FINANSTILSYNET

Nyt fra Finanstilsynet

5. september 2019

Anders Kragsnæs Balling, underdirektør
Finanstilsynet

Agenda

- Risikobilledet – IT-sikkerhed i den finansielle sektor
- Hvad gør Finanstilsynet
  - IT-tilsyn
  - Decentral enhed for cyber- og informationssikkerhed (DCIS)
- Nye regler mv.
  - Ledelsesbekendtgørelsens bilag 5
  - Nye EBA retningslinjer om outsourcing
- På vej - nye EBA retningslinjer vedr. ICT and security risk management

FINANSTILSYNET

Trusler mod IT-sikkerheden

Digitaliseringen giver stigende afhængighed af sikker og stabil IT-drift (uden IT – ingen bank).

Center for Cybersikkerhed vurderer, at niveauet for cybertrusler mod den finansielle sektor er højt.

Sektoren tilkendegiver:

- Stor bekymring omkring cybersikkerhed.
- Og cyberrisiko er den mest udfordrende at tackle.

Trusselsbilledet udvikler sig løbende. Angrebene bliver fortsat mere avancerede.

FINANSTILSYNET

Den finansielle sektor er sårbar overfor cyberangreb og IT-nedbrud

IT-sikkerhedsindretningen og ledelsens fokus har flere steder ikke fulgt tilstrækkeligt med udviklingen.

- Virksomhederne har fortsat mange sårbarheder.
- Topledelserne skal vide mere om IT-sikkerhed og involvere sig mere i virksomhedernes IT-sikkerheds- og risikostyring. Virksomhederne har typisk også brug for at styrke IT-sikkerhedskompetencerne i hele organisationen.
- Mangler effektive systemer til at styre deres IT-sikkerhed og -risici.
- Svaghederne gælder også i relation til leverandørstyring og IT-outsourcing.
- IT-risikorapporteringen til direktion og bestyrelse skal forbedres.

Hvad gør Finanstilsynet?

To roller:

- IT-tilsyn med de finansielle virksomheder
- Decentral Enhed for Cyber- og Informationssikkerhed for finanssektoren (DCIS finans)

IT-tilsyn - hvad gør Finanstilsynet?

- Tilsynsaktiviteter målrettet IT-sikkerhed
- Øget fokus på systemiske virksomheder
- Øget fokus på IT-sikkerhed i Finanstilsynets dialog med virksomhedernes topledelse
- Øget indsats i forhold til påbudsopfølgning.

DCIS – hvad er det?

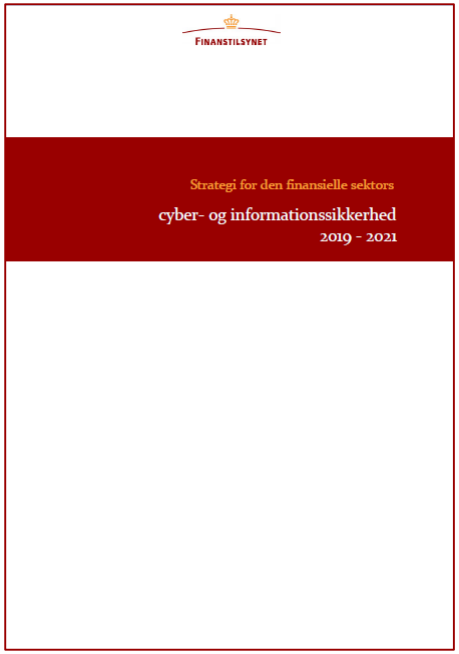
- National strategi for cyber- og informationssikkerhed

- Sektorvise delstrategier for de seks samfundskritiske sektorer
  - Energi, sundhed, transport, tele, **finans**, søfart,

- Strategi for den finansielle sektors cyber- og informationssikkerhed
  - Finanstilsynet udpeget som decentral enhed for cyber- og informationssikkerhed (DCIS)
  - **Formål**: *at fremme finansiel stabilitet og tillid til den finansielle sektor ved at styrke den samlede indsats for cyber- og informationssikkerhed*

