Forskning i trygge rammer

Delstrategi for Cyber- og Informationssikkerhed 2022-2024

Januar 2023

Uddannelses- og Forskningsstyrelsen

Udgivet af Uddannelses- og Forskningsstyrelsen
Haraldsgade 53
2100 København Ø
Tel.: 7231 7800
ufs@ufm.dk
www.ufm.dk

Publikationen kan hentes på ufm.dk/publikationer
ISBN (elektronisk publikation): 978-87-94128-56-8

Forskning i trygge rammer

Delstrategi for Cyber- og Informationssikkerhed 2022-2024

Januar 2023

Indhold

1.	Forord	5
2.	Indledning	6
3.	Universitetssektoren	8
4.	Truslen mod universitetssektoren	11
5.	Universiteternes Strategiske Pejlemærker	14
6.	Initiativer på universiteterne	16
7.	UFM som rummyndighed	19
8.	Initiativer på rumområdet	21
9.	Samarbejde på tværs	22
10.	Opfølgning og evaluering	23
11.	Litteraturliste	24

Bilag:
Bilag 1: Delstrategiens pejlemærker og initiativer

1. Forord

Vi lever i en verden, hvor digitaliseringen har været med til at skubbe grænserne for, hvad der er muligt at udrette. På én og samme tid er det væsentligt, at vi omfavner digitaliseringens gevinster, uden at vi går på kompromis med den sikkerhed og tryghed, som vi alle er afhængige af. For mens gevinsterne er åbenbare, må vi erkende, at der følger nye udfordringer med – nemlig en stigende trussel fra cyberangreb. En trussel der er vedvarende og i konstant udvikling og derfor vigtig at være på forkant med. Det gælder for samfundet generelt, og det gælder for uddannelses- og forskningssektoren specifikt.

For alle institutioner og aktører under Uddannelses- og Forskningsministeriets område udgør cyberangreb en reel risiko mod deres forretningskritiske processer. Universiteterne, professionshøjskolerne, erhvervsakademierne, de kunstneriske og de maritime institutioner samt aktører, der arbejder med videnbaseret innovation, har alle fokus på digital sikkerhed som en daglig og nødvendig opgave for at sikre deres drift og udøvelsen af deres kerneopgaver.

Med den nationale strategi for cyber- og informationssikkerhed 2022-2024 styrkedes cyber- og informationssikkerheden på tværs af samfundets sektorer med fokus på beskyttelsen af samfundsvigtige funktioner. For uddannelses- og forskningssektoren adresseres det sektorspecifikke fokus med denne delstrategi, som er målrettet forskningsområdet. Det er dog forhåbningen, at delstrategiens pejlemærker og initiativer kan tjene til inspiration på tværs af sektorens andre aktører inden for uddannelse og innovation.

Delstrategien forholder sig endvidere til det nationale og internationale samarbejde på rumområdet, for så vidt angår cyber- og informationssikkerhed. Rumbaseret infrastruktur understøtter mange tjenester, der leveres i Danmark, fra kommunikation til transport og finansielle transaktioner. Dermed understøtter infrastrukturen en lang række samfundsvigtige funktioner på tværs af sektorerne.

God læselyst!

Christina Egelund
Uddannelses- og forskningsminister

2. Indledning

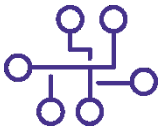
Digitalisering og globalisering er grundvilkår i det moderne samfund, vi kender i dag. I kølvandet på digitaliseringen følger en vedvarende trussel fra cyberspace. For uddannelses- og forskningssektoren betyder dette blandt andet en øget risiko for cyberspionage og cyberkriminalitet[1]. I denne delstrategi adresseres disse udfordringer med en række initiativer tilpasset sektorens behov og særkender.

Dermed understøtter delstrategien en række strategiske målsætninger formuleret i den nationale strategi for cyber og informationssikkerhed 2022-2024. Ligeledes vil delstrategien understøtte et tværsektorielt samarbejde på området. Dette samarbejde forankres i en decentral enhed for cyber- og informationssikkerhed (DCIS-UFM), der etableres i Uddannelses- og Forskningsstyrelsen.

Formålet med delstrategien er at styrke sektorens resiliens over for cyberangreb og sikre, at de funktioner, der er en forudsætning for samfundets generelle funktionsdygtighed, fortsat kan varetages. En kortlægning af sektorens samfundsvigtige funktioner har afdækket, at disse varetages på universiteterne. Derfor er denne strategi først og fremmest målrettet de danske universiteter, der ligeledes har bidraget til udarbejdelsen af delstrategiens pejlemærker og initiativer.

Cyber- og informationssikkerheden styrkes også gennem andre tiltag. Evnen til at øge samfundets og sektorens robusthed og resiliens er afhængig af, at vi har adgang til de nødvendige og rette kompetencer. De videregående uddannelsesinstitutioner er alle en drivkraft i at opbygge kompetencer inden for cyber- og informationssikkerhed, både med specialistviden og deres evne til at give et relevant perspektiv på tværs af faglige områder.

Cybersikkerhed
Cybersikkerhed dækker over it-sikkerhed for netværksforbundne it-systemer. Netværket kan være isoleret eller forbundet til andre netværk, som for eksempel internettet.



