DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

# Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed

# Kolofon

**DKCERT Trendrapport 2023**

Redaktion: Henrik Larsen og Eskil Sørensen, DKCERT.
Redaktionen afsluttet den 1. april 2023

**Tak til vores bidragydere:**
Morten Eeg Ejrnæs Nielsen, Security Advisor, Globeteam A/S
Berit Aadal, Seniorkonsulent, Dansk Standard
Christa Wulff Sarby, Kommunikation & event, Sundhedssektorens DCIS

Grafisk design: Kiberg & Gormsen

DeiC-journalnummer: DeiC-JS 22/1005735-1
DKCERT - en del af DeiC
DTU, Asmussens Allé, Bygn. 305
2800 Kgs. Lyngby

# Om DKCERT

DKCERT er Danmarks akademiske CSIRT (Computer Security Incident Response Team). Vi bygger på en vision om at skabe værdi for uddannelses- og forskningssektoren i form af øget informationssikkerhed. Det sker gennem offentliggørelse af viden om informationssikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen samt internationale samarbejdspartnere.

Det er DKCERTs mission at skabe øget fokus på informationssikkerhed i uddannelses- og forskningssektoren ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DKCERT i stand til at offentliggøre og udsende varsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DKCERT overvåger det danske forskningsnet for uønskede aktiviteter, sender varsler ud til uddannelsesinstitutionerne, indsamler oplysninger om sårbarheder og foretager sårbarhedsscanninger af uddannelses- og forskningsinstitutioner. På denne baggrund udvikler DKCERT services, der skaber merværdi for institutionerne på forskningsnettet og sætter dem i stand til bedre at sikre deres it-systemer.

DKCERT leveres gennem DeiC, Danish e-Infrastructure Cooperation. DeiC koordinerer leverancen og udviklingen af den nationale digitale forskningsinfrastruktur i et samarbejde med og mellem de danske universiteter.

DKCERT – grundlagt 1. juli 1991 med grundidé fra CERT/CC i USA - var blandt pionererne i etablering af et internationalt samarbejde om informationssikkerhed. DKCERT er siden 1993 fuldt medlem af FIRST (Forum of Incident Response and Security Teams) som et af de første teams uden for USA og var i 2000 blandt grundlæggerne af, siden 2002 akkrediteret medlem og fra marts 2023 kandidat til certificeret medlemskab af, Trusted Introducer og TF-CSIRT (Task Force Computer Security Incident Response Team).[1]

[1] Se referenceliste i kapitel 7.

# Indholdsfortegnelse


**Indholdsfortegnelse** ..... **5**

**1. Velkommen** ..... **6**

**2. Trusselsvurdering 2023** ..... **8**
2.1. Danske universiteter er attraktive ..... 8
2.2. Situationsbilledet for academia ..... 9
2.3. Situationsbilledet generelt ..... 12
2.4. Truslen mod dansk forskning ..... 13
2.5. Vurderinger af cybertruslen ..... 15

**3. Året i tal og ord** ..... **18**
3.1 Scanninger, varsler, hændelser og tekniske analyser ..... 18
3.1.1 Sårbarhedsscanninger ..... 18
3.1.2 Varsler fra DKCERT ..... 21
3.1.3 Varsler fra tredjeparter ..... 21
3.1.4 Sikkerhedshændelser i 2022 ..... 23
3.1.5 Uddannelses- og forskningssektorens MISP – deler indsigt om events ..... 24
3.1.6 Dataanalyse ..... 25
3.1.7 SIE Europe ..... 25
3.1.8 Honeypot – nyt værktøj til analyse af angrebstyper ..... 25
3.2 Videndeling ..... 27
3.2.1 Videndeling ved hændelser ..... 27
3.2.2 Mattermost – det der betyder mest ..... 27
3.2.3 Faglig videndeling i netværk ..... 27
3.2.4 DKCERTs deltagelse i Cybersikkerhedsrådet ..... 28
3.2.5 Videndeling blandt ligesindede i Rådet for digital sikkerhed ..... 28
3.2.6 International videndeling ..... 28
3.2.7 Internationale arbejdsgrupper ..... 29
3.2.8 Nyhedsformidling ..... 30
Klummer på cert.dk ..... 31
3.3 Tjenester ..... 32
3.3.1 DPO-tjenesten ..... 32
3.3.2 Awarenestjenesten Phish kan teste agtpågivenheden overfor phishingtrusler ..... 33
3.3.3 Beredskabsøvelser – håndtér en hændelse som i den virkelige universitetsverden ..... 33

**4 Forskning i trygge rammer** ..... **34**

**5 Eksterne bidrag** ..... **37**
5.1 NIS2 er landet ..... 38
5.2 Ændringer i ISO/IEC 27000-standarderne skal gøre dem nemmere at anvende ..... 40
5.3 En beretning fra en DCIS ..... 42

**6 Trends og anbefalinger** ..... **45**
6.1 Cybertrends ..... 45
6.2 GDPR-trends ..... 47
6.3 Anbefalinger til ledelsen på uddannelses- og forskningsinstitutionerne ..... 50
6.4 Anbefalinger til forskere, undervisere og teknisk-administrativt personale på uddannelses- og forskningsinstitutionerne ..... 51
6.5 Anbefalinger til it-ansvarlige på uddannelses- og forskningsinstitutionerne ..... 51

**7 Referenceliste** ..... **52**

# 1. Velkomst

**Velkommen til DKCERTs Trendrapport 2023.**

Supply-chain-angreb på kritisk infrastruktur. NIS2-direktivet vedtaget. Ny ISO27001 og ny ISO27002. Cyber- og informationssikkerhedsstrategier til de fleste ministerområder og opbygning af DCIS'er. Talen om hybridkrig tager til og de fleste midler i angribernes værktøjskasse bruges for at opnå økonomiske, politiske eller strategiske mål. Cyberaktivisme rammer steder, hvor det bemærkes i den offentlige debat.

It-, cyber- og informationssikkerhed fået sit afgørende gennembrud, men det var ikke på grundlag af en pandemi og krig i verden, at vi sikkerhedsfolk ønskede det.

**Vidensformidling**
DKCERTs mission er skabe øget fokus på informationssikkerhed i uddannelses- og forskningssektoren ved at opbygge og skabe aktuel, relevant og brugbar viden. Den viden skal også formidles, fordi gennem en grundlæggende forståelse af sikkerhed om informationer kan vi skabe den beskyttelse, der er behov for.

Vi ønsker med trendrapporten at skabe forståelse for behovet for øget informationssikkerhed i uddannelses- og forskningssektoren. Traditionelt betragtes alle sikkerhedstiltag som noget, der udgår fra ledelsen, fordi ledelsen har beslutningskraften til at prioritere. Men prioritering af sikkerhed kan ikke klares af ledelsen alene, særligt ikke på vores områder, hvor så mange enkeltpersoner, institutter og studerende arbejder med eget stof og er de bedste og eneste til at have dybt nok kendskab til vigtigheden af forskningsområdet og de opnåede resultater. De skal også træffe beslutning om sikkerheden.

Derfor introducerer vi i trendrapporten 2022 en ny målgruppe: Nemlig de ansatte og forskerne på uddannelsesinstitutionerne. Dem har vi forsøgt at nå og givet anbefalinger til i slutningen af rapporten.

**Trendrapportens opbygning**
Trendrapporten 2023 er bygget op med udgangspunkt i trusselsvurderingen, som gennemgår de trusler, vi ser på baggrund af vores kilder, hændelser og materiale fra vores samarbejdspartnere. Vi har bygget vurderingen op ud fra den metode, som alle institutioner bør stræbe efter: Kend din organisation og data, vurder datas værdi for organisationen, og find ud af, hvor sårbar din organisation er over for trusler. Hold dig orienteret om tendenser i forhold til fx internationale hændelser, angreb og evt. kompromit-

# 1. Velkomst

tering af information i den sektor, du er en del af. Det siger noget om trusselsbilledet. Lær de relevante trusler at kende og sørg for at være bevidst om, hvordan truslerne kan ramme dine data – og stil foranstaltninger op, der kan virke imod truslerne – så risikoen for kompromittering bliver mindre.

Trusselsvurderingen fremgår af kapitel 2, og i kapitel 3 gennemgår vi de opgaver, som DKCERT har løftet i 2022 og de tjenester, vi stiller til rådighed for sektoren. Vi giver bl.a. en status på sektorens MISP og de observationer, vi kan se ud fra vores sårbarhedsscanninger. Vi introducerer tre nye tjenester: en honeypot, passiv DNS-service samt dataanalyse af 'unormal' trafik på forskningsnettet.

I kapitel 4 har vi valgt at gengive indledningen og initiativerne fra den nye cyber- og informationssikkerhedsstrategi for uddannelses- og forskningssektoren. Det gør vi for at bidrage med at udbrede den til så mange som muligt inden for vores sektor.

I kapitel 5 giver nogle af vores samarbejdspartnere bud på hhv. betydningen af NIS2 for sektoren, og hvordan nye udgaver af sikkerhedsstandarden ISO27001, implementeringsvejledningen ISO27002 og risikostyringsstandarden ISO27005 skal gøre det lettere at arbejde med sikkerhed. Endelig fortæller Sundhedsdatastyrelsen om, hvordan sektorens decentrale cybersikkerhedsenhed (DCISSund) har arbejdet i de sidste fire år. Uddannelses- og Forskningsstyrelsen har netop etableret en DCIS i 2022.

I kapitel 6 gennemgår vi de trends, vi ser inden for databeskyttelses- og cyber- og informationssikkerhedsområdet, og formidler de anbefalinger, vi anser for at være de vigtigste for vores sektor. Kapitel 7 indeholder en liste over en række af de aktører, som DKCERT nationalt og internationalt har berøring med.

Rigtig god fornøjelse med læsningen.

**Henrik Larsen**
Chef for DKCERT

# 2. Trusselsvurdering 2023

**Cybertruslen mod den danske uddannelses- og forskningssektor**

## 2.1. DANSKE UNIVERSITETER ER ATTRAKTIVE

På World University Research Ranking over universiteter i verden ligger tre danske universiteter på top 100.[2] Ranglisten baserer sig på en række forskellige parametre, bl.a. forskningens impact og universitetets evne til at samarbejde med andre forskningsinstitutioner, antallet af forskningspublikationer, samarbejde med industrien, virksomheder og myndigheder og på tværs af landegrænser.

En anden opgørelse viser, at tre danske universiteter er med blandt de ti mest aktive deltagere i EU's forsknings- og innovationsprogram, Horizon Europe. Danmarks Tekniske Universitet, Aarhus Universitet og Københavns Universitet er hhv. nummer 3, 4 og 6 på listen over de ti universiteter i Europa, der opnår flest midler til forskning fra programmet.[3]

Der findes en lang række målinger verden over og lige så mange metoder til at vurdere et universitets eller et lands universitetssektors placering på en rangliste. Andelen af publikationer inden for et givet felt og evnen til at samarbejde har utvivlsomt en betydning for kvaliteten af det arbejde, som et universitet udfører og dermed også dets placering på en evt. verdensrangliste. Det er vigtigt for en forskningsinstitution at vise sin produktivitet og være synlig; det kan tiltrække de mest talentfulde forskere og studerende. Det er også vigtigt for et lands konkurrenceevne at have en fremtrædende uddannelses- og forskningssektor.

Det indgår formentlig i de fleste universiteters strategier, at de aktivt skal søge internationale samarbejdspartnere i forhold til udvikling af nye løsninger og teknologier til at imødegå udfordringer for samfundet. Det kan fx være sundheds- og klimaudfordringer, der i disse år fylder meget i den offentlige debat.

Selv om ranglister skal tilgås med en vis kritisk sans,[4] er der næppe tvivl om, at dansk forskning har et højt fagligt niveau, og at danske forskningsinstitutioner er dygtige til at indgå i internationale samarbejder.[5]

Men at være aktiv opsøgende og attraktiv tiltrækker ikke kun venligtsindede forskningsinstitutioner fra det internationale forskningsmiljø.

Høj kvalitet har også en tiltrækkende effekt på fremmede stater, der ulovligt ønsker at tilegne sig og dermed lukrere på den viden, som danske universiteter har frembragt.

> 'Danmarks førerposition inden for visse teknologiske områder udgør et væsentligt indtægtsgrundlag for dansk økonomi, men den gør samtidig Danmark til et attraktivt mål for fremmede stater som Kina, Rusland og Iran, der gennem spionage, herunder statsfinansieret industrispionage, og ulovlig anskaffelsesvirksomhed forsøger at få fat i den nyeste viden og teknologi.'[6]

Samtidig indgår it-, teknologi og digitalisering som en grundlæggende forudsætning i danske universiteter og forskningsinstitutioners daglige arbejde. Undervisning, vejledning og gruppearbejder for de studerende foregår i højere og højere grad i hybride miljøer, hvor digitale værktøjer gør det muligt for universiteterne at komme bredere ud og være mere effektiv i sin opgaveløsning.

Også selve forskningen og forskningssamarbejderne med danske og udenlandske virksomheder og forskningsinstitutioner baserer sig på anvendelse af de nyeste teknologiske løsninger, hvilket også gør sig gældende for så vidt angår behandlingen af store mængder data til udvikling af nye metoder og teknologier til løsning af store samfundsmæssige udfordringer. Endelig er universiteterne og forskningsinstitutioner præget af et traditionelt åbent forskningsmiljø med studerende og gæsteforskere fra en lang række lande.

Disse karakteristika gør uddannelses- og forskningssektoren særligt udsat for trusselsaktørers interesse.

