strategien bygger ovenpå og supplerer styrelsens øvrige arbejde med informationssikkerhed, og strategiperioden er derfor fastlagt, så den følger tidsplanen for arbejdet med styrelsens it-handlingsplan.

3.2 Etablering af en DCIS med operationel kapacitet

Erhvervsstyrelsen opretter en decentral cyber- og informationssikkerhedsenhed (DCIS) med operativ kapacitet med reference til Arkitekturforum. Enheden skal drive cyber- og informationssikkerheden i og omkring styrelsens samfundskritiske it-system og sikre håndtering af tværgående sikkerhedshændelser i samarbejde med driftsleverandøren og i koordinering med CFCS.

DCIS ledelsesforankres i styrelsens Arkitekturforum, hvor det resterende informationssikkerhedsarbejde er forankret. Mellem DCIS og Arkitekturforum indgår en ledelseskæde bestående af kontorchef og vicedirektør, der kvalitetssikrer indstillinger og materiale inden det forelægges den øverste ledelse i Arkitekturforum.

DCIS er operativ implementeret i styrelsens informationssikkerhedsenhed og opererer som kontaktpunkt mellem CFCS og driftsleverandør ved krisesituation, og er operativ. Driftsleverandør er en del af den operative kapacitet, har 24-timers drift og håndterer sikkerhedshændelser i forhold til gældende kontrakt.

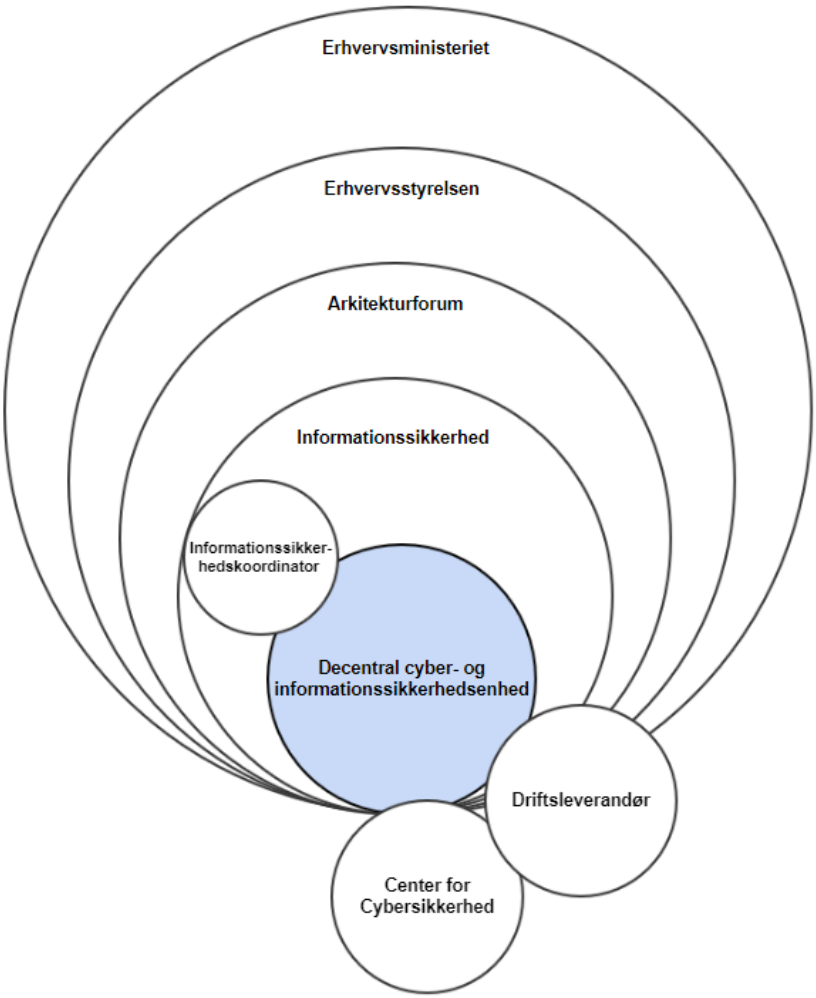
Der vil i strategiperioden være ekstra fokus på risikohåndtering i og omkring det samfundskritiske it-system med årlig udarbejdelse af en handlingsplan med konkrete initiativer til mitigering af eventuelle risici. Den decentrale cyber- og informationssikkerhedsenhed vil, som en del af risikoarbejdet i styrelsens ledelsessystem for informationssikkerhed (ISMS), årligt sikre, at der bliver udarbejdet handlingsplaner for it-systemer, som ikke har implementeret passende foranstaltninger.