Informationssikkerhed
Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger, der sikrer informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. Inden for informationssikkerhed arbejdes der blandt andet med organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

[1] CFCS, "Truslen fra cyberspionage mod dansk forskning og universiteter", sept. 2021

Virksomheder, offentlige myndigheder og institutioner får adgang til den nyeste viden på cyber- og informationssikkerhedsområdet blandt andet gennem nyuddannede dimittender. Samtidig er der et stort behov for efter- og videreuddannelse på arbejdsmarkedet. For at styrke kompetenceopbygningen er der som led i den nationale strategi for cyber- og informationssikkerhed 2022-2024 udmøntet midler til at udvikle uddannelseselementer og styrke viden og samarbejde inden for cyber- og informationssikkerhedsområdet på de videregående uddannelsesinstitutioner.

For universiteterne er ambitionen, at et øget fokus på den digitale sikkerhed ligeledes vil bidrage til at styrke rammerne for og tilliden til dansk forskning fremadrettet.

Som den koordinerende myndighed på rumområdet, arbejder UFM hver dag på at sikre, at Danmark fortsat har de bedste forudsætninger for at kunne drage nytte af rummets mange muligheder. Med samfundets øgede afhængighed af rumbaserede tjenester, indebærer dette i stigende grad, at vi i vores strategier og daglige arbejde tænker sikkerhed og risici ind i opgaveløsningen. Delstrategien vil dermed adressere den stigende cybertrussel mod rumbaserede tjenester med tre konkrete initiativer, der har til formål at styrke det tværsektorielle samarbejde på rumområdet.

Samfundsvigtige funktioner
De aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed. De samfundsvigtige funktioner i uddannelses- og forskningssektoren varetages i overvejende grad af universiteterne. Derudover varetages også en række samfundsvigtige funktioner i forbindelse med UFMs rolle som koordinerende rummyndighed i Danmark.

3. Universitetssektoren

Formålet med delstrategiens pejlemærker og initiativer er at styrke beskyttelsen af de samfundsvigtige funktioner, som i væsentlig grad er it-understøttet. Cyber- og informationssikkerhedsmæssige tiltag, der skal styrke beskyttelsen af de samfundsvigtige funktioner i sektoren, vil samtidigt styrke den digitale sikkerhed for universiteternes kerneopgaver og øvrige funktioner. Det gælder også forskningsdata og forskningsaktiviteter i det hele taget, som er helt centrale for universiteternes virke, og som ligeledes er udsat for et højt trusselsniveau fra cyberspace. Derfor tjener delstrategiens pejlemærker og initiativer også mere end ét formål for universiteterne.

3.1 Kerneopgaver

I fremtiden står Danmark som resten af verden over for en lang række udfordringer, der skal løses inden for eksempelvis klima, energi, sundhed mv. Her spiller forskning og videnbaseret innovation en central rolle i at afdække behov og skabe løsninger på lokale, nationale og globale udfordringer.

Forskning danner ligeledes det faglige grundlag for universiteternes forskningsbaserede uddannelser, der tilfører ny viden til alle dele af arbejdsmarkedet såvel private og offentlige virksomheder. Det sker både gennem ansættelse i etablerede virksomheder med et innovations- og udviklingsbehov og -potentiale, samt gennem iværksætteri, hvor nyskabelse er med til at skabe et fundament for vækst i samfundet.

3.2 Særkender

Delstrategien skal tage højde for universiteternes særlige kendetegn, som er forskningsfrihed, åbenhed og internationalt samarbejde. Disse faktorer er afgørende for, at forskningen kan trives og udvikles. Det er samtidig grundpræmisser, der medfører en række sårbarheder, som delstrategien skal være med til at håndtere og imødegå med passende tiltag.

Forskningsfriheden er helt central for forskningens væsen. Forskningsfrihed betyder blandt andet, at forskerne har mulighed for selv at vælge emner, materialer og metoder i tilrettelæggelsen af deres forskning. Deraf følger også et særligt behov for, at forskere kan vælge digitale løsninger, som ikke er en standardvare. Dette skal der også være mulighed for fremadrettet.

Kendetegnet for universiteterne er, at de er åbne og samfundsbærende institutioner. Det er en del af deres formålsbeskrivelse, at de skaber og deler viden og forskningsresultater, nationalt og internationalt.

Det nationale og internationale samarbejde er helt afgørende for at sikre forskning i Danmark af høj kvalitet. Samarbejdet giver adgang til udenlandske forskningsmiljøer, forskningsinfrastruktur og data mv. Samtidig tiltrækker danske forskningsmiljøer og infrastruktur udenlandske forskere. Den internationale mobilitet blandt videnskabeligt personale er en forudsætning for den fortsatte styrkelse af forskningskvalitet og videnbaseret innovation.

Udvalg om Retningslinjer for International forsknings- og Innovationssamarbejde (URIS)
Etiske, økonomiske og sikkerhedsmæssige risici har gjort internationalt samarbejde på forsknings- og innovationsområdet mere komplekst det seneste årti, ligesom spionage i højere grad end tidligere udgør en trussel. I maj 2022 udkom URIS med en række anbefalinger og et sæt konkrete retningslinjer, der kan understøtte danske uddannelses- og forskningsinstitutioner i deres internationale samarbejde.