2 https://worldresearchranking.com/
3 https://ufm.dk/aktuelt/nyheder/2023/fornem-placering-til-dansk-universitetsforskning-i-horizon-europe
4 https://www.dtu.dk/english/about/facts-and-figures/rankings
5 https://ufm.dk/publikationer/2021/filer/er-jeres-forskning-i-fare-dk.pdf
6 https://ufm.dk/publikationer/2022/filer/uris-afrapportering-2022.pdf

# 2. Trusselsvurdering 2023

## 2.2. SITUATIONSBILLEDET FOR ACADEMIA

Generelt vurderes interessen fra trusselsaktører mod universitets- og forskningsmiljøet (academia) til at være stigende. Tal fra en lang række globale sikkerhedsvirksomheder peger på, at uddannelses- og forskningssektoren er udsat. Mest markant er sikkerhedsvirksomheden Checkpoints 2023 Cyber Security Report,[7] hvor det fremgår, at der i gennemsnit har været 2.314 angreb pr. uge mod organisationer inden for uddannelse og forskning. Det svarer til en stigning på over 40 pct. i forhold til 2021. Sundhedssektoren står for den største stigning med 74 pct. i forhold til året før, svarende til 1.463 angreb pr. uge i gennemsnit.

Rapporter fra andre sikkerhedsvirksomheder viser også stigninger, men placerer dog ikke sektoren så højt som Checkpoint gør. Ifølge Crowdstrike var academia den sjette mest udsatte sektor for cyberangreb, mens samme rapport fra 2022 'Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report' anslog, at academia var på femtepladsen over sektorer, der var mest udsat for 'interactive intrusion activity'.[8] Det fremhæves ligeledes, at der har været en mærkbar stigning i aktiviteten rettet mod sundheds- og universitetssektoren.

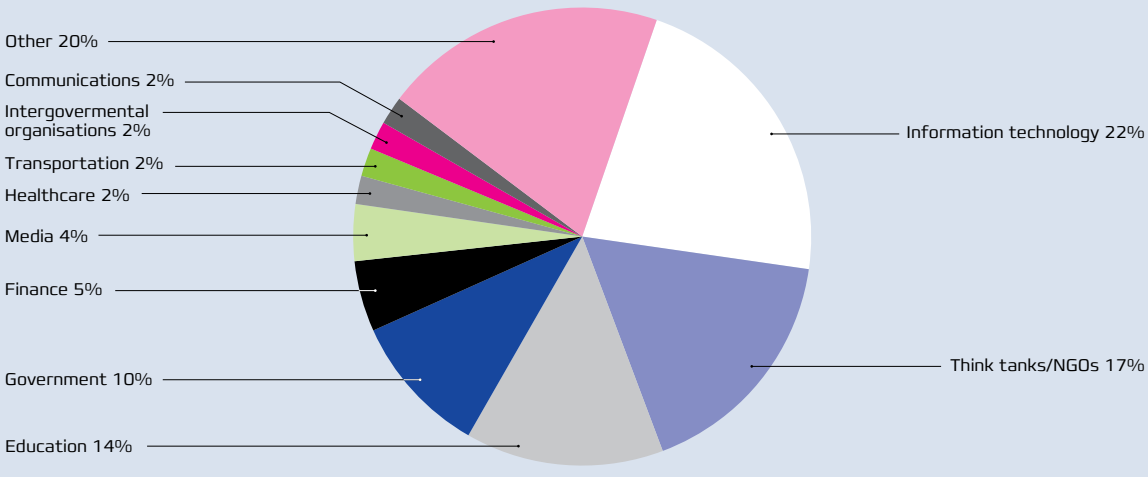
Microsofts Digital Defense Report fra 2022 anslår, at angreb på uddannelsessektoren repræsenterer 14 pct. af nationalstaters målrettede angreb i opgørelsen over angreb fordelt på sektorer. Hertil kommer angreb på tænketanke og NGO'er, der også har en vis tilknytning til sektoren.[9] Disse repræsenterer 17 pct.

I ENISAs Threat Landscape 2022 – hvis analyse baserer sig på tal fra bl.a. kommercielle virksomheders analyser og open source intelligence – fremgår det, at uddannelse var den tredjemest angrebne sektor efter bank-, finans og forsikring samt telekommunikation og tech. Det tilføjes, at uddannelsessektoren mest bliver angrebet i september og januar, hvor der er semesterstart.[11]

Også Verizons 'Data breach investigations report – DBIR' peger på, at 'educational services' er udsat. Heri hedder det, at uddannelsessektoren følger samme trend som andre brancher bl.a. med en dramatisk stigning på 30 pct. af ransomwareangreb.[12]

7 https://research.checkpoint.com/2023/2023-security-report-cyberattacks-reach-an-all-time-high-in-response-to-geo-political-conflict-and-the-rise-of-disruption-and-destruction-malware/
8 https://go.crowdstrike.com/rs/281-OBQ-266/images/2022OverWatchThreatHuntingReport.pdf (side 9)
9 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us (side 35)
10 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=enus&country=us
11 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (side 75)
12 https://www.verizon.com/business/resources/reports/dbir/

**Figur 1 Enisas opgørelse over sektorer, der er angrebet af statsaktører** [10]



# 2. Trusselsvurdering 2023

Men, hedder det i Verizons rapport: Selv om en sektor ikke synes at være lige så udsat som andre, så er tallene påvirket af adskillige faktorer, fx lovgivning der kræver offentliggørelse af hændelser og deres partneres synlighed. Derfor rådes læserne af DBIR-rapporten til ikke at konkludere, hvor udsat de er, alene på baggrund af tallene.

Andre aktører opstiller også lister over antallet og andelen af angreb på institutioner inden for forsknings- og uddannelsessektoren. Fx har den tyske sikkerhedskonsulent Bert Kondruss opgjort antallet af cyberangreb på universiteter og 'colleges' verden over til at være 66 i 2022 mod 32 i 2021. Alene frem til den 1. april 2023 har der ifølge samme været historier om 35 cyberangreb på universiteter i verden. Tallene er baseret på en optælling af omtaler af angrebene i internetbårne medier, som de fremgår af Bert Kondruss' hjemmeside.[13]

Bert Kondruss vurderer selv, at universiteter generelt er åbne om cyberangreb, delvist på grund af at et stort antal studerende vil være påvirket. Derfor antages antallet af ikke-kendte tilfælde at være lavt, 'i det mindste for store cyberangreb.' De mest spektakulære cyberangreb, som fx medfører utilgængelige services, aflyste eksaminer osv, som følge af ransomwareangreb eller hacktivisme, får altid mest omtale.

Spørgsmålet er, om andre typer af cyberangreb får samme opmærksomhed, og om medierne er lige så gode til at rapportere om cyberangreb med kompromittering af fortrolighed til følge, som kan være en konsekvens af cyberspionage. Spørgsmålet er også, om fx cyberspionage i samme grad som cyberkriminalitet overhovedet bliver opdaget i nuet eller om det først sker flere år efter – om overhovedet. Der er næppe tvivl om, at cyberspionage og cyberkriminalitet er præget af mørketal – også inden for uddannelses- og forskningsområdet.

I Danmark har der efter DKCERTs vidende været et angreb på DTU i august 2022, mens der i januar 2023 blev konstateret angreb mod professionshøjskolen Absalon og Aalborg Universitet.[14] Motivet bag disse angreb har formentlig været cyberkriminalitet. I uge 5 2023 var der været DDoS-angreb på tre universiteter i Danmark. Og i uge 8 gennemførte gruppen Anonymous Sudan forsøg på DDoS-angreb på seks universiteter med henvisning til afbrændingen af koranen i Sverige, dvs. cyberaktivisme.[15]

[13] https://konbriefing.com/en-topics/cyber-attacks-universities.html

[14] https://www.version2.dk/artikel/hackere-gemte-sig-hos-aau-i-et-aar-det-er-bekymrende-det-maa-jo-ikke-ske
https://www.version2.dk/artikel/10000-ramt-af-angreb-paa-aau-hacker-havde-adgang-til-helbredsoplysninger

[15] https://cert.dk/da/news/2023-02-23/Advarer-om-DDOS-angreb-mod-danske-universiteter

# Hændelser i den danske uddannelses- og forskningssektor 2022-23

**Malware på webserver i Aalborg**
AAU konstaterede i januar 2023, at der var malware på webserver, som indeholdt persondata. Analyser viste, at indtrængen skete i januar 2022, mens hændelsen blev opdaget og udbedret i starten af januar 2023. Alle registrerede, som kunne være omfattet, blev informeret om hændelsen, Datatilsynet blev underrettet, ligesom sagen blev omtalt i pressen.

Angrebsvektor: Software på webserveren var sårbar overfor CVE-2021-3129.

**Advarsel fra Hamborg bragt videre**
Den 17. januar 2023 lukkede professionshøjskolen Absalon sine it-systemer ned efter at have konstateret, at skolen var ramt af et cyberangreb. Dagen inden – den 16. januar – havde DKCERT viderebragt informationer til Absalon fra det tyske forskningsnet, DFN-CERT, der efterforskede en hændelse på HAW, Hochschule für Angewandte Wissenschafte i Hamburg. I forbindelse med efterforskningen var DFN-CERT blevet opmærksom på, at et angreb på Absalon var forestående.

Selv var HAW blevet angrebet den 27. december. Et velvalgt tidspunkt pga. juleferie, hvilket gjorde, at angrebet blev opdaget sent.

DKCERT deltog i udredningen af hændelsen på Absalon. Trusselsaktøren bag angrebet var Vice Society, der er kendt for målrettet at gå efter uddannelsesinstitutioner. Motivet var at levere ransomware i institutionens servermiljø.

Ifølge DKCERTs oplysninger var angrebsvektoren udnyttelse af to sårbarheder i Exchange. Allerede i efteråret 2022 var sårbarhederne blevet kendt for offentligheden, og DKCERT omtalte sagen på cert.dk i flere omgange. Den 21. december udsendte DKCERT et generelt varsel om Proxynotshell-sårbarhederne på Exchange on-prem løsninger. Den 5. januar blev sagen omtalt på cert.dk med oplysninger om, at der internationalt fortsat var mange upatchede Exchangeløsninger.

Forløbet viser, hvor vigtigt det er at have et netværk inden for miljøet og lige så vigtigt: at udveksle viden om cyberangreb og -metoder.

**25.000 på DTU måtte skifte kodeord**
I august 2022 opdagedes mistænkelig trafik på en server i den centrale infrastruktur på DTU. Angriberne var trængt igennem et system til DTUs studerende, og derfra kunne de i flere trin arbejde sig ind i DTUs centrale systemer. Angrebsmetoden var sandsynligvis phishing, hvor angriberne kan have udnyttet den situation, at mange af DTUs studerende er udenlandske og i august tilmed nyoptagede ifm. studiestart.

Motiv og angribernes identitet er fortsat uafklaret.

Hændelsen medførte, at DTU lukkede ned for systemerne både for ansatte og studerende, og at 25.000 brugere af DTUs systemer måtte skifte kodeord. I forlængelsen af hændelsen har DTU bl.a. i højere grad opdelt sine netværk i segmenter, hvilket forhindrer utilsigtet trafik på tværs. De senere års hændelser har gjort, at der investeres betydelige beløb i at højne cyber- og informationssikkerheden.

**Cyberaktivisme mod danske universiteter**
Den 23. februar 2023 blev DKCERT gjort bekendt med en besked på Anonymous Sudans Telegramkanal om, at et DDoS-angreb mod danske universiteter var forestående. Ifølge kanalen var anledningen den meget omtalte afbrænding af koranen i Sverige, som også blev brugt som årsag til samme gruppes angreb på svenske universiteter og lufthavne i januar og danske lufthavne tidligere i februar.

Angrebets intensitet blev mindre end frygtet med forsøg på angreb på seks universiteter i morgentimerne den 23. februar. Det svenske sikkerhedsfirma TrueSec oplyste i løbet af dagen, at 61 servere fra Anonymous Sudan blev taget ned fra IBMs cloud layer i Tyskland. De pågældende servere havde C2-funktionalitet. Nedtagningen af serverne var sandsynligvis årsagen til en lavere angrebsintensitet end ventet.[16]

Dagen efter det bebudede angreb gengav gruppen på sin kanal, at angrebet den 23. kun var en test, og at nye mere kraftfulde angreb var under forberedelse. DKCERT er dog ikke bekendt med yderligere forsøg på overbelastningsangreb mod den danske uddannelses- og forskningssektor siden den 23. februar.

Der er formodninger om, at angriberne har tilknytning til Rusland, og at årsagen til de aktivistiske angreb skyldes den danske støtte til Ukraine. Koranafbrændingen har sandsynligvis kun været skalkeskjul og anvendt til mobilisering af grupperinger og enkeltpersoner uden tilknytning til krigen til at rette overbelastningsangreb mod en dansk sektor.

[16] C2 står for command-and-control og indebærer, at en trusselsaktør overtager kontrollen med en server og kan udstede kommandoer til serveren om fx at iværksætte et overbelastningsangreb.

# 2. Trusselsvurdering 2023

## 2.3. SITUATIONSBILLEDET GENERELT

Forsvarets Efterretningstjeneste (FE) skriver i sin seneste publikation fra december 2022 'Udsyn - En efterretningsbaseret vurdering af de ydre vilkår for Danmarks sikkerhed og varetagelsen af danske interesser', at Ruslands krig mod Ukraine har ændret den sikkerhedspolitiske situation, så den minder om trækkene fra den kolde krig.[17]

FE vurderer, at Danmark står over for et nyt trusselsbillede, hvor 'tidligere tydelige tærskler mellem fred, krise og krig er blevet erstattet af slørede og overlappende overgange.'

Danmark kan blive udsat for russiske forsøg på at skabe splid i Vesten – og Kina vil forsøge at styrke sin indflydelse internationalt udfordre Vesten økonomisk og videnskabsmæssigt gennem målrettede indsatser for at tilegne sig vestlig teknologi og viden.[18]

FE skriver, at de alvorligste cybertrusler mod Danmark kommer fra russisk og kinesisk cyberspionage og fra cyberkriminalitet udført af organiserede kriminelle netværk i udlandet.[19]

Cyberkriminalitet er kendetegnet ved, at de kriminelle grupperinger er motiveret af berigelse. I princippet er typen af data mindre interessant for cyberkriminelle. Har data en værdi for en dataejer, har det det også for en cyberkriminel, da det fx kan anvendes i en afpresningssituation. Cyberkriminelle er, som det fremgår af FEs publikation, som udgangspunkt opportunistiske, apolitiske og økonomisk motiverede.