DCIS årshjul adresserer 10 krav:

- Udarbejdelse af strategi for cyber- og informationssikkerheden for it-understøttelse af de samfundsvigtige funktioner
- Etablering af en DCIS med operationel kapacitet
- Kortlægning af kritisk infrastruktur
- Stillingtagen til klassificeret kommunikation
- Udarbejdelse af logningspolitik
- Tilslutning til CFCS's sensornetværk
- Vurdering af behov for inddragelse af CFCS ved indkøb og udbud
- Vurdering af behov for indberetningspligt, sikkerhedsgodkendelser og beredskabsaftaler
- Specifikation af vejledninger og anbefalinger, der følges i Erhvervsstyrelsen
- Stillingtagen til behov for ny lovgivning vedr. cyber- og informationssikkerhed

Nedenstående figur illustrerer forankring af DCIS i Erhvervsstyrelsens sikkerhedsorganisation.

Figur 2: Forankring af DCIS i Erhvervsstyrelsens sikkerhedsorganisation Erhvervsstyrelsens sikkerhedsorganisation



3.3 Kortlægning af kritisk infrastruktur

Erhvervsstyrelsens vurdering og kortlægning af styrelsens it-systemers kritikalitet følger Digitaliseringsstyrelsens Vejledning, definitioner mv. vedrørende model for porteføljestyring af statslige it-systemer[3], hvoraf det bl.a. fremgår, at:

> *"It-systemer hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet som helhed, fx i form af økonomiske tab hos stat, virksomheder eller borgere, længerevarende nedbrud af kritisk infrastruktur eller reelle trusler for den nationale sikkerhed. Samfundskritiske it-systemer*

[3] Vejledning til model for porteføljestyring af statslige it-systemer, Digitaliseringsstyrelsen, juni 2021

er således it-systemer, hvor utilgængelighed og driftsustabilitet i it-systemerne kan få markante følger for samfundet og for opretholdelsen af samfundskritiske processer."

Erhvervsstyrelsen har med afsæt heri vurderet, at styrelsen udfører en samfundsvigtig funktion, som er it-understøttet af det samfundskritiske it-system.

Kortlægningen foregår ved et genbesøg af den eksisterende kortlægning. Arkitekturforum genbesøger således fremover minimum hvert år kritikaliteten af styrelsens systemportefølje på baggrund af indstilling fra DCIS og ledelseskæden bestående af kontorchef og vicedirektør. Systemejere for samfundskritiske it-systemer har et særligt ansvar for at sikre, at dokumentationen omkring systemet er opdateret.

3.4 Stillingtagen til klassificeret kommunikation

Erhvervsstyrelsen følger sikkerhedscirkulæret. Kommunikation i og omkring samfundskritiske it-systemer er som al øvrig kommunikation omfattet af Erhvervsstyrelsens retningslinjer for sikker it-anvendelse og brugeradfærd.

Erhvervsstyrelsen udfører samfundsvigtige opgaver, som er it-understøttet. It-understøttelsen udveksler ikke klassificeret data med andre myndigheder. Nuværende vurderes det, at der ikke er behov for at anvende klassificeret kommunikation i og omkring det samfundskritiske it-system.

DCIS genbesøger fremover årligt behovet for at kommunikere klassificeret i og omkring de samfundskritiske it-systemer.

3.5 Udarbejdelse af logningspolitik

Formålet med Erhvervsstyrelsens logningspolitik er at sikre, at it-sikkerhedshændelser kan undersøges, sikre data kan genskabes og monitorere logs.

Erhvervsstyrelsen arbejder med styrelsens logning i henhold til statens 20 tekniske minimumskrav[4]. Styrelsen har implementeret ISO 27001:2013, som indebærer at registrere hændelser og tilvejebringe bevis gennem bl.a. hændelseslogning og administrator- og operatørlog.

DCIS genbesøger Erhvervsstyrelsens tiltag for logning i 2023 med henblik på at understøtte arbejdet i og omkring samfundskritiske it-systemer ved eventuelle sikkerhedshændelser gennem monitorering af logs både internt og eksternt hos driftsleverandør.

3.6 Tilslutning til CFCS's sensornetværk

CFCS driver et sensornetværk, som kan opdage forsøg på avancerede cyberangreb. Sensornetværket alarmerer baseret på kendt skadelig trafik og benyttes til at analysere avancerede forsøg på cyberspionage. Hvis en sensor udløser en alarm, bliver alarmen analyseret af CFCS for at afklare situationen. Hvis der er begrundet mistanke om, at et system er ramt af en sikkerhedshændelse, kan CFCS reagere og sende varsel til Erhvervsstyrelsen.