De seneste år har vist nødvendigheden af en øget bevidsthed om den overordnede tilgang til forskningssamarbejde, særligt med internationale samarbejdspartnere. Det fremgår af afrapporteringen fra Udvalg om Retningslinjer for International Forsknings- og Innovationssamarbejde (URIS) fra maj 2022, der netop fremhæver behovet for relevante sikkerhedsmæssige tiltag i universitetssektoren, som i højere grad end tidligere er nødt til at overveje etiske, økonomiske og sikkerhedsmæssige risici[2], herunder også som følge af truslen om cyberspionage.

Den meget høje trussel mod universitetssektoren taget i betragtning, vil øget fokus på den digitale sikkerhed være med til at styrke rammerne for forskning fremadrettet. God forskningspraksis og principper om høj sikkerhed vil understøtte, at danske forskere og forskningsinstitutioner forbliver attraktive samarbejdspartnere fremadrettet og vil styrke tilliden til dansk forskning i ind- og udland. Derved sikres det, at danske forskere og forskningsinstitutioner fortsat kan være garanter for excellent forskning.

For delstrategiens pejlemærker og initiativer er der derfor fokus på at styrke rammerne, så de er tidssvarende og understøtter, at forskningen kan foregå i trygge og sikre (digitale) rammer, hvilket vil styrke fremtidens forskning.

[2] Se URIS-rapport, maj 2022.

3.3 Universiteternes samarbejde med DeiC

En velfungerende it-infrastruktur er afgørende for at sikre opretholdelsen af samfundsvigtige funktioner samt fortroligheden, integriteten og tilgængeligheden af universiteternes forskningsdata.

En del af den infrastruktur sikres gennem Danish e-Infrastructure Cooperation (DeiC). DeiC er et samarbejde mellem Uddannelses- og Forskningsministeriet og de danske universiteter og har til formål at sikre regnekraft, datalagring og netværksinfrastruktur til dansk forskning og uddannelse.

Den digitale forskningsinfrastruktur, forskningsnettet, forbinder danske universiteter og forskningsinstitutioner med forskningsnet verden over. Dermed er DeiC medvirkende til at sikre et højt cyber- og informationssikkerhedsniveau i universitetssektoren. Der vil derfor også være et samspil med DeiC ved implementering af og opfølgningen på delstrategien.

4. Truslen mod universitetssektoren

Ligesom de øvrige sektorer i Danmark er universitetssektoren udsat for en vedvarende trussel fra cyberangreb, og ligesom i de øvrige sektorer kan denne trussel manifestere sig på forskellige måder. Som den nationale myndighed på cybersikkerhedsområdet udarbejder Center for Cybersikkerhed (CFCS) årlige trusselsvurderinger med fokus på cybertruslen i Danmark. Dertil blev der i efteråret 2021 publiceret en sektorspecifik trusselsvurdering for uddannelses- og forskningssektoren[3].

Aktuelt vurderer CFCS, at de to største trusler mod universitetssektoren i Danmark er cyberspionage og cyberkriminalitet. Truslen fra cyberaktivisme vurderes at være middel blandt andet som følge af krigen i Ukraine, mens truslen fra destruktive cyberangreb vurderes som lav.

Trusselsvurdering	
Cyberspionage	Meget høj
Cyberkriminalitet	Meget høj
Cyberaktivisme	Middel
Destruktive angreb	Lav

Når CFCS vurderer en trussel som meget høj, betyder det, at der er en specifik trussel, og at der eksisterer både kapacitet, hensigt, planlægning og mulig iværksættelse.

4.1 Truslen fra cyberspionage mod universitetssektoren

Spionagetruslen udgør en særlig trussel for universitetssektoren. Motiver og mål kan variere, men baseret på konkrete sager i ind- og udland ses det, at visse forskningsområder er mere udsatte end andre. Det er for eksempel områder inden for sikkerheds- og udenrigspolitik, herunder Arktis.[4] Der har også været mål inden for forskningsområder som økonomi, sundhed, kemi, fysik, geologi, miljø og transport[5]. Teknologisk viden, der vurderes at kunne have militære anvendelsesmuligheder, er ligeledes et attraktivt mål for fremmede stater.

At spionagetruslen mod universitetssektoren i Danmark er højaktuel og har været det i en årrække, adresseres af såvel en Rigsrevisionsberetning fra

[3] CFCS, "Truslen fra cyberspionage mod dansk forskning og universiteter", sept. 2021
[4] Ibid., s. 6
[5] PET/UFM, "Er jeres forskning i fare?", 2021 s. 5

2018[6], samt af URIS-rapporten fra maj 2022. Rigsrevisionen fremhævede, med udgangspunkt i en erkendelse af truslen fra cyberangreb og cyberspionage, at universiteterne skulle styrke beskyttelsen af deres forskningsdata. URIS-rapporten konkluderer blandt andet, at internationalt forsknings- og innovationssamarbejde er blevet mere komplekst, og at spionage udgør en stigende udfordring.