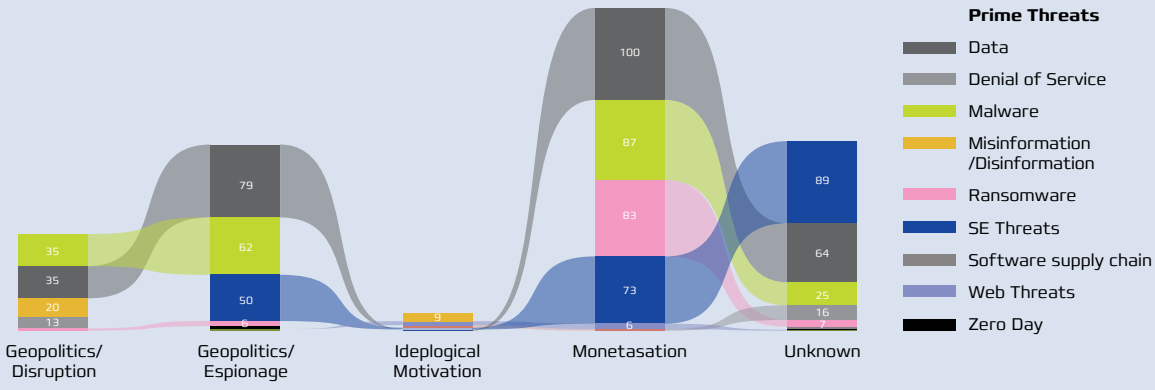
Mens aktører inden for cyberspionage er politisk *og* økonomisk motiveret. Cyberspionage udføres typisk af stater og er rettet mod vidensindhentning.[20]

En spionageoperation tager længere tid og baserer sig på, at angriberne ikke skal blive opdaget. Derfor antages det, at cyberspionageoperationer kræver flere kompetencer og er mere komplekse at udføre. Det kan ikke udelukkes, at cyberspioner har flere kompetencer end cyberkriminelle, men de kan have været rekrutteret af fx statslige efterretningstjenester i kraft af viden, som er opbygget gennem erfaring med cyberkriminalitet i tidligere karrierer.

17 https://www.fe-ddis.dk/globalassets/fe/dokumenter/2022/udsyn-2022/-fe-udsyn-2022_sider-.pdf
18 Ibid, side 40
19 do
20 https://www.cfcs.dk/da/nyheder/2022/cybertruslen-mod-danmark-2022/

**Figur 2 Trusselsaktørers motivation fordelt på trusselskategorier**

Trusselaktørers motivation er primært drevet af økonomiske grunde. Herefter kommer spionage/geopolitiske/disruptive årsager (hvis der ses bort fra kategorien 'ukendt'). Figuren her kan bruges til at vurdere de trusler, som aktører iværksætter for at opfylde deres formål. Ransomwareangreb har fx. næsten udlukkende økonomiske formål, mens det fylder mindre ved spionage. Her udgør Denial of Service, malware og social engineering (SE Threats) størstedelen af truslerne.



# 2. Trusselsvurdering 2023

## 2.4. TRUSLEN MOD DANSK FORSKNING

Allerede i foråret 2021 hævede DKCERT i sin vurdering af truslen fra cyberspionage mod sektoren niveauet fra HØJ til MEGET HØJ i forbindelse med udgivelsen af trendrapporten for 2021.[21] I Center for cybersikkerheds (CFCS) vurdering af truslen fra cyberspionage mod dansk forskning og universiteter fra september 2021 fremgik det, at '..det er meget sandsynligt, at danske universiteter og forskningsinstitutioner vil blive udsat for forsøg på cyberspionage inden for de næste to år.'[22] Dermed hævede CFCS også sin vurdering af niveauet af truslen fra cyberspionage fra HØJ til MEGET HØJ for danske universiteter og forskning.

Det fremgår af CFCSs generelle trusselsvurdering fra 2022, at der her er særligt fokus på forsvars- og udenrigspolitiske mål og at '..myndigheder og virksomheder med en tilknytning til disse myndighedsområder bliver løbende udsat for forsøg på cyberspionage.' Mens truslen fra cyberspionage i andre dele af samfundet i højere grad varierer '..over tid og følger generelt skiftende fokus i fremmede staters efterretningsarbejde.'[23]

Det fremgår videre, at truslen fra cyberspionage især kommer fra Rusland og Kina, men at Nordkorea, Iran, Vietnam, Pakistan og Indien også har kapaciteten. Og at danske universiteter og forskningsinstitutioner, der har viden, samarbejdspartnere eller forskning, som er interessant for et eller flere af disse lande, er også udsat for truslen fra cyberspionage.

Nogle fremmede stater spionerer sandsynligvis også for at fremskynde national forskning og udvikling af samfundsmæssige ydelser, såsom bedre kritisk infrastruktur.

I publikationen 'Dansk Sikkerhed og forsvar frem mod 2035' (september 2022) fremgår det yderligere, at de kinesiske efterretningstjenester for eksempel i de seneste mange år har '..haft særligt fokus på at stjæle vestlige forretningshemmeligheder og patenter til gavn for den kinesiske industri.[24]

Uddannelses- og Forskningsministeriets 'Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde' udsendte i maj 2022 en rapport over sit arbejde.[25] Også heri fremgår det – med henvisning til PETs 'Vurdering af spionagetruslen mod Danmark', at fremmede staters efterretningsvirksomhed i Danmark er blevet mere markant, og at der er tale om spionage, påvirkning, chikane, forsøg på ulovligt at anskaffe produkter, teknologi og viden. 'Vurderingen er særlig relevant for de danske forskningsinstitutioner, da Danmark på en række områder er førende i verden inden for teknologi, innovation og forskning.'

Med andre ord: Spionage – med det formål at få adgang til viden og teknologier, der kan udnyttes kommercielt, til at opnå mere indflydelse og i sikkerhedspolitisk øjemed – er ubetinget blevet en større trussel mod danske universitets- og forskningsinstitutioner end tidligere. Og situationen med en mere usikker sikkerhedspolitisk situation har ikke ændret dette til det bedre, snarere tværtimod, på de fire måneder der er gået fra udgivelsen af 'Udsyn' i december 2022 til færdiggørelsen af denne trendrapport i april 2023.

Men i modsætning til fx hacktivister, der er meget synlige om angreb for at få en platform for deres politiske budskaber, og cyberkriminelle, der fx. i forbindelse med et ransomwareangreb også bliver synlige, er cyberspionage kendetegnet ved, at aktørerne har et behov for at operere i det skjulte. Bliver forsøg på cyberspionage opdaget, vil den forurettede organisation gøre alt for at lukke hullet og forsøge at hindre, at det sker igen.

I sagens natur er der derfor ikke mange erkendte eksempler på cyberspionage inden for uddannelses- og forskningssektoren, men det er DKCERTs vurdering, at det sker. Også i Danmark.

21 https://cert.dk/sites/default/files/uploads/PDF/DKCERT_Trendrapport_2021_END.pdf
22 https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-forskning-og-universiteter.pdf
23 https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/arkiv/cybertruslen-mod-danmark-2022.pdf (side 7)
24 https://www.forsvaret.dk/globalassets/fmn/dokumenter/nyheder/2022/-dansk-sikkerhed-og-forsvar-mod-2035-den-sikkerhedspolitiske-analyserapport-.pdf (side ?)
25 https://www.fe-ddis.dk/globalassets/fe/dokumenter/2022/udsyn-2022/-fe-udsyn-2022_sider-.pdf

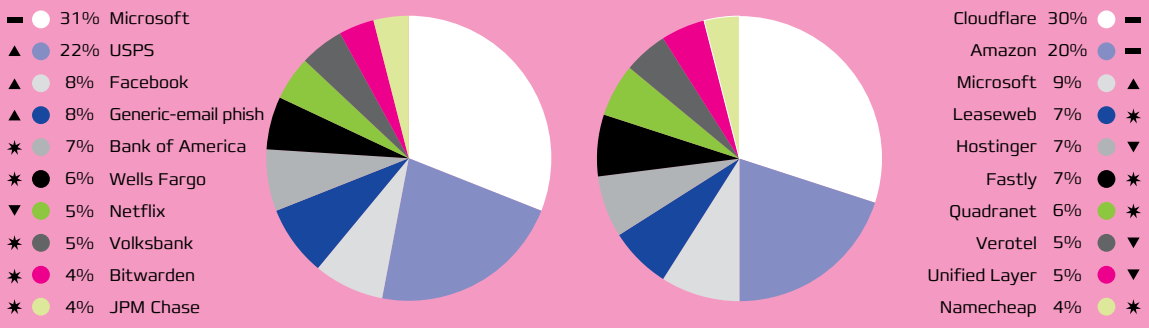
# Vejen ind, metoder og angrebsvektorer

Angribere anvender typisk samme metoder til at få adgang til data. Phishing indtager atter en fremtrædende plads i trusselsaktørernes værktøjskasse, hvad enten formålet er cyberspionage eller cyberkriminalitet. Det virker - både for den førstegangskriminelle amatør og de mere professionelle gengangere.

## Top 10 phished brands

## Top 10 phishing hosts

Af figuren, som er gengivet i sikkerhedsfirmaet CSIS' Threat Matrix rapport [https://csis.com/the-hub/threat-matrix-report/] for andet halvår af 2022, ses det, at Microsoft atter indtager førstepladsen over de kendte varemærker, der anvendes i forbindelse med phishingangreb. Selve angrebsforsøgene udgår i halvdelene af tilfældene fra cloudtjenesterne Cloudfare og Amazon.

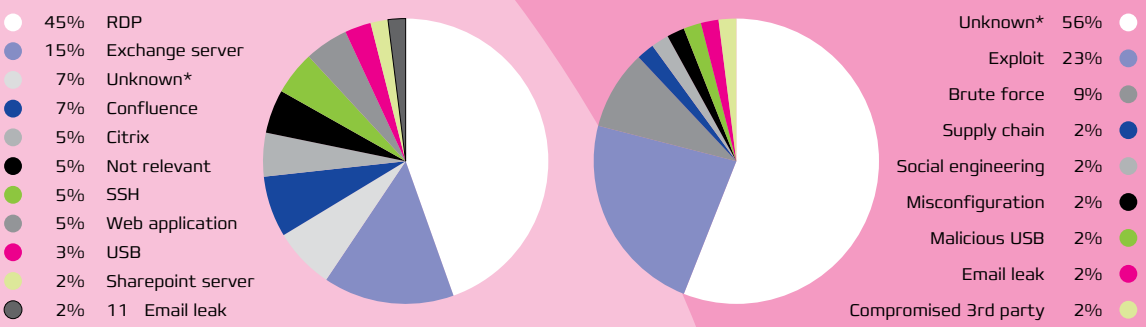



Changes in the last 6 months ✶ New ▬ Unchanged ▲ Moved up ▼ Moved down

## Kompromitterede services

## Angrebsvektorer

Ifølge CSIS' statistik over incident response-sager er de mest eftertragtede services, der misbruges af trusselsaktører, remote desktop protocol efterfulgt af Exchange Server. Af de angrebsvektorer, der har været mulige at identificere, er de mest fremtrædende udnyttelse af sårbarheder og brute force. Årsagen til den store andel af ukendte angrebsvektorer er bl.a., at CSIS i sin incident response-service hos sine kunder ikke har haft adgang til relevante logfiler, at der er anvendt tekniker for at skjule sporene, eller at angrebsvektorerne ikke har indgået i undersøgelsesscopet.



# 2. Trusselsvurdering 2023

## 2.5. VURDERINGER AF CYBERTRUSLEN

### > Cyberspionage

Høj kvalitet i forskningsdata giver fremmede stater og kriminelle, der arbejder for fremmede stater, mulighed for et betydeligt strategisk og kommercielt udbytte, hvis det lykkes af få adgang til forskningsdata og intellektuel ejendom fra vores sektor. Uddannelses- og forskningsmiljøets åbne karakter giver en 'nem' adgang til viden for cyberspionageaktører, der typisk kan have flere ressourcer bag sig og kan i højere grad investere tid og værktøjer til at iværksætte angreb, hvor de på forhånd har udset sig mål, de ønsker at gå efter.

**Dette gør, at forudsætningerne for cyberspionage mod den danske uddannelses- og forskningssektor i meget høj grad er til stede, hvorfor truslen vurderes til at være MEGET HØJ.**[26]

### > Cyberkriminalitet

Begrebet cyberkriminalitet bruges af CFCS som en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret økonomisk. Uddannelses- og forskningssektorens anvendelse af data og digitale tjenester giver cyberkriminelle muligheder for at kapitalisere på sektorens behov for fortrolighed, integritet og tilgængelighed af data. Der er en hård konkurrence mellem trusselsaktører, som udvikler nye metoder og produkter, der gør det mere effektivt at iværksætte angreb og sværere for sektoren at beskytte sig og håndtere angreb. Samtidig er sektoren præget af åbenhed og forskningsfrihed.