[4] Tekniske minimumskrav for statslige myndigheder, september 2022

Erhvervsstyrelsen er tilmeldt CFCS' sensornetværk. Såfremt Erhvervsstyrelsen i fremtiden kommer til at drifte yderligere samfundskritiske it-systemer, vurderer styrelsen behovet for tilslutning af disse til CFCS' sensornetværk, hvilket sker i forbindelse med kortlægning af kritisk infrastruktur.

3.7 Vurdering af behov for inddragelse af CFCS ved indkøb og udbud

Erhvervsstyrelsens varetager en samfundsvigtig funktion gennem opretholdelse og vedligehold af det samfundskritiske it-system, som medfører et øget behov for sikkerhed omkring systemets oplysninger. Erhvervsstyrelsen vil i strategiperioden implementerer kommende minimumskrav til statslige myndigheders styring af kontrakter i og omkring samfundskritiske it-systemer, herunder at CFCS skal bruges som sikkerhedsrådgiver ved kommende udbud og indkøb af samfundskritiske it-systemer samt eventuelt ved indkøb af it-systemer, der understøtter samfundskritiske it-systemer.

3.8 Vurdering af behov for indberetningspligt, sikkerhedsgodkendelser og beredskabsaftaler

Erhvervsstyrelsen følger Sikkerhedscirkulæret og vurderer løbende behovet for sikkerhedsgodkendelser af medarbejdere. Styrelsen stiller krav til, at interne medarbejdere og eksterne, der arbejder i og omkring samfundskritiske it-systemer, har pligt til at indberette sikkerhedshændelser. Ligeledes foreligger der beredskabsaftaler med leverandører om it-beredskabet ift. håndtering af en it-sikkerhedshændelse. Der afholdes årligt beredskabsøvelser med driftsleverandør.

DCIS vil fremover årligt vurderer behovet for ovenstående. Vurderingen sker gennem en indstilling til Erhvervsstyrelsens Arkitekturforum.

3.9 Specifikation af vejledninger og anbefalinger, der følges i Erhvervsstyrelsen

Med henblik på at sikre, at Erhvervsstyrelsens arbejde med it-understøttelse af samfundsvigtige funktioner følger best practice, tages der udgangspunkt i nedenstående vejledninger og anbefalinger til styrelsens cyber- og informationssikkerhedsarbejde.

Sikkerhedsstandarder og vejledninger

Erhvervsstyrelsen skal som statslig myndighed efterleve sikkerhedsstandarden ISO 27001:2013. Sikkerhedsstandarden skal sikre, at Erhvervsstyrelsen arbejder systematisk og standardiseret med områder, der kan styrke cyber- og informationssikkerheden.

Erhvervsstyrelsen har siden 2016 haft implementeret ISO/IEC 27001:2013 Ledelsessystem for informationssikkerhed – krav. Erhvervsstyrelsen anvender i tillæg til sikkerhedsstandarten følgende vejledninger til understøttelse af styrelsens ledelsessystem for informationssikkerhed:

- ISO27002;2014 Regelsæt for styring af informationssikkerhed
- ISO27005:2018 Information technology - Security techniques - Information security risk management

- Digitaliseringsstyrelsen/Erhvervsstyrelsens vejledninger til implementering af ISO27001[5]

Tekniske minimumskrav

Som nævnt i afsnit *3.5 Udarbejdelse af logningspolitik* efterlever styrelsen de tekniske minimumskrav for statslige myndigheder. Kravene har til formål at beskytte statslige myndigheder mod ondsindede cyber- og informationssikkerhedshændelser, fx hackerangreb og spredning af malware.

Som led i den nationale strategi for cyber- og informationssikkerhed 2022-2024 er de 20 krav blevet opdateret og præciseret. Samtidig er det besluttet, at de tekniske minimumskrav skal udbygges med nye krav, og at behovet for nye eller reviderede krav løbende vurderes. Der forventes derfor i strategiperioden at komme nye tekniske minimumskrav og justering af eksisterende, som skal efterleves. Erhvervsstyrelsen vil løbende følge dette og foretage de nødvendige tilpasninger.

- Tekniske minimumskrav[6]

National strategi for cyber -og informationssikkerhed

Erhvervsstyrelsen følger og implementerer krav i den nationale strategi for cyber og informationssikkerhedsstrategi[7].