"Truslen mod dansk forskning er reel. Gennem de senere år har der været fere eksempler på spionage og anden udenlandsk indblanding. Dansk forskning har en tradition for stor åbenhed og et bredt internationalt samarbejde og kan derfor anses for at være et relativt nemt mål for fremmede stater. Samtidig er Danmark et attraktivt mål på grund af sit høje forskningsmæssige niveau og sin geopolitiske placering"

- PET/UFM, "Er jeres forskning i fare?" 2021

4.2 Truslen fra insidere mod universitetssektoren

Tæt forbundet med truslen om cyberspionage er truslen fra Insidere. Ifølge DKCERT (Danish Computer Security Incident Response Team), som håndterer sikkerhedshændelser på forskningsnettet, vurderes denne trussel at være meget høj for universiteterne. Insidere er ansatte, der via deres handlinger kan kompromittere fortroligheden, integriteten eller tilgængeligheden af universiteternes forskningsdata. Dette kan ske både som bevidste, ondsindede handlinger (eksempelvis spionage), eller det kan ske ubevidst og/eller uagtsomt. Det store antal forskere og studerende fra ind- og udland på universiteterne fordrer, at der er fokus på at styrke tiltag, der kan minimere risikoen herfra.

4.3 Truslen fra cyberkriminalitet og cyberaktivisme mod universitetssektoren

Ved cyberkriminalitet er der typisk tale om aktører, der er bevæger sig i spektret inden for tyveri, bedrageri og afpresning[7]. Ligesom truslen fra cyberspionage udgør disse aktører en vedvarende trussel for universiteternes forretningsprocesser og forskningsdata. Det skyldes eksempelvis deres brug af ransomware, hvorved data og systemer bliver gjort utilgængelige for offeret, ofte ved kryptering, og derved holdt som gidsel. Da universiteterne beskæftiger mange studerende og ansatte, har kriminelle mange indgangsvinkler til universiteternes systemer.

Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver. Cyberaktivister kan fokusere på enkeltsager, personer eller organisationer,

[6] Se Rigsrevisionens Beretning 8/2018 vedr. universiteternes beskyttelse af forskningsdata
[7] CFCS, "Cybertruslen mod Danmark", 2022

som de opfatter som modstandere af deres sag. Trusselsvurderingen har tidligere været lav, men i kraft af krigen i Ukraine, er der set en stigning af cyberaktivisme mod NATO-lande.

5. Universiteternes strategiske pejlemærker

Strategiens pejlemærker og initiativer er afledt af kendskabet til truslerne, og de risici, de udgør for de samfundsvigtige funktioner og universiteternes forskningsaktiviteter.

Arbejdet med cyber- og informationssikkerheden i den kommende strategiperiode (2022-2024) vil tage udgangspunkt i nedenstående strategiske pejlemærker.

Under strategiperioden vil universiteterne ligeledes arbejde på at etablere et CERT-samarbejde med en klar governance-struktur.

1 - Ledelsesforankring

Cyber- og informationssikkerhed skal være forankret i universiteternes topledelse, og modenheden omkring cyber- og informationssikkerhed skal styrkes i alle organisatoriske lag, da den ledelsesmæssige prioritering er uløseligt forbundet med cyber- og informationssikkerhed.

2 - Høj sikkerhed som en nødvendig forudsætning

For at beskytte universiteternes åbne kultur er evnen til at identificere områder og informationer, som skal beskyttes, nøglen til høj sikkerhed. Universiteterne bør i forlængelse af den nationale strategi for data management, baseret på FAIR-principper, udvikle processer og procedurer, som understøtter evnen til at identificere områder og informationer, som skal beskyttes.

3 - Strategien skal understøtte og udvikle den risikobaserede tilgang

De 8 universiteter varierer i størrelse, organisering og forskningsområder. En risikobaseret tilgang skal derfor sikre den bedst mulige underbygning af arbejdet med cyber- og informationssikkerhed på det enkelte universitet.

4 - Styrket samarbejde og koordinering på tværs af sektoren

Samarbejde og koordinering om initiativer og standarder for cyber- og informationssikkerhed på tværs af sektoren skal dels sikre gennemsigtighed og understøtte mobilitet i sektoren for forskere, studerende, og samarbejdspartnere samt sikre den bedst mulige udnyttelse af de tilgængelige kompetencer på tværs af sektoren.

6. Initiativer på universiteterne

1 – Ledelsesforankring

Initiativ 1.1: Ledelsesforankring med udgangspunkt i den enkelte organisations risikoappetit og med øget fokus på tidssvarende risikostyring

Cyber- og informationssikkerhed skal være forankret i ledelsen på de enkelte universiteter. Dette udmøntes via løbende stillingtagen til risikoappetitten hos de enkelte universiteter, således at sikkerhedsmæssige udfordringer mødes rettidigt og balanceret i forhold til det aktuelle trusselsbillede.

Initiativ 1.2: Øget modenhed i forhold til cyber- og informationssikkerhed

Universiteternes ledelser foretager en løbende stillingtagen til det ønskede niveau af modenhed inden for cyber- og informationssikkerhed, som indlejres som en del af den strategiske forretningsudvikling.

Initiativ 1.3: Øget strategisk målbarhed på sikkerheds- og modenhedsniveauet

For at sikre at de cyber- og informationssikkerhedsmæssige tiltag i universitetssektoren opnår de ønskede mål, er det nødvendigt med et fokus på målbarhed af effekt. For at kunne opbygge det mest retvisende billede af hele sektoren, er det vigtigt, at tiltag på de enkelte universiteter måles på baggrund af sammenlignelige kriterier.