**Dette gør, at forudsætningerne for cyberkriminalitet i meget høj grad er til stede, hvilket underbygges af daglige angrebsforsøg mod sektoren og resten af samfundet. Derfor vurderes truslen fra cyberkriminalitet mod uddannelses- og forskningssektoren til at være er MEGET HØJ.**

### > Cyberaktivisme

Enkeltsager – typisk politisk motiveret – præger ikke forskningsmiljøet, men cyberaktivismens karakter gør, at der kan opstå opmærksomhed mod sektoren og enkeltforskere uden eller med kort varsel. Offentlige ytringer fra fx forskere eller personer med tilknytninger til en sag vil kunne fremprovokere aktioner fra cyberaktivister, der ønsker at få opmærksomhed. Anonymous Sudans bebudede og forsøgte DDoS-angreb mod sektoren i februar 2023 med henvisning til afbrænding af koranen viser, at også sager uden for sektoren kan bruges som anledning til et angreb. Formålet med den form for cyberaktivisme er at skabe frygt og mistillid til samfundets evne til at beskytte sig og sine borgere.

Truslen fra cyberaktivisme har i en længere periode været LAV, men krigen mellem Rusland og Ukraine og konfliktfyldte situation mellem Rusland og Vesten som følge af krigen har skabt ændringer i trusselsbilledet, som hæver niveauet. Samtidig oplever cyberaktivister, at deres aktioner medfører den omtale, de eftersøger.

**Det øger forudsætningerne for cyberaktivisme, hvorfor trusselsniveauet for cyberaktivisme mod uddannelses- og forskningssektoren vurderes at være HØJ. Det er ikke usandsynligt, at niveauet af truslen i løbet af det kommende år hæves til MEGET HØJ.**

### > Destruktive cyberangreb

Destruktive cyberangreb kommer typisk fra statslige aktører, der ser et formål ved at ødelægge fx kritisk eller samfundsvigtig infrastruktur. CFCS definerer destruktive cyberangreb, hvor den forventede effekt er

- > død eller personskade,
- > betydelig skade på fysiske objekter,
- > ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Sektoren må i højere grad anses for at være et mål for kriminelle grupperinger, der vil iværksætte

[26] Se Forsvarets Efterretningstjenestes beskrivelse af trusselsniveauer nedenfor.

# 2. Trusselsvurdering 2023

aktioner med profit for øje, mens cyberaktivister ønsker at skabe opmærksomhed ved fx DDoS-angreb, som det er set i januar og februar 2023. Cyberspioner har i modsætning hertil en interesse i at holde sektoren 'kørende' og vil iværksætte spionagetiltag, der ikke opdages. Det vil med andre ord sige, at en destruktiv aktion mod fx en forskningsinstitution kan ødelægge en forretningsmulighed for en cyberkriminel aktør, et strategisk mål for cyberspionage og et politisk mål for en cyberaktivist.

Ydermere kan et fjendtligtsindet lands involvering i et decideret destruktiv cyberangreb mod Danmark og danske interesser blive betragtet som et angreb på et NATO-land, som vil kunne udløse en artikel 5-reaktion.[27] Det kan i sig selv afholde aktører mod destruktive angreb.[28]

FE skriver i sin rapport 'Udsyn', at det er 'sandsynligt, at Rusland på kort sigt vil afholde sig fra at rette destruktive cyberangreb direkte mod NATO-lande.[29]

**Det gør, at forudsætningerne for destruktive cyberangreb mod sektoren kun i lav grad er til stede, hvorfor truslen fra destruktive cyberangreb mod uddannelses- og forskningssektoren vurderes til at være LAV.**

### > Cyberterror

CFCS definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, fx cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur. CFCS vurderer, at det er usandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberterror inden for de næste to år. På den måde har cyberterror lighed med fysisk terror, men CFCS har ikke set udførte cyberterrorangreb, der har svaret til konventionel terror.[30]

**Det gør, at forudsætningerne for cyberterror rettet mod den danske uddannelses- og forskningsinstitutioner ikke er til stede, hvorfor det er DKCERTs vurdering, at truslen fra cyberterror mod uddannelses- og forskningssektoren er INGEN.**

Disse vurderinger og konklusioner bygger på indsamlede oplysninger fra både eksterne kilder og egne kilder, herunder oplysninger fra institutioner og samarbejdspartnere. DKCERTs vurdering baserer sig på en samlet analyse af disse oplysninger. For sammenlignelighedens skyld er anvendt samme skala og definitioner som CFCS benytter. CFCS kommer i publikationen 'Cybertruslen mod dansk forskning og universiteter' frem til tilsvarende vurderinger.[31]

27 https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en
28 https://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/2022/-dansk-sikkerhed-og-forsvar-mod-2035-den-sikkerhedspolitiske-analyserapport-.pdf (side 39)
29 https://www.fe-ddis.dk/globalassets/fe/dokumenter/2022/udsyn-2022/-fe-udsyn-2022_sider-.pdf (side 14)
30 https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2022b.pdf
31 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/forskning-og-universiteter/

**TRUSSELSNIVEAUER IFØLGE FORSVARETS EFTERRETNINGSTJENESTE:**

**Ingen:** Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.

**Lav:** Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.

**Middel:** Der er generelle trusler. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.

**Høj:** Der er erkendte trusler. Der er kapacitet, hensigt og planlægning. Angreb/ skadevoldende aktivitet er sandsynlig.

**Meget høj:** Der er konkrete trusler. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

# Truslen fra den menneskelige faktor

Den største trussel mod beskyttelse af informationers fortrolighed, integritet og tilgængelighed anses for at være menneskelige fejl. Det kan kan have sin baggrund i manglende kompetencer, uagtsomhed eller bevidste handlinger udført af hhv. ubevidste, uagtsomme eller uvederhæftige medarbejdere.

DKCERT opererer med disse tre betegnelser for medarbejdere inden for trusselskategorien **den menneskelige faktor**:

**Den ubevidste medarbejder** (som også kan være en studerende, en gæsteforelæser mv. på en uddannelsesinstitution) er en person, som på grund af fx uklare, manglende sikkerhedspolitikker eller manglende uddannelse ubevidst bryder organisationens sikkerhedspolitikker.

**Den uagtsomme medarbejder** (eller studerende mv.) er en person, der bevidst bryder reglerne, selv om han eller hun har kendskabet til dem. Årsagen kan være, at sikkerhedsreglerne opleves at umuliggøre udførelsen af arbejdet. Det kan også være skødesløshed som følge af, at reglerne gør arbejdet mindre effektivt. Den uagtsomme bryder ikke nødvendigvis regler af ond mening.

Handlinger fra de uagtsomme og ubevidste kan være skadelige – ikke mindst fordi de sjældent vil være opmærksomme på at anmelde sikkerhedsbrud i organisationen. De ubevidste og de uagtsomme er ubetinget årsag til de fleste sikkerhedsbrud.

**Den uvederhæftige medarbejder** (eller studerende mv.) har til hensigt at udføre handlinger, der kan medføre skade på en organisation. Mens ondsindede, udefrakommende angribere i mange tilfælde vil blive stoppet af organisationens sikkerhedsmekanismer som firewalls, e-mailscanning og antivirus-filtre, vil den uvederhæftige ofte have succes med sine handlinger. Det kan skyldes, at sikkerhedsmekanismerne ikke altid beskytter mod en person, der vil være i stand til at udføre sine handlinger i kraft af misbrug af sin stilling, kendskab til fortrolig information og legitime it-adgange. Denne person er svær at opdage, men hans eller hendes skadevirkende adfærd kan til en vis grad begrænses med funktionsadskillelse, bruger/rettighedsstyring og logs.

Der er eksempler på, at cyberkriminelle grupper systematisk har arbejdet med rekruttering af virksomheders medarbejdere mod betaling eller ved afpresning.

Menneskelige fejl kan aldrig undgås, men sikkerhedspolitikker, retningslinjer, løbende uddannelse og vedligeholdelse af en sikkerhedskultur er metoder til nedbringelse af menneskelige fejl.

Undersøgelser peger på, at uddannelses- og forskningssektoren kan være særligt udsat for menneskelige fejl i forbindelse med studie- og semesterstart. Det peger på, at indsatser skal iværksættes allerede før studiestart.

# 3. Året i tal og ord

**DKCERT har som mission at skabe øget fokus på informationssikkerhed i uddannelses- og forskningssektoren ved at opbygge og skabe aktuel, relevant og brugbar viden. Det sker gennem en række aktiviteter, som gør DKCERT i stand til at offentliggøre og udsende varsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.**

## 3.1 SCANNINGER, VARSLER, HÆNDELSER OG TEKNISKE ANALYSER

### 3.1.1 Sårbarhedsscanninger

DKCERT tilbyder sårbarhedsscanninger til institutioner tilknyttet forskningsnettet.

Scanningerne gennemføres på baggrund af konkrete bestillinger fra institutionerne. Enkelte institutioner får gennemført scanninger en-to gange årligt, mens andre får hyppigere scanninger, typisk hver måned. Af de 12 institutioner på forskningsnettet, der regelmæssigt benytter sig af tjenesten, får fem institutioner udført scanninger hver eller hver anden måned. Syv institutioner får gennemført scanninger en gang i kvartalet eller hvert halve år. Der er ca. 40 institutioner på forskningsnettet.[32]

**DKCERT mener:**
**I forhold til det nuværende trusselsbillede er det DKCERTs anbefaling, at institutioner på forskningsnettet i højere grad og ud fra faste aftaler bør få udført scanninger mindst en gang om måneden. DKCERTs sårbarhedsscanninger er gratis for medlemmer af forskningsnettet.**

Scanningerne undersøger, om institutionernes it-systemer har kendte sårbarheder, som er publiceret i National Vulnerability Database. (se Figur 3)

På baggrund af scanningerne udarbejdes en rapport om de fundne sårbarheder i institutionerne med forslag til hvilke tiltag, som bør iværksættes for at højne sikkerheden for den enkelte institution. Rapporterne indeholder en prioritering af de fundne sårbarheder og anbefalinger til institutionens håndtering af disse ud fra sårbarhedernes alvorlighedsgrad.

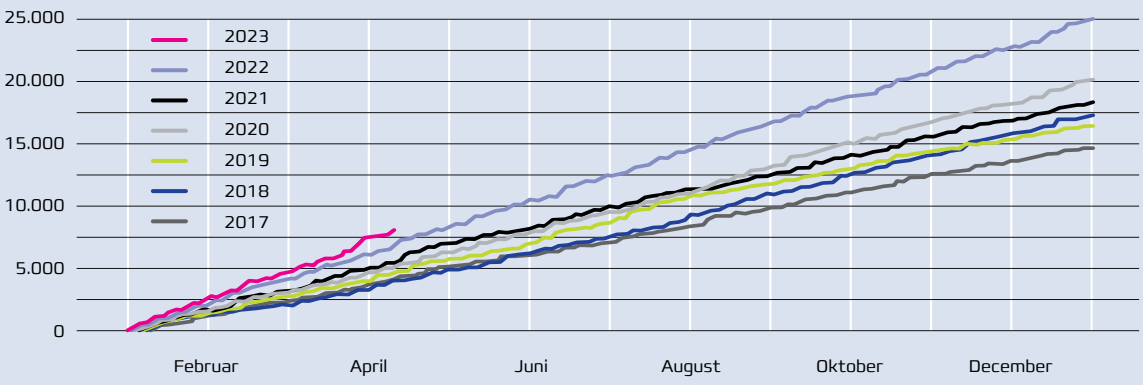
Anbefalingerne til prioriteringen baseres på sårbarhedernes score i forhold til CVSS – Common Vulnerability Scoring System. CVSS er den internationalt anerkendte metode til scoring af sårbarheder kritikalitet på en skala fra 1-10.

I 2022 har DKCERT gennemført 200 scanninger af institutioner, hvoraf var 183 var faste tilbagevendende scanninger, mens 10 har været interne og syv ad hoc-scanninger. I 2021 var det samlede antal på hhv. 174, i 2020 103 og i 2019 52.

[32] https://www.deic.dk/da/forskningsnet/basisnet/tilslutning/tilsluttede-institutioner

**Figur 3: Udviklingen i publicerede sårbarheder i NVD fra 2017 - 2023**

DKCERTs scanninger efter sårbarheder baserer sig på de CVE-numre, der bliver publiceret på Mitres CVE-liste, som endvidere behandles til videreformidling på National Vulnerability Database (https://nvd.nist.gov/). Den nedenstående graf viser udviklingen i antallet af CVE-numre, der har været publiceret sine 2017. Det fremgår af grafen, at der har været en støt stigning henover årene, hvor 2022 var det år med flest publicerede sårbarheder på over 26000. Grafen findes på first.org's hjemmeside https://www.first.org/epss/data_stats og opdateres løbende. Her findes også andre relevante grafer og data om CVE-numre.



# 3. Året i tal og ord

De syv ad hoc-scanninger er gennemført på baggrund af en konkret mistanke om en sårbarhed. Processen foregår ved, at der bestilles en scanning på en given server udelukkende med den pågældende sårbarhed i sigte.

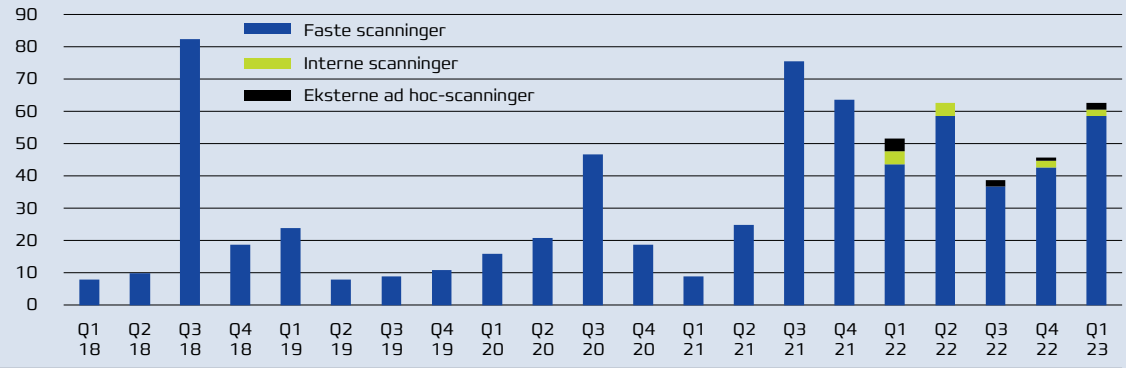
De 10 interne scanninger er ligeledes blevet til på baggrund af konkrete bestillinger fra institutionerne og gennemføres inden for institutionens firewall, hvor lokale netværk scannes, mens eksterne scanninger udføres uden for firewall'en. Den interne scanning giver mulighed for en mere fintmasket undersøgelse af institutionernes systemer, da det her er muligt at påvise sårbarheder, hvis man er på domænet som autoriseret bruger. Herved kan der evt. findes systemer med sårbarheder, der kan udnyttes af såvel udefrakommende (uautoriserede brugere) og som interne, autoriserede brugere.