Som følge af initiativ 1 i National strategi for cyber -og informationssikkerhed 2022-2024, *robust beskyttelse af de samfundsvigtige funktioner,* har Erhvervsstyrelsen implementeret initiativ 1.1 om styrket sikkerhed omkring samfundsvigtige funktioner. Målet med initiativ 1 er at sikre, at Erhvervsstyrelsen kan opretholde samfundsvigtige funktioner og økonomisk aktivitet i en krisesituation, hvor kritisk it-infrastruktur sættes ud af kraft i kortere eller længere tid.

Erhvervsstyrelsen vil opretholde et sikkerhedsniveau, der med kort varsel gør styrelsen i stand til at agere i tilfælde af alvorlige cyberhændelser.

Yderligere initiativer på området implementeres, såfremt det er relevant.

Anbefalinger, vejledninger og Best Practice

Erhvervsstyrelsen anvender desuden følgende vejledninger og anbefalinger i styrelsens arbejde med informationssikkerhed:

- Vejledninger og skabeloner (sikkerdigital.dk), Forebyggelse (cfcs.dk)
- Tiltag til styrket cyberforsvar, Logning – en del af et godt cyberforsvar, Cyberforsvar, der virker[8]
- Passwordsikkerhed[9]
- God kultur ved distancearbejde[10]

[5] ISO 27001 implementering
[6] Tekniske minimumskrav for statslige myndigheder
[7] National strategi for cyber- og informationssikkerhed 2022-2024, Digitaliseringsstyrelsen december 2021
[8] Logning – en del af et godt cyberforsvar, Center for cybersikkerhed, januar 2022
[9] Passwordsikkerhed, Center for cybersikkerhed, marts 2020
[10] God kultur ved distancearbejde, Center for cybersikkerhed / Digitaliseringsstyrelsen, januar 2021

- Cybersikkerhed på rejsen – organisationens ansvar[11]
- Råd om sikkerhed på mobile enheder: God, Bedre, Bedst[12]

Løbende opdatering af oversigten

Såfremt der udgives nye vejledninger i strategiperioden, vil Erhvervsstyrelsen vurdere om disse skal følges. Erhvervsstyrelsens informationssikkerhedskoordinator er ansvarlig for at holde sig opdateret om nye krav, vejledninger og anbefalinger om cyber- og informationssikkerheden, og videreformidle disse til styrelsens sikkerhedsorganisation.

3.10 Stillingtagen til behov for ny lovgivning vedr. cyber- og informationssikkerhed

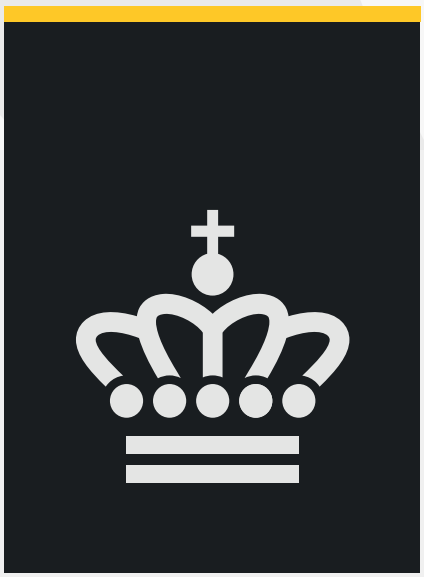
Med afsæt i DCIS løbende arbejde med cyber- og informationssikkerhed, herunder identificerede sårbarheder som følge af risikovurderinger eller beredskabsøvelser, vurderer Arkitekturforum årligt, om Erhvervsstyrelsen har de nødvendige juridiske beføjelser til at sikre det rette niveau for cyber- og informationssikkerheden for de samfundsvigtige funktioner, som Erhvervsstyrelsen er ansvarlig for.

4. Afslutning

Ovenstående strategi og initiativer er sidestillet og implementeret i styrelsens arbejde med informationssikkerhed. Initiativerne implementeres i årshjul for ISMS, og løses, afrapporteres og evalueres således igennem det eksisterende arbejde omkring informationssikkerhed. DCIS foretager løbende sikkerhedsjusteringer til strategi og handlingsplaner, som sker ved større systemændringer eller markante forandringer.

[11] Cybersikkerhed på rejsen - organisationens ansvar, Center for cybersikkerhed, januar 2022

[12] Råd om sikkerhed på mobile enheder, Center for cybersikkerhed, maj 2018



ERHVERVSSTYRELSEN

Langelinie Allé 17
2100 København Ø

T: 3529 1000
@: erst@erst.dk
W: erhvervsstyrelsen.dk