2 - Høj sikkerhed som en nødvendig forudsætning

Initiativ 2.1: Håndtering af universiteternes specifikke omstændigheder

Universiteternes arbejde med cyber- og informationssikkerhed er påvirket af en række specifikke omstændigheder, som har indflydelse på mulige sikkerhedsmæssige initiativer og restriktioner. Udvælgelsen af passende organisatoriske og tekniske foranstaltninger er derfor underlagt det grundvilkår, at en højere grad af frihed kan være en nødvendighed for opfyldelsen af sektorens lovfastsatte formål.

Initiativ 2.2: Detektion og påvisning

Oparbejdelse af kompetencer og redskaber blandt universitetssektorens medarbejdere til at opdage og påvise hændelser på universiteternes netværk er en grundlæggende forudsætning for at kunne styrke universitetssektorens arbejde med cyber- og informationssikkerhed.

3 - Strategien skal understøtte og udvikle den risikobaserede tilgang

Initiativ 3.1: Løbende trussels- og risikoanalyser for universitetssektoren

Arbejdet med cyber- og informationssikkerhed på universiteterne vil tage afsæt i universiteternes egne, løbende trussels- og risikovurdering, tværgående vurderinger, DKCERT's sektorspecifikke trusselsvurderinger og CFCS' analyse af det generelle trusselsbillede.

Initiativ 3.2: Løbende risikovurderinger af kritisk it-infrastruktur der understøtter samfundsvigtige funktioner

For at sikre en målrettet tilgang i arbejdet med cyber- og informationssikkerhed er det nødvendigt løbende at genbesøge, og revurdere kortlægningen af den it-infrastruktur, der understøtter de samfundsvigtige funktioner. DCIS-UFM er ansvarlig for årligt at opdatere kortlægning i samarbejde med universiteterne.

Initiativ 3.3: Øget indsigt i trusler og konsekvenser hos forskerne

Det er ikke længere tilstrækkeligt, at kendskabet til trusselsniveau og muligheder for udmøntning af trusler findes på ledelses- og/eller teknisk niveau. Der er brug for, at også universiteternes ansatte, herunder forskere, får et øget kendskab til cyber- og informationssikkerhedsmæssige aspekter af den verden, de bevæger sig i, således at de kan være med til at højne sikkerheden omkring deres videnskabelige fremdrift.

Initiativ 3.4: Løbende vurdering om universiteternes tilslutning til CFCS' sensornetværk

Tilslutning til CFCS' sensornetværk overvejes for samfundsvigtige aktiviteter ift. risiko- og trusselseksponering og proportionalitet. I vurderingen heraf tages afsæt i en konkret risikovurdering af it-understøttelsen af sektorens

samfundsvigtige funktioner. Den endelige beslutning om tilslutning tages af universiteternes øverste daglige ledelse og vil ske i dialog med CFCS.

4 - Styrket samarbejde og koordinering på tværs af sektoren

Initiativ 4.1: Etablering af operativ DCIS

For at sikre koordineret håndtering af tværgående hændelser oprettes på ministerområdet en operativ DCIS, der kan sikre videndeling om cyber- og informationssikkerhed omkring it-understøttelsen af de samfundsvigtige funktioner samt koordinere håndteringen af tværgående hændelser.

Initiativ 4.2: Deling af viden om aktuelle trusler med relevante fora

For at understøtte opdagelse og håndtering af sikkerhedshændelser skal universitetssektoren dele sin viden om aktuelle trusler i relevante fora. Behovet for videndeling og oprettelsen af nye fora skal afdækkes.

Initiativ 4.3: Styrket sikkerhedstilsyn med systemleverandører og databehandlere

For at højne cyber- og informationssikkerheden vil universitetssektoren, evt. i samarbejde med CFCS, afdække mulighederne for at udvikle fælles sikkerhedskrav til systemleverandører og databehandlere samt styrke sikkerhedstilsyn med disse.

Initiativ 4.4: Intelligent overvågning

Det er vigtigt at have et højt fælles niveau for overvågning samt klare kommunikationslinjer, beredskabs- og handleplaner i tilfælde af en sikkerhedshændelse. Herved kan en hændelse hurtigt inddæmmes, og en evt. spredning i sektoren forhindres. Behovet herfor, samt behovet for at kunne tilgå og kommunikere klassificerede oplysninger, skal afdækkes. For så vidt angår beredskabsaftaler og sikkerhedsgodkendelser i forbindelse med tilgangen til klassificerede oplysninger, vil der blive foretaget løbende ajourføring.

Initiativ 4.5: Tværuniversitære awareness-fremmende tiltag

Der skal i højere grad sikres en ensartet og genkendelig awareness-strategi på tværs af universiteterne, der kan medvirke til at skabe en større sammenhængskraft, eksempelvis når en forsker flytter mellem danske universiteter.

7. UFM som rummyndighed

Hver dag er rumbaseret teknologi med til at understøtte en lang række funktioner på tværs af landets sektorer, der har afgørende betydning for samfundets generelle funktionsdygtighed. Dette gælder for eksempel opgaver inden for kommunikation, finansielle transaktioner, sikkerhed og beredskab samt navigation til lands, til vands og i luften. Med sin globale dækning, høje digitaliseringsgrad og teknologiske udviklingsområder skaber rumbaseret teknologi ligeledes nye muligheder inden for den grønne omstilling. Dermed er en stabil og sikker infrastruktur på området afgørende for mange af landets samfundskritiske og samfundsvigtige sektorer.