Intern scanning udføres for medgået tid og kan bestilles af institutionerne på linje med eksterne scanninger, dvs. ved kontakt til cert@cert.dk.

**DKCERT mener:**
**Stigningen i antallet af scanninger fra 164 til 200 bekræfter tendensen fra de sidste år med flere scanninger. Det er glædeligt og et udtryk for fortsat øget opmærksomhed fra institutionerne på risikoen for, at sårbarheder udnyttes til konkrete angreb. Vi anbefaler dog også, at flere interne scanninger foretages.**

**Figur 4: Scanninger på forskningsnettet 2018 - Q1 2023**

I 2022 udførte DKCERT 200 scanninger for institutioner, hvoraf 10 var interne scanninger. Syv scanninger var ad-hoc-scanninger.



# 3. Året i tal og ord

Det samlede antal scannede host-enheder/IP-adresser i 2022 var 332.974 mod 115.069 i 2021, mens der var godt 300.000 i 2020.

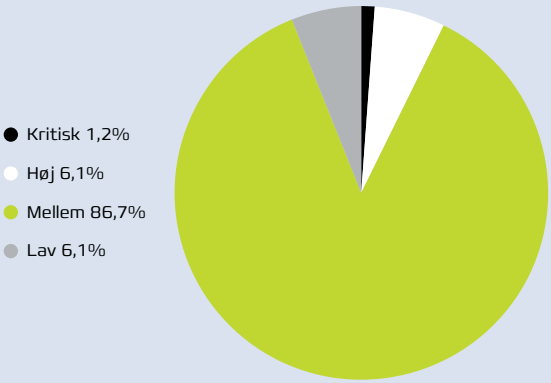
Af det samlede antal scannede host-enheder/IP-adresser er 156.685 i 'live'. Det betyder, at der aktivitet på dem. Samlet har 651 host-enheder i 2022 en kritisk eller høj sårbarhed, hvilket svarer til 0,42 pct. I 2021 var andelen fire pct. I alt er der fundet 22.075 sårbarheder, hvor langt de fleste er 'mellem' i kritikalitet. I 2021 blev der fundet 22.549 sårbarheder.

Det relativt høje tal kan skyldes, at sårbarhederne kan tælle med flere gange, hvis institutionerne er længe om at opdatere. Det kan i princippet kan gøre tallene mindre valide, men ikke ændre ved situationen, at der er fundet sårbarheder.

**DKCERT mener:**
**Faldet i andelen af enheder med en kritisk eller høj sårbarhed kan ses som et udtryk for, at institutionerne er blevet bedre til at håndtere sårbarhederne. Men der er stadig mange mellemfejl, hvis høje antal kan være et udtryk for, at de ikke prioriteres af institutionerne.**

**Figur 5: Fordelingen af de fundne sårbarheder ift. kritalitet**

Figuren viser sårbarhedernes fordeling på kritikalitet ud af de i alt 22.075 fundne sårbarheder i de 190 ikke-interne scanninger i 2022, som DKCERT har gennemført. Godt 1,2 pct. af sårbarhederne er kritiske, mens 6,1 pct. har vurderingen høj. 86,7 pct. er middel og 6,1 pct. er lav. I alt er der fundet 22.075 sårbarheder. Sårbarhedernes opdeling er baseret på OWASP TOP 10 Web Application Security Risks 2021.[33]




[33] https://owasp.org/www-project-top-ten/

# 3. Året i tal og ord

### 3.1.2 Varsler fra DKCERT

I maj 2021 begyndte DKCERT at sende varsler til vores modtagere på det danske forskningsnet om sårbarheder og opdateringer i systemer. Varslerne kommer bl.a. fra oplysninger, som DKCERT selv modtager fra egne kilder, holder øje med i miljøet eller som kommer fra CFCS. Varslerne skrives altid i det samme, velkendte format, så modtagerne hurtigt kan navigere i dem og vurdere om varslerne er relevante, og om de kræver handling. Varslerne indeholder en teknisk beskrivelse, oplysninger om de berørte systemer, CVSS-scoren, Indicators of Compromise (IoC'er), anbefalinger samt referencer.

### 3.1.3 Varsler fra tredjeparter

I 2022 modtog og udsendte DKCERT varsler om 38 forskellige typer sårbarheder, som er identificeret hos institutioner tilknyttet forskningsnettet. Denne service blev introduceret i slutningen af 2014 og hjælper det danske forskningsnet med at afdække, hvilke mulige angrebspunkter, som ondsindede aktører nemt kan finde. Advarslerne kommer fra samarbejdspartnere, først og fremmest Shadowserver-projektet, der dagligt scanner internettet for en række kendte og hyppigt udnyttede sårbarheder.[34] DKCERT bidrager til Shadowserver-projektet med en dansk honeypot.

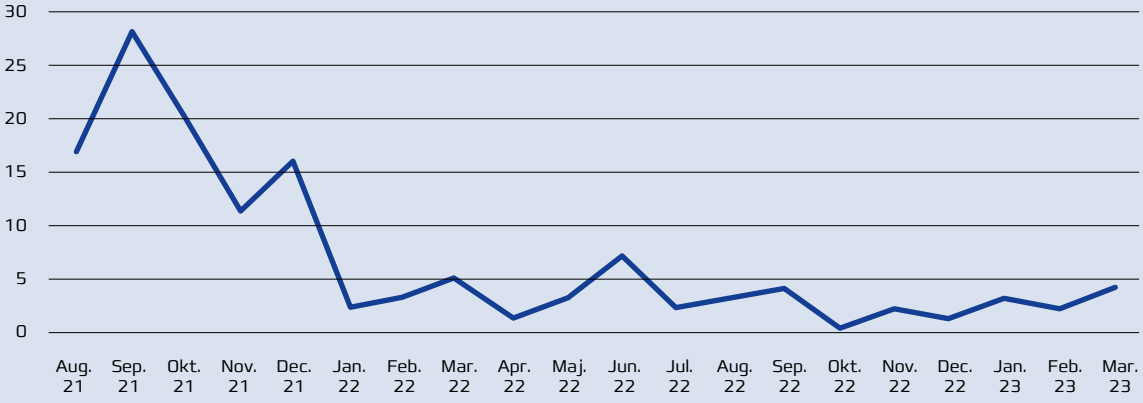
Det er altid op til den enkelte institution at håndtere sårbarhederne ud fra egen prioritering, som er bestemt af institutionernes risikovurdering og risikotolerance. Her spiller konsekvensen ved tab af det sårbare system, adgang på netværket, samt alvoren af sårbarheden ind, hvorfor sårbarheder på visse systemer er længere tid om at blive håndteret end andre. Afgørende for håndtering af sårbarheden er dog, om institutionerne overhovedet er klar over, at de har systemer med sårbarheder. Der kan sårbarhedsscanninger og varsler være en god hjælp.

I 2022 er der i gennemsnit blevet udsendt ca. 175 unikke varsler pr. måned vedr. sårbarheder på forskningsnettet. Det anslås, at omkring 60-70 pct. af disse er dubletter, dvs. går igen i de scanningerne fra gang til gang.

[34] https://www.shadowserver.org

**Figur 6 Varsler udsendt af DKCERT**

Varsler fra DKCERT fra august 2021. Årsagen til faldet fra starten til det nuværende leje skyldes, at DKCERTs interne kvalitetssikring udelukkede visse sårbarheder og kilder.



# 3. Året i tal og ord

Siden 2016 har udsendelse af varsler fra tredjeparter været automatiseret. Grafen i Figur 7 viser, at antallet af varsler, sendt til institutioner til det danske forskningsnet, generelt er faldende fra i gennemsnit 650 på måned i 2016 til 176 pr. måned i 2020. Faldet frem til 2020 skyldes efter DKCERTs opfattelse, at institutionerne er blevet bedre til at patche, men der kan være en tendens til, at antallet af varsler er i svag stigning.

**Figur 7 Varsler fra tredjeparter (2016-Q1 2023)**

Varsler fra tredjeparter fra januar 2016 til første kvartal 2023. Data fra juni 2022 er taget ud, fordi en justering af indsamlingsmetoden viste langt flere varsler, end der var grundlag for at viderebringe. Systemet blev i 2021/22 ændret til kun at tælle de sager, som de enkelte institutioner ønsker at modtage information om. DKCERT justerer løbende udsendelsen af varsler i forhold til institutionernes ønsker og varslernes karakter.

# 3. Året i tal og ord

### 3.1.4 Sikkerhedshændelser i 2022

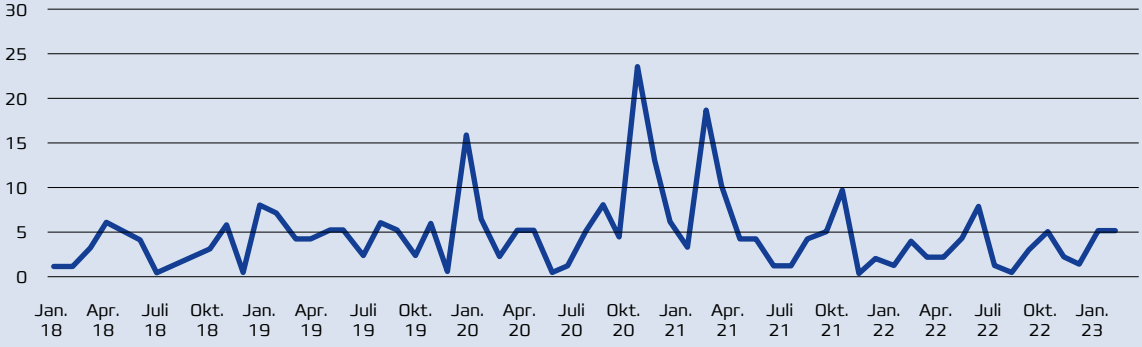
DKCERT behandler sikkerhedshændelser på forskningsnettet. Henvendelserne kommer fra eksterne kilder som sikkerhedsfirmaer, myndigheder eller andre CERT/CSIRT-organisationer rundt i verden, der har observeret uønsket adfærd fra IP-adresser på forskningsnettet. Institutionerne på forskningsnettet henvender sig ligeledes med relevante og konkrete sikkerhedshændelser.

DKCERT er kontaktpunkt ved henvendelser vedrørende alle forskningsnettets IP-adresser. Det er vores opgave at filtrere ikke-relevante henvendelser fra, involvere de berørte aktører, udføre en indledende analyse/efterforskning af problemstillingen og derefter være til rådighed som vejlednings- og kommunikationsportal for de berørte.

DKCERT modtog i 2022 oplysninger om 629 hændelser, som er samlet i 34 undersøgelser, der typisk omhandler inficerede systemer på forskningsnettet. DKCERT undersøger bl.a., om en mistanke om malware på et system kan bekræftes, sørger for notifikation til de berørte parter, rådgivning og hjælp til kommunikation til eksterne ressourcer. I 2021 blev der gennemført 67 undersøgelser.

**Figur 8 Undersøgelser 2018-Q1 2023**

DKCERTs undersøgelser fra 2018 til første kvartal 2023. DKCERT får typisk flere rapporter, der omhandler den samme sagstype og det samme ip-nummer. De samles derfor i én undersøgelse – frem for 10 om det samme til den samme modtager. Antallet af rapporter og undersøgelser svinger derfor meget fra måned til måned. Nye sagstyper er altid genstand for nye undersøgelser og vil derfor slå ud i grafen.



# 3. Året i tal og ord

### 3.1.5 Uddannelses- og forskningssektorens MISP – deler indsigt om events

Uddannelses- og forskningssektorens MISP åbnede som pilotprojekt for de første brugere i juli 2020. I 2021 gik MISP'en officielt i drift med 13 institutioner – heraf de fleste universiteter - tilknyttet MISP'en. Der er i alt 65 brugere med rettigheder til at indtaste data.

MISP er en platform, hvor man systematisk deler viden om sikkerhedshændelser og angreb. I dag bruger mere end 6000 organisationer verden over MISP.[35]

En MISP kan sikre, at der sker hurtigere deling, kommunikation og alarmering på tværs af aktører og sektorer. I kraft af MISP'ens metode til registrering af IoC'er kan brugerne tilpasse MISP'en, så de kun modtager den information, der er relevant for deres organisation. Delingen foregår enten manuelt eller automatisk ved integration til virksomhedens filtre eller logsystemer.