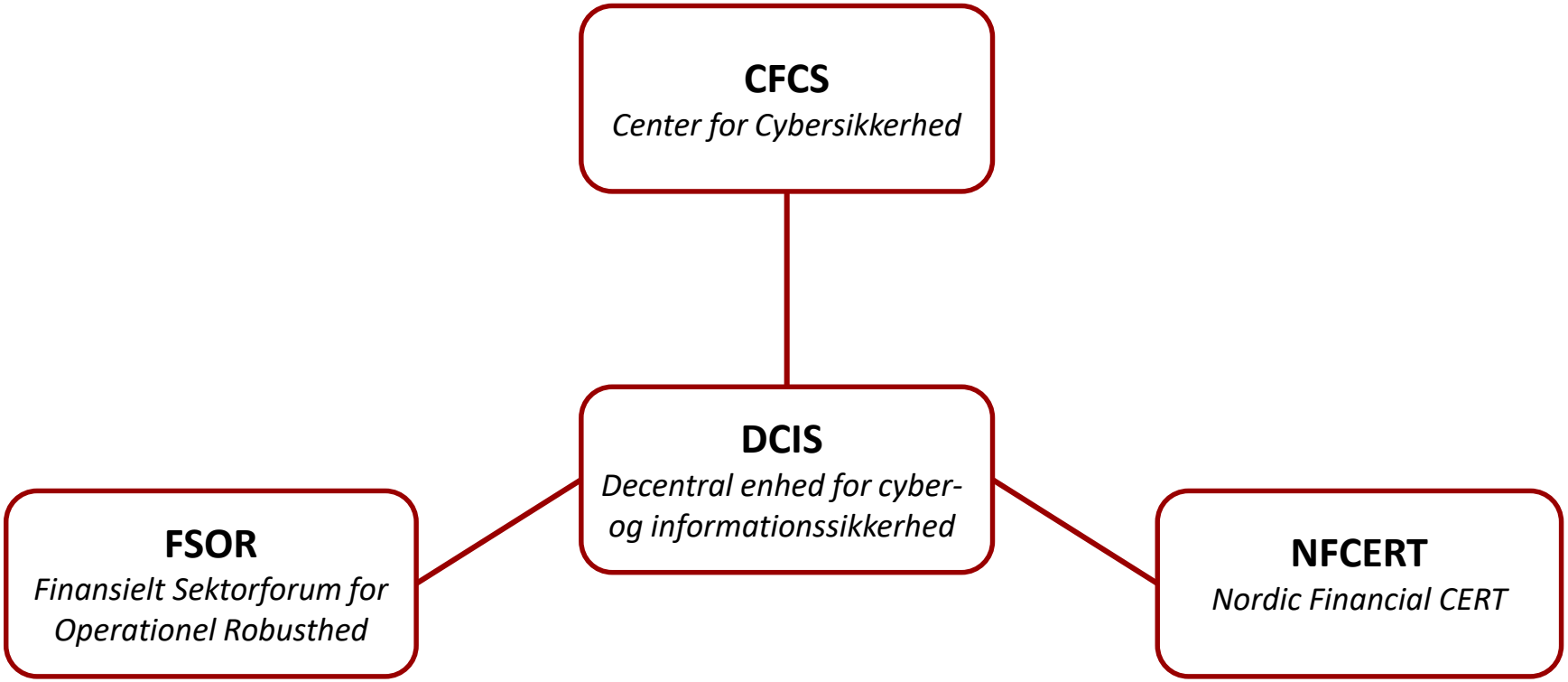
Strategiens fokus og initiativer

- Strategiens tre hovedspor:
  - trussels-, sårbarheds- og risikovurdering
    - *eks. løbende afdækning af sektorens sårbarheder og kritiske infrastruktur*
  - sektorberedskab
    - *eks. løbende udvikling og test af kriseberedskab*
  - videndeling
    - *eks. oplysning til finanssektorens kunder og indsats i forhold til finanssektorens ansatte*



FINANSTILSYNET

DCIS-organiseringen baseret på samarbejde mellem myndigheder



FINANSTILSYNET

Invitation til samarbejde

- Sektorstrategien sætter overskrifterne
- Prioriteringsrum under overskrifter
- Hvor kan vi i DCIS skabe mest værdi?
- Meget gerne input fra sektorens virksomheder og interessenter

Nye regler mv.

- Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.

Revision af bilag 5

- Nye EBA retningslinjer om outsourcing

FINANSTILSYNET

Præcisering af krav til IT-sikkerhed – bilag 5

- Ændring af bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. Gældende fra 1. september 2019

- Indeholder flere detaljerede bestemmelser herunder risikostyring, adgangsstyring og beredskabsplanlægning

  - Politik for IT-risikostyring og risikoansvarlig (nyt krav i forhold til datacentraler)

  - Detaljerede krav til forretningsgange for bruger- og rettighedsstyring samt dokumentation af funktionsadskillelse. Krav om løbende klassificering og identificering af kritiske adgange på tværs af systemerne og om logning af kritiske systemadgange for at sikre en effektiv overvågning og rettidig sporing af uautoriseret aktivitet.

  - Detaljerede krav til IT-beredskabsplan, test og rapportering

FINANSTILSYNET

Nye EBA retningslinjer om outsourcing

- Nye EBA retningslinjer om outsourcing er offentliggjort 25. februar 2019

  - Behov for opdatering og ajourføring
  - Retningslinjerne erstatter CEBS' retningslinjer om outsourcing fra 2006
  - Retningslinjerne indarbejder og erstatter EBA's henstilling om brugen af cloud-tjenester

  - Gælder for kreditinstitutter, investeringsselskaber, betalingsinstitutter og e-pengeinstitutter

  - Retningslinjerne træder i kraft 30. september 2019
    - Retningslinjerne gælder ikke i dansk ret før de er implementeret

FINANSTILSYNET

Mere eksplicitte definitioner af centrale begreber

- Der er generelt tilsigtet en risikobaseret tilgang
  - Kompleksitet
  - Risici
  - Hvor kritisk og vigtig er aktiviteten?
  - Betydning for virksomhedens fortsatte drift

- Retningslinjerne sondrer mellem 3 situationer:
  - ”Tredjepartsservice”, ”Outsourcing af funktioner” og ”Kritisk eller vigtig outsourcing af funktioner”
  - Der gælder forskellige krav i de 3 forskellige situationer.

- ”Outsourcing”-begrebet:
  - Ethvert arrangement hvor en leverandør udfører en proces, ydelse eller aktivitet, der ellers ville være blevet foretaget af virksomheden

- En ”funktion” - En samlebetegnelse for processer, ydelser eller aktiviteter

Governance

- Retningslinjerne indeholder flere nye krav til governance og god ledelse, herunder:
  - Outsourcing-politik og indhold,
  - Beredskabsplaner
  - Interne revisionsfunktion
  - Dokumentationskrav
- Nye krav til proces for indgåelse af aftaler om outsourcing, herunder:
  - Præ-outsourcing analyser
  - Tilsynsmæssige krav til leverandør
  - Risikovurdering af outsourcing-arrangementet
  - Due diligence

Flere nye krav

- Også nye krav til Outsourcing-kontrakten, herunder:
  - Indhold i kontrakten
  - Vedrørende videreoutsourcing
  - Sikring af data og systemer
  - Adgangs-, informations- og revisionsrettigheder
  - Opsigelsesrettigheder

- Krav om overvågning af alle outsourcede funktioner

- Krav om exit-strategier og planer

- Krav til tilsynsmyndigheder/håndhævelse

FINANSTILSYNET

Krav vedrørende videreoutsourcing

- For kritisk eller vigtig outsourcing, hvor der kan ske videreoutsourcing, skal kontrakten blandt andet indeholde bestemmelser om:
  - Hvad er undtaget fra videreoutsourcing?
  - Hvilke betingelser skal være opfyldt ved videreoutsourcing?
  - Leverandørens tilsynsforpligtelser overfor underleverandører
  - Krav om at leverandøren skal indhente tilladelse hos virksomheden før videreoutsourcing af data
  - Leverandørens underretningspligter overfor virksomheden i tilfælde af videreoutsourcing
  - Sikring af muligheden for "the right to object" mod videreoutsourcing eller ved væsentlige ændringer, eller krav om eksplicit godkendelse
  - Sikre opsigelsesrettigheder, såfremt risikoen ved videreoutsourcingen overstiger et uønsket niveau