Som den koordinerende myndighed på området arbejder Uddannelses- og Forskningsministeriet hver dag på at sikre, at Danmark fortsat har de bedste forudsætninger for at kunne drage nytte af rummets mange muligheder. Med samfundets øgede afhængighed af rumbaserede tjenester indebærer dette i stigende grad, at vi i vores strategier og daglige arbejde tænker sikkerhed og risici ind i opgaveløsningen.

Vi står i dag i en sikkerhedspolitisk situation, der skaber nye udfordringer for brugen af rumbaserede tjenester. Et øget og mere sofistikeret trusselsbillede stiller krav til sikkerheden og robustheden af både satellitterne, såvel som de tilknyttede jordstationer, brugernes modtagerudstyr og signalerne herimellem. Truslerne kan være alt fra soludbrud, kollision af satellitter, til egentlige ondsindede handlinger, herunder cyberangreb. For eksempel bevidnede vi i februar 2022, hvordan cyberangreb mod Viasats satellitbaserede tjenester påvirkede borgere, myndigheder og virksomheder i store dele af Europa.

Det dynamiske trusselsbillede er adresseret i Danmarks seneste strategi for rumområdet, hvor der blandt andet rettes fokus mod Danmarks bidrag til den europæiske rumsikkerhed. Ligeledes arbejdes der fortsat på at styrke samarbejdet på tværs af landets sektorer. Netop rummets brede anvendelsesmuligheder nødvendiggør et fokus på tværsektorielt samarbejde, dels for at sikre bedst mulige vilkår for videndeling og erfaringsudveksling, og dels

for at muliggøre udarbejdelsen af et fyldestgørende trusselsbillede på rumområdet.

Med afsæt i den nationale strategi for cyber- og informationssikkerhed, arbejdes der på at etablere en tværministeriel taskforce, der har til formål at se på, hvordan Danmark kan styrke sit bidrag til cybersikkerheden i den europæiske rumbaserede infrastruktur. I den indeværende strategiperiode vil sektorens DCIS understøtte dette arbejde, der er forankret i Uddannelses- og Forskningsstyrelsen.

8. Initiativer på rumområdet

For at understøtte det fremadrettede arbejde med at styrke cyber- og informationssikkerheden på rumområdet præsenteres der 3 initiativer, som danner rammen for det overordnede fokus i indeværende strategiperiode 2022-2024.

Initiativ 5.1: Understøtte arbejdet omkring styrkelse af Danmarks bidrag til cybersikkerheden i den europæiske rumbaserede infrastruktur

Konkret vil sektorens DCIS yde rådgivning og sparring til Uddannelses- og Forskningsstyrelsen og den tværministerielle rumtaskforce.

Initiativ 5.2: Skabe øget bevidsthed om cybertruslen

Sektorens DCIS vil bidrage til en øget bevidsthed på tværs af sektorerne om samfundsvigtige funktioners afhængighed af rumbaserede tjenester og sårbarheder over for cyberangreb.

Initiativ 5.3: Bidrage til udarbejdelsen af et trusselsbillede for rumområdet

Sektorens DCIS vil arbejde på at etablere et tværsektorielt DCIS-samarbejde, hvor fokus er på videndeling og erfaringsudvikling. Konkret vil sektorens DCIS søge at skabe en kortlægning af samfundskritiske og samfundsvigtige funktioners afhængighed af rumbaserede tjenester, samt cybertruslen mod disse.

9. Samarbejde på tværs

National strategi for cyber- og informationssikkerhed pålægger hvert ministerområder med ansvar for samfundsvigtige funktioner at etablere en operativ decentral cyber- og informationssikkerhedsenhed (DCIS). DCIS-UFM etableres i løbet af 2023 og placeres i Uddannelses- og Forskningsstyrelsen.

DCIS-UFM har flere formål. Dels skal den sikre evnen til at koordinere håndtering af tværgående it-relaterede hændelser med CFCS, sektorens berørte aktører og andre DCIS'er. Det skyldes ikke mindst, at truslen om cyberangreb påvirker samfundet på tværs, og at der derfor er brug for et øget fokus på tværsektorielt samarbejde.

Derudover vil DCIS-UFM være en samlende sektorenhed for viden om cyber- og informationssikkerhed og vil ligeledes understøtte det fremadrettede arbejde med cyber- og informationssikkerhed i sektoren, herunder implementering af delstrategiens pejlemærker og initiativer.

Der nedsættes en styregruppe som tilknyttes DCIS-UFM, sammensat af aktører fra sektoren samt Uddannelses- og Forskningsministeriet. Styregruppen agerer som referencegruppe og får til opgave løbende at bidrage med faglig sparring, rådgivning og anbefalinger til Uddannelses- og Forskningsministeriets cyber- og informationssikkerhedsindsats i sektoren. Det kan eksempelvis være ved at forholde sig til behovet for ny lovgivning på området. Styregruppen udgøres af personer fra sektoren på ledelsesniveau, hvilket er med til at sikre den ledelsesforankrede styring af cyber- og informationssikkerhed på tværs af sektoren.