[35] MISPs formelle navn er Open Source Threat Intelligence and Sharing Platform
https://www.misp-project.org/

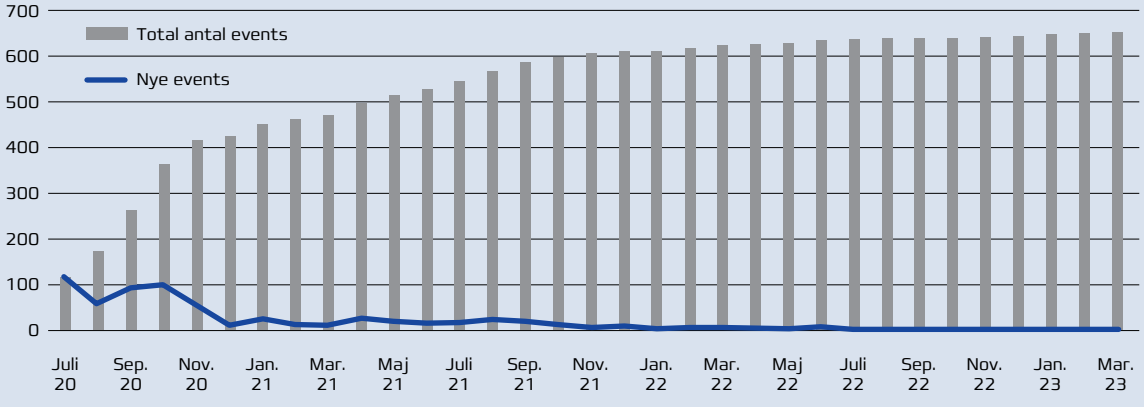
**DKCERT mener:**
**32 nye events i MISP i 2022 kan efter DKCERTs opfattelse ikke afspejle det reelle tal og er et udtryk for en mindre aktiv brug af MISP end oprindeligt tiltænkt. DKCERT vil i 2023 understøtte en højere grad af indrapportering af events i MISP, så videndelingsplatformens potentiale kan udnyttes.**

At være tilknyttet MISP'en betyder, at institutioner selv kan tilføje IoC'er og hændelser samt få information om, hvad andre institutioner indrapporterer. Samtidig kan brugerne søge tilbage i databasen efter hændelsestype, frekvens og andre relevante oplysninger, der kan medvirke til analyse af et aktuelt trusselslandskab. Uddannelses- og forskningssektorens MISP er i første omgang sat op til at dele og distribuere trusselsinformation mellem universiteter og andre institutioner på forskningsnettet.

Parallelt med den nuværende anvendelse planlægger DKCERT og de andre forskningsnet-CERT'er at etablere en infrastruktur for at kunne dele IoC'er regionalt i Norden. Fra januar 2023 deltager to medarbejdere fra DKCERT i et delprojekt under GEANTs GN5-1 WP8. Projektet (subtask CTI) skal understøtte deling af cybertrusselsinformation mellem forskningsnet i Europa. DKCERT har sat den MISP op, der indgår i dette samarbejde.

**Figur 9 Events i MISP fra juli 2020 til marts 2023**

Antal hændelser i universiteternes MISP siden pilotdriften i juli 2020. Samlet har der været registreret 32 nye events i 2022, svarende til 2,67 pr. måned. Det er en nedgang fra 187 nye events i 2021.



# 3. Året i tal og ord

### 3.1.6 Dataanalyse

Data om netværkstrafik på forskningsnettet kan give ny viden om angrebsmønstre og proaktivt opdage angreb, der ellers ikke ville blive registreret, før det er for sent. Ud fra den tanke kan DKCERT analysere trafikdata fra routerne på nettet. Dataanalyse kan også anvendes reaktivt fx til efterforskning af sikkerhedshændelser for institutionerne og i forbindelse med politisager. DKCERT har gennemført dataanalyse i forbindelse med hændelsen på DTU i august 2022 og hændelsen på Absalon i januar 2023.

### 3.1.7 SIE Europe

SIE Europe er et europæiskbaseret fællesskab af internetbrugere, der ønsker at gøre brugen af internettet mere sikker.[36] SIE Europe står for indsamlingen og tilbyder en platform til indsamling, aggregering og deling af passive DNS-data inden for Europa. SIE Europe indsamler kun DNS-data, der er relevante i kampen mod cyberkriminalitet og danner samarbejdsrelationer med deltagende organisationer, som bidrager med DNS-data.

Organisationer, som er tilknyttet SIE Europe-fællesskabet, deler passive DNS-data for at få adgang til ændringer, der finder sted på internettet, som kan indikere ondsindet aktivitet. Jo flere organisationer, der deltager, jo større er muligheden for at afbøde potentiel skade på systemer, netværk og infrastruktur, forhindre tab af data og modvirke svindelaktiviteter og anden cyberkriminalitet.

I Danmark deltager DKCERT pt. med passiv DNS-data sammen med KU, AU, SDU, AAU, CFCS og CSIS Security Group, men flere kan deltage. Kontakt gerne cert@cert.dk for yderligere information.

### 3.1.8 Honeypot – nyt værktøj til analyse af angrebstyper

DKCERT begyndte i december 2022 afprøvningen af et nyt værktøj. Værktøjet er en honeypot, der inden for sikkerhedsmiljøet fungerer på samme måde som naturens honningkrukke. Den udgiver sig for at være en legitim tjeneste og kan derfor bruges til en analyse af tiltrækningskraften på angribere, hvordan og hvilke enheder, der forsøges kompromitteret.

Ved at lytte til forskellige porte kan værktøjet detektere forskellige angrebstyper og derfor give et godt billede af den aktuelle trusselssituation og udviklingen i den, hvis man har tilstrækkeligt antal honeypotter og historiske data at sammenligne med.

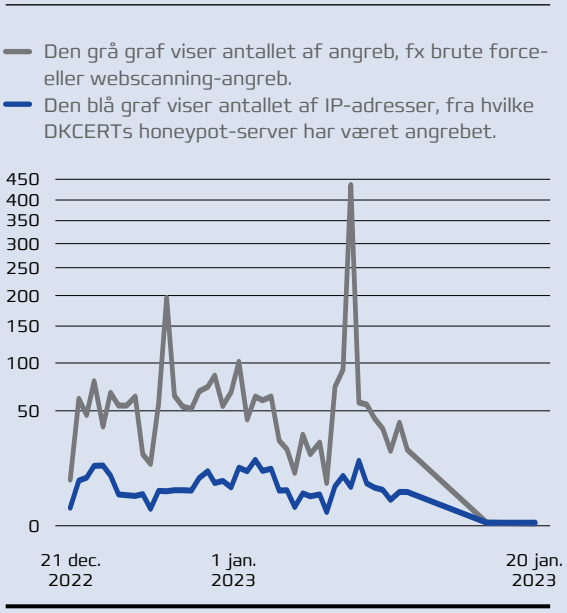
DKCERTs honeypot har i første omgang været installeret som et proof-of-concept for at undersøge, om der kan indsamles relevante data for uddannelses- og forskningssektoren. De foreløbige resultater ses i Figur 10.

DKCERT forventer at kunne levere en plug-and-play løsning ift. til opsætning af en honeypot og hjælper med rådgivning. En standardopsætning kræver ca. en halv dags arbejde afhængig af kompleksiteten i opsætningen.

Data fra honeypotten vil kunne trækkes automatisk ind i MISP, hvorved resultaterne bliver tilgængelige for flere. Herfra vil DKCERT også kunne udstille analyse af log, anbefalinger til imødegåelse og øget beskyttelse.

Drift, vedligeholdelse og formidling af data er gratis for medlemmer af forskningsnettet.

**Figur 10: Data fra honeypotten**




[36] https://www.sie-europe.net/

# Passkey – giganternes kamp for et sikrere login

Kodeord til login i brugerkonti har altid været et af de største hovedbrud for sikkerhedsfolk. 'Genbrug aldrig kodeord' er mantraet, men når de mange kodeord skal være lange og komplekse, falder brugerne for fristelsen om at genbruge kodeord, der kan huskes. Et godt hjælpeværktøj til opbevaring af de forskellige kodeord er en passwordmanager og to-faktorlogin. Men sikkerheden ved to-faktorlogin er ikke altid lige god. [37]

**En stærk alliance**

I maj 2022 annoncerede Google, Apple og Microsoft, at de er gået sammen om at udvikle en sikker løsning til kodeordsfrit login. Løsningen baserer sig på FIDO2/WebAuthn, som er udviklet af FIDO-alliancen netop med udgangspunkt i login uden adgangskoder.[38] Giganternes løsning har fået navnet Passkey.

Passkey ligger i et 'økosystem' og er tilgængeligt via hardwareenheder, som fx kan være en telefon, en computer, iPad, et ur eller en FIDO-nøgle. Med enheden kan brugere logge ind på apps og websteder med en pinkode eller en biometrisk sensor. Rent praktisk kan enheden erstatte både adgangskode og den anden faktor i et og samme trin – og den markedsføres som værende lige så enkel at anvende som en automatisk udfyldt adgangskodeformular.

**Siloer forbindes**

At Google, Apple og Microsoft er gået sammen betyder ikke, at de anvender samme teknologiske løsning. De har hver deres silo i økosystemet, men har aftalt en metode, der kan gå på tværs af siloerne.

Metoden baseres på QR-koder. Hvis en bruger fx har sin passkey tilgængelig via en Apple-enhed, men skal logge ind på en tjeneste via en Windows-pc, kan brugeren via QR-koden åbne et loginbillede på sin telefon. Her fra kan pinkoden eller biometrien aktiveres.

Google beskriver løsningen som en digital legitimation, der er knyttet til en brugerkonto og et websted eller en applikation.

**Brug kræver registrering**

Rent teknisk sker der det, at brugerens enhed genererer en signaturbaseret på passkey. Denne signatur bruges til at bekræfte loginlegitimationsoplysningerne mellem passkey og webstedet.

Forbindelsen mellem applikationen og brugeren kræver dog først en registrering. Med registreringen oprettes brugerens profil og passkey'en som loginmetode, på samme måde som man hidtil har skulle oprette sig med brugernavn og kodeord. Ønsker en bruger at logge ind på en tjeneste med krav om passkey, hjælper browseren eller operativsystemet med valg og brug af den rigtige passkey.

**Fordelene ved passkey er flere**

- Passkey er baseret på en standard. Det betyder, at implementeringen sker ud fra samme metode, hvilket er nemt for brugerne at anvende og sikkerhedsfolk at vedligeholde.
- Løsningen er phishingresistent i modsætning til SMS eller app-baserede engangsadgangskoder. Den specifikke passkey er uløseligt forbundet med den app eller tjeneste, den er oprettet til. Derfor vil en falsk tjeneste fra et websted med en beslægtet URL ikke kunne få forbindelse med den enkelte passkey.
- Webserverne opbevarer kun de offentlige nøgler, aldrig de private. Det kan sænke antallet af cyberangreb på webserverne.
- Løsningen understøtter privacy. Andre tjenester kan ikke se, hvor den specifikke pass-key er anvendt.
- Brugerne er ikke begrænset til at bruge deres passkey på den enhed, der er brugt til den initiale registering.
- De tre største techvirksomheder i verden gået sammen om løsningen og enige om det samme navn. Det styrker udbredelsen.

Endelig udmærker løsningen sig ved at være sikker og brugervenlig. Eneste ulempe er, at brugerne skal vænnes til at anvende en ny metode til login.[39]

[37] Se fx https://www.cert.dk/da/information/trendrapporter (trendrapport for 2022)

[38] DKCERT har sat en løsning op, så til universiteternes sikkerhedsmedarbejdere skal anvende FIDO-nøgle til indlogning på MISP og Mattermost.

[39] https://fidoalliance.org/passkeys/
https://media.fidoalliance.org/wp-content/uploads/2022/03/How-FIDO-Addresses-a-Full-Range-of-Use-Cases-March24.pdf
https://developers.google.com/identity/passkeys,
https://developer.apple.com/passkeys/,
https://webauthn.io/

# 3. Året i tal og ord

## 3.2 VIDENDELING

### 3.2.1 Videndeling ved hændelser

Ved større hændelser på forskningsnettet og universiteterne deltager DKCERT i arbejdet med at koordinere videndelingen om hændelsen mellem medlemmer af forskningsnettet og facilitere kontakt til myndigheder og andre sektorer.

Med videndeling om hændelser kan andre institutioner forberede sig og evt. forebygge, at de rammes af samme type hændelser. Blandt cyberkriminelle er kendskab til succesfulde metoder til brud i bestemte sektorer eftertragtet viden og vil lynhurtigt brede sig, så andre vil forsøge at anvende samme metoder.

En institution, som fx er udsat for en hændelse, kan derfor kontakte DKCERT og orientere om forløbet og de iværksatte foranstaltninger. Denne viden bringer DKCERT videre til medlemmerne af forskningsnettet, så institutionerne fx kan tage egne forholdsregler eller gøre beredskabet klar.

Den initiale videndeling foregår primært via vores fælles MISP og sekundært på CISO-niveau. Derudover udsendes varsler til alle institutioner tilknyttet forskningsnettet.

I 2022 har DKCERT deltaget i håndteringen og formidlingen af information om DTU-hændelsen i august 2022.[40]

### 3.2.2 Mattermost – det der betyder mest

I 2021 stillede DKCERT et nyt chatværktøj - Mattermost - til rådighed for sikkerhedsteknikere ved universiteterne. Mattermost er en sikker kanal til udveksling af informationer, og det bruges i vidt omfang af sikkerhedsteknikerne til hurtig deling relevant af viden og udveksling af erfaringer. Der er pt. 45 medlemmer af chatkanalen, som kræver tilknytning til en forsknings- og uddannelsesinstitution. Kanalen bruges oftest i forbindelse med hændelser i sektoren og er en 'on-prem' løsning, der driftsafvikles hos DKCERT. Anvendelse af kanalen kræver tofaktorlogin ved hjælp af FIDO-nøgler.

Tilmelding til Mattermost sker ved henvendelse til cert@cert.dk.

### 3.2.3 Faglig videndeling i netværk

DKCERT driver et netværk for sikkerhedsteknikere. SikRef er DKCERTs videndelingsforum for alle, der arbejder med sikkerhed ved forskningsnettets institutioner. Formålet med forummet er at skabe et mødested for teknikerne, hvor de i et fortroligt rum kan udveksle erfaringer med hinanden, give råd, orientere hinanden om nye tiltag, brug af sikkerhedsteknologi, hændelser, trusler osv.

Der deltager hver gang 25-30 sikkerhedsmedarbejdere i møderne. Styrken ved netværket er ikke kun, at medarbejdere på tværs af institutioner mødes. Netværkets medlemmer repræsenterer også forskellige fagområder, der lærer af hinandens kompetencer.