- Videreoutsourcing må kun tillades, såfremt underleverandøren overholder lovgivning og indgåede kontrakter samt tillader samme adgangs- og revisionsrettigheder, som krævet af leverandøren
- Leverandøren skal løbende overvåge underleverandøren
- Virksomheden skal udøve sine rettigheder "the right to object", hvis risikoen ikke kan accepteres, eller skal lade kontrakten ophøre

FINANSTILSYNET

Krav om sikring af data og adgangsrettigheder

- Krav om sikring af data og systemer:
  - Hvis relevant skal der for al outsourcing ske fornøden kontraktuel sikring af data og systemer
    - Der skal defineres data og systemkrav i outsourcing-kontrakten
    - Skal forholde sig til dataopbevaring, -beskyttelse, og –behandling, herunder bestemmelserne i GDPR

- Adgangs-, informations- og revisionsrettigheder:
  - Outsourcing-kontrakten skal indeholde bestemmelser om:
    - Intern audits adgang til at gennemgå de outsourcede funktioner
    - Henvisning til myndigheders mulighed for informationsindsamling og for at foretage undersøgelser
    - Adgang for myndigheder til at foretage inspektioner hos leverandøren
  - Der må ikke være begrænsninger for revisorers og myndigheders adgangs- og revisionsrettigheder

FINANSTILSYNET

Krav om exit-strategier og planer

Virksomheden skal have en exit-strategi for kritisk eller vigtige funktioner ved opsigelse, fejl og mangler, risikoforøgelse hos leverandør, fald i kvalitet:

- Exit-strategien skal være i overensstemmelse med outsourcing-politikken og beredskabsplaner
- Der skal udarbejdes exit-planer og identificeres alternative løsninger
- Yderligere krav til exit-strategien, herunder eksempelvis overvågningsindikatorer, der trigger iværksættelse af genopretningsplaner

Proces for dansk implementering

- Forventninger til implementeringsprocessen for de nye retningslinjer:
  - Kræver ændring på lov-, bekendtgørelses- og vejledningsniveau
  - Målet er, at reglerne skal træde i kraft samtidigt pr. 1. juli 2020
  - Sædvanlige høringsprocesser

- Finanstilsynet tager udgangspunkt i gældende dansk ret:
  - Lov, bekendtgørelse og vejledning skal efterleves uanset fremtidige ændringer

Nye EBA Guidelines på vej

- Nye EBA guidelines om ICT and security risk management,
- Som følge af den stigende afhængighed af IT, hvor trusselsudviklingen gør virksomhederne sårbare
- Indeholder krav til mitigering og styring af risici i relation til anvendelsen af Informations- og kommunikationsteknologi
- Kommer til at gælde for kreditinstitutter, visse investeringsinstitutter i henhold til CRD, samt betalingstjenesteudbydere i henhold til PSD2
- Risikobaseret tilgang og proportionalitet

Indeholder flere detaljerede krav

- Retningslinjerne har et højere detaljeringsniveau, giver mere vejledning, og indeholder flere specifikke krav inden for følgende områder:

  - Governance and strategy
  - Risk management framework
  - Information security
  - Operations management
  - Project and Change management
  - Business continuity management

  Indeholder bl.a. specifikke krav vedr.

  - Three lines of defence
  - Revision af governance, systemer og processer

FINANSTILSYNET

EBA guidelines om ICT and security risk management

- EBA's Public consultation blev afsluttet den 13. marts 2019 og der arbejdes på at færdiggøre de endelige retningslinjer.

- Der er endnu ikke taget stilling til dansk implementering, men arbejdet igangsættes når retningslinjerne er offentliggjort i endelig version.

- Læs mere på: https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management

FINANSTILSYNET

Opsamling

Øget IT-anvendelse

Højt trusselsniveau

Mere regulering på vej

Løsningen er ikke...

...den her strategi...