10. Opfølgning og evaluering

Udarbejdelsen af delstrategien for cyber- og informationssikkerhed sker på baggrund af en konkret trussel fra cyberspace. Det er en trussel, som er under kontinuerlig udvikling, og som løbende præsenterer sektoren for nye udfordringer.

I indeværende strategiperiode er der en opgave med at modne sektorens fælles indsats på cyber- og informationssikkerhedsområdet. Undervejs i strategiperioden vil der blive gjort konkrete erfaringer med de forskellige indsatser, ligesom nye trusler, risici og sårbarheder vil vise sig. For effektivt at kunne imødegå både nuværende og fremtidige trusler er det væsentligt, at der aktivt og løbende følges op og evalueres på delstrategiens rammer og indsatser.

Sektorens DCIS vil i samarbejde med styregruppen og relevante aktører og myndigheder løbende samle op på de erfaringer og den viden, der skabes og indsamles. Det vil ligge til grund for en tilpasning og effektivisering af cyber- og informationssikkerheden i sektoren.

11. Litteraturliste

- Center for Cybersikkerhed (CFCS), "Cybertruslen mod Danmark", juni 2022
- Iris Group, "Når forskning og uddannelse bliver til nye virksomheder", 2022.
- Danmarks Statistik, "Forskning, udvikling og innovation 2022", 2022.
- Udvalget om Retningslinjer for Internationalt Forsknings- og Innovationssamarbejde (URIS), Afrapportering maj 2022
- CFCS, "Truslen fra cyberspionage mod dansk forskning og universiteter", sept. 2021
- PET/UFM, "Er jeres forskning i fare?", 2021
- Rigsrevisionsberetning 8/2018 – Beretning om Universiteternes beskyttelse af forskningsdata
- https://www.maastrichtuniversity.nl/news/update-cyber-attack-um
- https://www.tu.berlin/en/topics/restricted-it-services
- https://www.cert.dk/da/news/2022-06-28/Vice-Society-tager-ansvar-for-ransom-ware-angreb-paa-universitet
- https://www.fmn.dk/da/nyheder/2022/rusland-star-bag-destruktivt-cyberangreb-mod-satellitudstyr-i-forbindelse-med-invasionen-af-ukraine/

Bilag 1. Pejlemærker og initiativer.

UNIVERSITETSSEKTOREN

1 Ledelsesforankring

Cyber- og informationssikkerhed skal være forankret i universiteternes topledelse og modenheden omkring cyber- og informationssikkerhed skal styrkes i alle organisatoriske lag, da den ledelsesmæssige prioritering er uløseligt forbundet med cyber- og informationssikkerhed.

2 Høj sikkerhed som en nødvendig forudsætning

For at beskytte universiteternes åbne kultur, er evnen til at identificere områder og informationer som skal beskyttes, nøglen til høj sikkerhed. Universiteterne bør i forlængelse af den national strategi for data management, baseret på FAIR-principper, udvikle processer og procedurer som understøtter evnen til at identificere områder og informationer som skal beskyttes.

3 Strategien skal understøtte og udvikle den risikobaserede tilgang

De 8 universiteter varierer i størrelse, organisering og forskningsområder. En risikobaseret tilgang skal derfor sikre den bedst mulige underbygning af arbejdet med cyber- og informationssikkerhed på det enkelte universitet.

4 Styrket samarbejde og koordinering på tværs af sektoren

Samarbejde og koordinering om initiativer og standarder for cyber- og informationssikkerhed på tværs af sektoren skal dels sikre gennemsigtighed og understøtte mobilitet i sektoren for forskere, studerende, og samarbejdspartnere samt sikre den bedst mulige udnyttelse af de tilgængelige kompetencer på tværs af sektoren.

Initiativer

Initiativ 1.1: Ledelsesforankring med udgangspunkt i den enkelte organisations risikoappetit og med øget fokus på tidssvarende risikostyring

Cyber- og informationssikkerhed skal være forankret i ledelsen på de enkelte universiteter. Dette udmøntes via løbende stillingtagen til risikoappetitten hos de enkelte universiteter, således at sikkerhedsmæssige udfordringer mødes rettidigt og balanceret i forhold til det aktuelle trusselsbillede.

Initiativ 2.1: Håndtering af universiteternes specifikke omstændigheder

Universiteternes arbejde med cyber- og informationssikkerhed er påvirket af en række specifikke omstændigheder, som har indflydelse på rækkevidden af mulige sikkerhedsmæssige initiativer og restriktioner. Udvælgelsen af passende organisatoriske og tekniske foranstaltninger er derfor underlagt det grundvilkår, at en højere grad af frihed kan være en nødvendighed for opfyldelsen af sektorens lovfastsatte formål.

Initiativ 3.1: Løbende trussels- og risikoanalyser for universitetssektoren

Arbejdet med cyber- og informationssikkerhed på universiteterne vil tage afsæt i universiteternes egne løbende trussels- og risikovurdering, tværgående vurderinger, DKCERT's sektorspecifikke trusselsvurderinger og CFCS' analyse af det generelle trusselsbillede.

Initiativ 4.1: etablering af operativ DCIS

For at sikre koordineret håndtering af tværgående hændelser oprettes på ministerområdet en operativ DCIS, der kan sikre viden om cyber- og informationssikkerhed omkring it-understøttelsen af de samfundsvigtige funktioner samt koordinere håndteringen af tværgående hændelse.