I 2022 er der gennemført to fysiske møder på hhv. Syddansk Universitet i Odense og på Københavns Universitet og to onlinemøder. De fysiske møder omhandlede den tekniske og organisatoriske implementering af passwordmanager på et universitet, den fortsatte tilpasning af MISP (læs mere om MISP i afsnit 3.3.4), hvor man systematisk deler viden om IoC'er (trusler og hændelser, fx igangværende, uautoriserede scanninger).

Som led i den daglige anvendelse af MISP'en er der etableret en MISP-arbejdsgruppe, der mødes ca. hver anden måned.

For at styrke det faglige fællesskab på DPO-området driver DKCERT endvidere et netværk for universiteter og professionshøjskolers GDPR-professionelle. Det sker i regi af DPO-tjenesten. (Læs mere om DPO-tjenesten i afsnit 3.3.1)

Endelig er chefen for DKCERT observatør i CISO-forum, som er en underarbejdsgruppe under Danske Universiteters CIO-Gruppe. Forummet, hvis formand udpeges af og blandt CIO-Gruppen, har til formål at koordinere og udveksle viden og erfaringer om aktuelle udfordringer for sikkerheden på forskningsnettet og universiteterne mellem universiteternes informationssikkerhedschefer og -koordinatorer.

CISO-forum har holdt møder i gennemsnit ca. en gang om måneden i 2022 bl.a. som følge af krigen i Ukraine og i forbindelse med udarbejdelse af sektorens cyber- og informationssikkerhedsstrategi.

[40] Læs mere om DTU-hændelsen på side 11.

# 3. Året i tal og ord

### 3.2.4 DKCERTs deltagelse i Cybersikkerhedsrådet

Chefen for DKCERT Henrik Larsen blev i slutningen af 2021 genudpeget som medlem af Cybersikkerhedsrådet for den fornyede mandatperiode 2022-2023. Rådet er nedsat for at rådgive regeringen om, hvordan den digitale sikkerhed styrkes og sikre videndeling mellem myndigheder, erhvervsliv og forskningsverdenen. I forbindelse med regeringsdannelsen i efteråret 2022 blev årets sidste møde i november aflyst, men møderne er genoptaget i marts 2023. Rådet har i 2022 bl.a. drøftet cybertruslen mod Danmark, videreudvikling af Sikkerdigital.dk, opdatering af de tekniske minimumskrav til statslige myndigheder, cyberstrategiens initiativ om etablering af en cyberhotline og kompetenceudfordringer på cyberområdet.

### 3.2.5 Videndeling blandt ligesindede i Rådet for digital sikkerhed

DKCERT er medlem af Rådet for Digital Sikkerhed med Henrik Larsen som bestyrelsesmedlem, og medarbejderne ved DKCERT deltager i visse af Rådets arbejdsgrupper i det omfang, der er faglig sammenhæng med opgaveløsningen. Endvidere bidrager DKCERT, når rådet sender høringssvar mv. til relevante ministerier eller offentliggør holdningspapirer.

DKCERT har i 2022 deltaget i en arbejdsgruppe vedrørende international overvågning. Deltagelse i arbejdsgrupperne er med til at nuancere problemstillingerne og øge DKCERTs medarbejderes netværk og viden.

Rådet er en uafhængig medlemsorganisation, der 'arbejder for at fremme et trygt og frit digitalt samfund for alle'. Foreningen deltager i debatter og høringer om udspil fra regeringen og EU ud fra den målsætning om at understøtte et samfund med god balance mellem effektiv brug af moderne teknologi, beskyttelse mod digitale trusler og den enkeltes ret til privatliv.[41]

### 3.2.6 International videndeling

CERT'erne for de fem nordiske forskningsnet holder møder sammen med NORDUnet-CERT ca. en gang om måneden.[42] På møderne diskuterer deltagerne aktuelle sikkerhedshændelser og erfaringer med værktøjer og metoder. Møderne foregår som onlinemøder, hvorved netværk etableret på fx konferencer og workshops holdes ved lige. I 2022 afløste norske Uninett CERT (nu eduCSC-NO) DKCERT i rollen som netværkets mødeleder. I 2023 varetages rollen af finske Funet CERT.

DKCERT har siden 2002 været akkrediteret medlem og fra marts 2023 kandidat til certificeret medlemskab af Trusted Introducer og dermed af TF-CSIRT.[43] TF-CSIRT er en organisation for CERT/CSIRT'er, der er hjemmehørende og mødes i Europa, men som nu optager teams fra alle geografiske regioner. Netværket, der pt. har omkring 500 medlemsteams, faciliteredes 2000-2022 af de europæiske forskningsnets paraplyorganisation GÉANT. Fra 2022 af the Open CSIRT Foundation.

Siden 1993 har DKCERT været medlem af FIRST.org (Forum of Incident Response and Security Teams), som er en organisation for 687 CERT/CSIRT/PSIRT-teams i 104 lande, heraf otte medlemmer i Danmark (pr. 1. april 2023).[44] DKCERT-medarbejdere deltager i et årligt regionalt seminar for Europa samt i årskonferencen og generalforsamlingen.

41 https://www.digitalsikkerhed.dk
42 CERT® var fra 1997 til 2021 et registreret varemærke og stod oprindeligt for Computer Emergency Response Team. Den mere generiske betegnelse CSIRT (Computer Security Incident Response Team) er i dag mere almindelig anvendt. DKCERTs officielle navn er Danish Computer Security Incident Response Team.
43 https://www.trusted-introducer.org/
https://tf-csirt.org/
44 https://www.first.org/members/map

# 3. Året i tal og ord

### 3.2.7 Internationale arbejdsgrupper

DKCERT deltager i forskellige internationale arbejdsgrupper, de såkaldte Special Interest Groups (SIG), som grundlæggende set har til formål at gøre internettet mere sikkert. SIG'erne er organiseret både i GÉANT og FIRST.

- Målet med **GÉANTs Cyber Threat Intelligence subtask (GN5-1 WP8, CTI)** er etablering af European R&E Security Intelligence Hub, en virtuel organisation, der har til formål at indsamle, analysere, klassificere og udveksle sikkerhedsefterretninger i kombination med levering af værktøjer, processer og procedurer. Analyserne resulterer i værdifuld information for både GÉANT og forskningsnettene (NRENs), som gøres tilgængelig via en central MISP, koblet med hver NRENs MISP. GÉANT og forskningsnettene vil med dette få indsigt i trusselslandskabet, som kan hjælpe dem med at forberede sig på en lang række potentielle cyberangreb og kriser.
- **GÉANT GN5-1** er et projekt under GÉANTs awareness for medarbejdere på forskningsnettene, der arbejder med læring og formidling af cyber- og informationssikkerhed. Projektet er under etablering.
- **GÉANTs SIG-ISM (Special Interest Group Information Security Management)** beskæftiger sig med de nationale forsknings- og uddannelsesnetværks interne sikkerhed og har halvårlige møder, heraf et årligt fællesmøde i WISE Community, som er et globalt netværk for sikkerhed i forsknings-it-infrastrukturer (bl.a. udsprunget af CERN). Desuden er gruppen arrangør af sikkerhedsdagen ved GÉANTs årlige TNC-konference, ligesom den er involveret i bl.a. koordinationen af NIS2-forberedelserne for de europæiske forskningsnet.
- **FIRSTs global Academic Security SIG** sigter mod at tilvejebringe en platform specifikt til samarbejde med akademiske sikkerhedsteam, deling af erfaringer mv. Gruppen mødes fysisk en gang årligt i forbindelse med FIRST.org's årskonference og en til to gange via onlinemøder. I 2022 blev møderne gennemført virtuelt i februar og fysisk i forbindelse med årskonferencen i juni. SIG udveksler i øvrigt viden året rundt på en mailingliste.
- **First Automation SIGs** formål er at dele viden om de eksisterende løsninger, som hver CERT/CSIRT/PSIRT har kørende. Gruppen skal understøtte læring og rådgivning mellem medlemmerne af gruppen.

# 3. Året i tal og ord

### 3.2.8 Nyhedsformidling

I 2022 udgav DKCERT 311 artikler om forskellige aspekter af informationssikkerhed på cert.dk mod 346 i 2021 og 307 i 2020.

Artiklerne publiceres dagligt eller næsten dagligt på cert.dk. Artiklerne dækker bredt og skrives ud fra, hvad der relevant for sektoren: Nyheder om tekniske sårbarheder, nyheder om nye og gamle trusler, hændelser på universiteter og forskningsinstitutioner i verden, større databrud og cybersikkerhedspolitik fra ind- og udland. Hver mandag samles den foregående uges nyheder i et nyhedsbrev, der udsendes til abonnenterne.

Cert.dk havde i 2022 15.764 unikke pageviews. Antallet er faldet en del i forhold til de tidligere år, hvor det i 2021 var 56.783 og 81.288 i 2020.

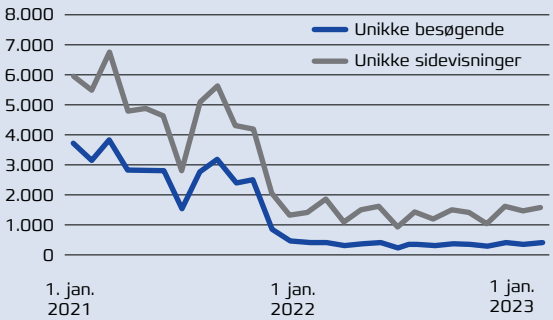
Faldet kan skyldes, at flere medier er begyndt at publicere nyheder om cybersikkerhed, podcast og temaartikler, ligesom også CFCS er blevet mere aktiv i sin kommunikation.

DKCERT har indtil et par år siden været en af de eneste institutioner med egentlig nyhedsdækning, hvilket har imødekommet mange interesserede læseres behov for aktuel viden. Den position er nu ændret, og det kan have medført, at færre besøgende spontant opsøger DKCERTs hjemmeside.

Ved udgangen af 2022 abonnerede i alt 1.609 personer på et af DKCERTs nyhedsbreve. Det tilsvarende tal i slutningen af 2021 var 1.558. DKCERT har ved udgangen af 2022 3369 følgere på Twitter. En stigning fra 3257 i 2020.

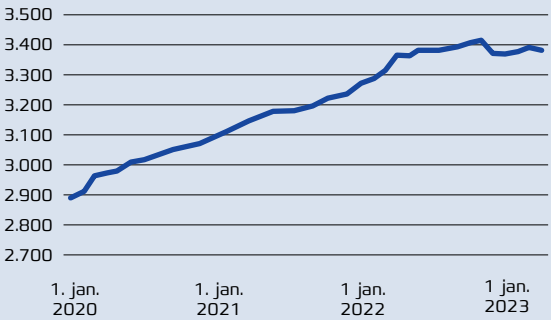
**Figur 11: Unikke pageviews, cert.dk i 2022**

Unikke besøgende og sidevisninger på cert.dk i 2022




**Figur 12: Twitterfølgere fra januar 2020**

DKCERT på Twitter fra januar 2020. Stigningen i marts 2022 skyldes formentlig Ruslands invasion i Ukraine, mens faldet fra november kan finde sin årsag i det generelle fald i antallet af Twitterbrugere efter den megen omtale i forbindelse med Elon Musks overtagelse af Twitter.



# Klummer på cert.dk

Henrik Larsen skriver fra tid til anden en klumme på cert.dk, hvor der sættes spot på en aktuel problemstilling i forhold til cyber- og informationssikkerhed.

**Januar: Ny strategi for cybersikkerhed lanceret**
Regeringen har udgivet sin nye Nationale Cyber- og Informationssikkerhedsstrategi med nye krav til statslige myndigheder. Forskningssektoren udpeges til at være samfundsvigtig.

**Februar: Sådan kan du modstå påvirkningskampagner**
TRUST-modellen – en tilgang til håndtering af påvirkninger.

**Marts: Hvordan skal man forholde sig til et uændret, men MEGET HØJT trusselsniveau?**
Kend dit it- og informationsdomæne og fokuser på grundlæggende cyber- og informationssikkerhed.