UNIVERSITETSSEKTOREN

Initiativ 1.2: Øget modenhed i forhold til Cyber- og Informationssikkerhed

Universiteternes ledelser foretager en løbende stillingtagen til det ønskede niveau af modenhed indenfor cyber- og informationssikkerhed som indlejres som en del af den strategiske forretningsudvikling.

Initiativ 2.2: Detektion og påvisning

Oparbejdelse af kompetencer og redskaber blandt universitetssektorens medarbejdere til at detektere of påvise hændelser på universiteternes netværk er en grundlæggende forudsætning for at kunne styrke universitetssektorens arbejde med cyber- og informationssikkerhed.

Initiativ 3.2 Løbende risikovurderinger af kritisk it-infrastruktur der understøtter samfundsvigtige funktioner

For at sikre en målrettet tilgang i arbejdet med cyber- og informationssikkerhed er det nødvendigt løbende at genbesøge og revurdere kortlægningen af den it-infrastruktur, der understøtter de samfundsvigtige funktioner, som varetages af universiteterne. DCIS er ansvarlig for årligt at opdatere kortlægningen i samarbejde med universiteterne.

Initiativ 4.2: Deling af viden om aktuelle trusler med relevante fora

For at understøtte opdagelse og håndtering af sikkerhedshændelser skal universitetssektoren dele sin viden om aktuelle trusler i relevante fora. Behovet for videndeling og oprettelsen af nye fora skal afdækkes.

Initiativ 1.3: Øget strategisk målbarhed på sikkerheds- og modenhedsniveauet

For at sørge for at cyber- og informationssikkerhedsmæssige tiltag i universitetssektoren opnår de ønskede mål, er det nødvendigt med et fokus på målbarhed af effekt. For at kunne opbygge det mest retvisende billede af hele sektoren, er det vigtig at tiltag på de enkelte universiteter måles på baggrund af ens kriterier på tværs

Initiativ 3.3: Øget indsigt i trusler og konsekvenser hos forskerne

Det er ikke længere tilstrækkeligt, at kendskabet til trusselsniveau og muligheder for udmøntning af trusler findes på ledelses- og/eller teknisk niveau. Der er brug for, at også universiteternes ansatte, herunder forskere, får et øget kendskab til cyber- og informationssikkerhedsmæssige aspekter af den verden, de bevæger sig i, således at de kan være med til at højne sikkerheden omkring deres videnskabelige fremdrift.

Initiativ 4.3: Styrket sikkerhedstilsyn med systemleverandører og databehandlere

For at højne cyber- og informationssikkerheden vil universitetssektoren, evt. i samarbejde med CFCS, afdække mulighederne for at udvikle fælles sikkerhedskrav til systemleverandører og databehandlere samt styrke sikkerhedstilsyn med disse.

UNIVERSITETSSEKTOREN

Initiativ 3.4: Løbende vurdering om universiteternes tilslutning til CFCS' sensornetværk
Tilslutning til CFCS' sensornetværk overvejes for samfundsvigtige aktiviteter ift. risiko- og trusselseksponering og proportionalitet. I vurderingen heraf tages afsæt i en konkret risikovurdering af it-understøttelsen af sektorens samfundsvigtige funktioner. Den endelige beslutning om tilslutning tages af universiteternes øverste daglige ledelse og vil ske i dialog med CFCS.

Initiativ 4.4: Intelligent overvågning
Det er vigtigt at have et højt fælles niveau for overvågning samt klare kommunikationslinjer, beredskabs- og handleplaner i tilfælde af en sikkerhedshændelse. Herved kan en hændelse hurtigt inddæmmes og en evt. spredning i sektoren forhindres. Behovet herfor samt behovet for at kunne tilgå og kommunikere klassificerede oplysninger skal afdækkes. For så vidt angår beredskabsaftaler og sikkerhedsgodkendelser i forbindelse med tilgangen til klassificerede oplysninger vil der blive foretaget løbende ajourføring.

Initiativ 4.5: Tværuniversitære awareness-fremmende tiltag
Der skal i højere grad sikres en ensartet og genkendelig awareness-strategi på tværs af universiteterne, der kan medvirke til at skabe en større sammenhængskrav, eksempelvis når en forsker flytter mellem danske universiteter.

RUMOMRÅDET

Initiativ 5.1: Understøtte arbejdet omkring evt. styrkelse af Danmarks bidrag til cybersikkerheden i den europæiske rumbaserede infrastruktur

Sektorens DCIS vil yde rådgivning og sparring til Kontor for RUM og den tværministerielle taskforce.

Initiativ 5.2: Skabe øget bevidsthed om cybertruslen

Sektorens DCIS vil bidrage til en øget bevidsthed på tværs af sektorerne om samfundsvigtige funktioners afhængighed af rumbaserede tjenester og sårbarheder over for cyberangreb.

Initiativ 5.3: Bidrage til udarbejdelsen af et trusselsbillede for rumområdet

Sektorens DCIS vil arbejde på at etablere et tværsektorielt DCIS-samarbejde, hvor fokus er på øget videndeling og erfaringsudvikling. Konkret vil sektorens DCIS søge at skabe en kortlægning af samfundskritiske og samfundsvigtige funktioners afhængighed af rumbaserede tjenester, samt cybertruslen mod disse.