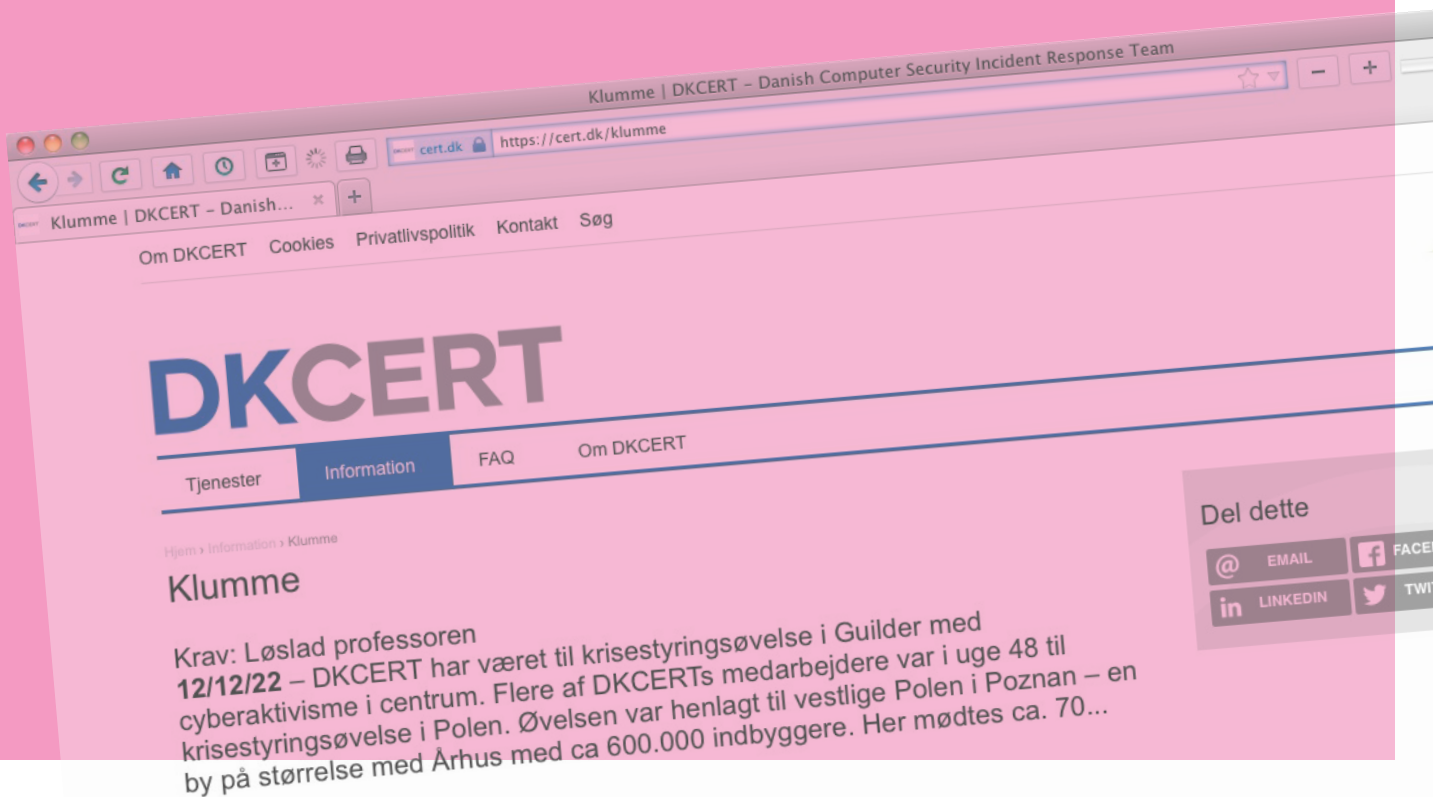
**Maj: Der findes flere forskellige slags MFA'er**
Multifaktorautentifikation (MFA) er udråbt til at være den Hellige Gral i adgangskontrol og er i mange tilfælde løsningen på alle ledere og systemadministratorers hovedpine: Dårlige kodeord. Men hvilken MFA er egentlig den bedste?

**Juni: CFCS hæver trusselsniveauet mod telesektoren**
Truslen fra cyberaktivisme stiger, mens truslen fra cyberspionage falder.

**August: TLP 2.0 lanceret**
Et af de bedste trafiksystemer er blevet bedre.

**December: Krav: Løslad professoren**
DKCERT har været til krisestyringsøvelse i Guilder med cyberaktivisme i centrum

Læs klummerne i deres helhed på https://cert.dk/klumme



# 3. Året i tal og ord

## 3.3 TJENESTER

### 3.3.1 DPO-tjenesten

DKCERTs DPO-tjeneste hjælper institutioner fra uddannelses- og forskningsektoren med forskellige opgaver inden for databeskyttelse, herunder GDPR. Tjenesten indgår som fast ekstern DPO eller DPO-vikar for kunderne samt yder GDPR-konsulentbistand på timebasis. Det kan være i perioder, hvor en uddannelsesinstitution har manglet en DPO, eller det kan være henvendelser om rådgivning ved særlige situationer eller svære spørgsmål om fx dataansvar ved projekter med flere parter.

DPO-tjenesten består af tre medarbejdere, der har fordelt institutionerne vest og øst for Storebælt mellem sig.

DPO-tjenesten har oplevet en højere grad af modenhed hos kunderne end tidligere, hvilket har gjort de fleste mere selvkørende. Enkelte har valgt at hjemtage DPO-opgaven og løse den inden for egne rammer.

Tjenesten har dog samtidigt oplevet en tilgang af nye kunder og opgaver, hvilket har medført at tjenesten i 2022 leverede 33 procent flere timer til institutionerne end i 2021.

**Udvidet rådgivning**

Inden for de seneste år har der været en tendens til, at opgaven udvikler sig til også at omfatte rådgivning inden for anden lovgivning og informationssikkerhed, hvilket har bidraget til det øgede antal leverede timer. Anden lovgivning kan eksempelvis være sundhedsloven, når forskningsprojekter får videregivet data fra eller indeholder sundhedsbehandlinger, hvor der fx skal indhentes informeret samtykke til selve sundhedsbehandlingen, samtidig med at der databeskyttelsesretligt skal informeres om behandling af personoplysninger. Der er tale om information om to forskellige behandlinger, og der kan også opstå uklarhed om samtykket: Hvad gives der samtykke til?

Der rådgives også inden for informationssikkerhedsområdet, hvilket forventes at fortsætte i 2023. Det har affødt et behov for udvidelse af tjenestens kompetenceområder. Videreuddannelse af tjenestens medarbejdere er derfor fortsat et fokuspunkt.

**DPO-netværket**

DPO-netværket afholder to årlige virtuelle møder, dog med mulighed for fysisk fremmøde. DPO-netværket har medvirket til at sikre videndeling og erfaringsudveksling på tværs af uddannelses- og forskningsinstitutionerne. De danske universiteter, professionshøjskoler og kunstneriske skoler har været faste medlemmer siden 2018.

# 3. Året i tal og ord

**Intern rådgivning**
DPO-tjenesten yder også rådgivning til en række af DeiCs tjenester, fx i forbindelse med databehandleraftaler, forberedelse til certificeringer og national godkendelse af identitetsføderationen WAYF som NemLog-in3 broker.

### 3.3.2 Awarenesstjenesten Phish kan teste agtpågivenheden overfor phishingtrusler

DKCERT stiller en phishingawareness-tjeneste til rådighed for universiteter og andre institutioner på forskningsnettet, der kan bruge den til at få udsendt fingerede phishing-mails til ansatte og studerende mhp. at monitorere reaktionsmønstre hos brugerne. DKCERT hjælper med gennemførelsen af phishingkampagnen, der afsluttes med en detaljeret og anonymiseret rapport. DKCERT løser opgaven pr medgået tid, hvilket for institutionerne typisk indebærer en udgift på 10-15.000 kr. pr. kampagne.

DKCERT har ikke haft efterspørgsel på phishingawareness-tjenesten i 2022.

### 3.3.3 Beredskabsøvelser – håndtér en hændelse som i den virkelige universitetsverden

DKCERT har i flere år bidraget til planlægning og gennemførelse af den europæiske beredskabsworkshop CLAW. CLAW-workshoppen gennemføres i regi af GÉANT og tilbydes alle europæiske forskningsnet.

CLAW er en workshop med en interaktiv kriseøvelse, som giver deltagerne mulighed for i et realistisk scenarium at afprøve de forskellige aktiviteter og fagligheder, der skal i spil i forbindelse med håndtering af kriser. Beredskabsøvelserne blev oprindeligt udviklet som analoge to-dagsworkshops, men har i 2020 og 2021 været gennemført som virtuelle en-dagsberedskabsøvelser. I 2022 var det oprindelige format tilbage, og i 2023 tilbydes begge formater. Hver deltager får tildelt en rolle som hhv. CISO, sikkerhedstekniker, netværkstekniker eller presserådgiver. I løbet af øvelsen bliver rollerne stillet en række spørgsmål og dilemmaer, som man under stort tidspres skal håndtere.

I 2021 begyndte DKCERT at tilbyde institutionerne på forskningsnettet beredskabsøvelser efter inspiration i CLAW-konceptet. I februar 2021 blev konceptet afprøvet sammen med Det Kongelige Bibliotek og er siden tilbudt andre institutioner. Workshoppen er tilrettelagt i et virtuelt format, men vil også kunne gennemføres med fysisk tilstedeværelse.

# 4. Forskning i trygge rammer

**I marts 2023 blev den første delstrategi for uddannelses- og forskningsssektoren udgivet. Med dette har sektoren fået et strategisk fokuspunkt for det kommende års arbejde med cyber- og informationssikkerhed.**

**Vi gengiver her indledningen til delstrategien og de 17 initiativer, der skal udmønte den.**
**Strategien kan læses i sin helhed her.**

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. 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.

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.

**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.

**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.

# 4. Forskning i trygge rammer

**Strategiens fire pejlemærker**

> 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.

**Initiativer**

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

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

> Initiativ 1.3: Øget strategisk målbarhed på sikkerheds- og modenhedsniveauet

> Initiativ 2.1: Håndtering af universiteternes specifikke omstændigheder

> Initiativ 2.2: Detektion og påvisning

> Initiativ 3.1: Løbende trussels- og risikoanalyser for universitetssektoren

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

> Initiativ 3.3: Øget indsigt i trusler og konsekvenser hos forskerne

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

> Initiativ 4.1: Etablering af operativ DCIS

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

> Initiativ 4.3: Styrket sikkerhedstilsyn med systemleverandører og databehandlere

> Initiativ 4.4: Intelligent overvågning

> Initiativ 4.5: Tværuniversitære awareness-fremmende tiltag

**Initiativer på rumområdet**

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

> Initiativ 5.2: Skabe øget bevidsthed om cybertruslen

> Initiativ 5.3: Bidrage til udarbejdelsen af et trusselsbillede for rumområdet.

# 5. Eksterne bidrag

# 5. Eksterne bidrag

**Eksterne bidrag om cyber- og informationssikkerhed om det nyeste af relevans for sektoren.**

Mange nye indsatser præger alle sektorer i disse år. Vi har taget de mest relevante frem her i kapitlet med bidrag fra nogle af vores eksterne samarbejdspartnere.

På overstatsligt niveau sætter NIS2-direktivet en retning for sektoren selv om det endnu er uklart, i hvilken grad sektoren er omfattet. En analyse fra Industriens Fond viser, at over 1000 danske private virksomheder virksomheder skal leve op til direktivets tekst inden oktober 2024, mens en lang række offentlige myndigheder også skal gøre det. En af Danmarks fremmeste eksperter i NIS2, Morten Eeg Ejrnæs Nielsen, giver sit bud på, hvad direktivet betyder for uddannelses- og forskningssektoren.

Nye versioner af sikkerhedsstandarderne i ISO27000-serien forsøger at gøre det lettere at følge og implementere standarderne. Det er relevant for universiteterne, idet Uddannelses- og Forskningsministeriet fører tilsyn med universiteterne med udgangspunkt i ISO27001. Dansk Standards Berit Aadal beskriver, hvordan standarderne i forbindelse med en opdatering i 2022 er blevet nemmere at arbejde med for brugerne.

Uddannelses- og forskningssektoren skal have sin egen decentrale cyber- og informationssikkerhedsenhed. Men hvad er det for en størrelse og hvordan fungerer den? Christa Wulff Sarby fra Sundhedssektorens DCIS, DCISSund, fortæller om erfaringer med at have og drive en decentral cyber- og informationssikkerhedsenhed.

# 5. Eksterne bidrag

## 5.1 NIS2 ER LANDET

**NIS2-direktivet trådte i kraft den 17. januar 2023, og skal efterleves fra den 18. oktober 2024, men hvad betyder det for universiteterne?**

AF MORTEN EEG EJRNÆS NIELSEN,
SECURITY ADVISOR, GLOBETEAM A/S

NIS2-direktivet er en del af en bølge af lovgivning, som kommer fra EU, og som EU selv kalder "the digital decade". Det startede med GDPR og det første NIS-direktiv, nu kommer NIS2, Critical Entities Resilience Directive (CER) og Data Act, yderligere kommer Cyber Resilience Act (CRA), Data Governance Act og AI Act inden for de næste år. Alle er lovgivninger, som sigter mod at beskytte forskellige dele af den digitale infrastruktur i medlemslandene.

NIS2-direktivet har til formål at opnå et højt fælles cybersikkerhedsniveau i hele unionen ved at højne beskyttelsen af den digitale infrastruktur, som beskytter tjenester, som er vigtige for samfundet. Det lyder flot, men i bund og grund handler det om, at vores samfund bliver mere og mere digitalt, og derfor også mere og mere afhængige af digitalt tjenester. Derfor kommer NIS2-direktivet med krav til disse tjenester, således at de er mere robuste og tilgængelige.

**Ikke omfattet direkte, men indirekte**
For universiteterne kunne det godt tyde på, at de ikke bliver direkte omfattet af direktivets krav. Det er nemlig overladt til medlemsstaterne selv at fastsætte, om uddannelsesinstitutioner, navnlig hvor de udfører kritiske forskningsaktiviteter, er direkte omfattet af direktivets krav. Alt tyder på, at man ikke ønsker det i en dansk kontekst.

Direktivets krav er dog stadig relevante for universiteterne, og derfor er det vigtigt, at universiteterne forholder sig til dem.

Grunden til dette er, at flere af universiteterne godt kan være omfattet af direktivet, selvom uddannelsesinstitutioner ikke er en omfattet sektor. Der er nemlig flere universiteter, som har tjenester, der alligevel falder ind under direktivets anvendelsesområde.

Det område, hvor flere af landets universiteter alligevel godt kan blive omfattet af direktivets krav er vedr. 'Udbydere af datacentertjenester'.

Datacentertjenester defineres nemlig således i direktivets artikel 6:

'En tjeneste, der omfatter strukturer eller grupper af strukturer, der er beregnet til central opbevaring, sammenkobling og drift af IT- og netværksudstyr, der leverer datalagrings-, -behandlings- og -transporttjenester samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol.'[45]

**HPC-anlæg som en datacentertjeneste**
Dette vil sandsynligvis omfatte alle HPC-anlæg

[45] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1679306015166

# 5. Eksterne bidrag

hos de danske universiteter, hvilket betyder, at disse vil være omfattet for den del af deres drift. Dette vil så betyde, at alle HPC-anlæg vil være underlagt de 10 materielle krav i direktivets artikel 21, men også kravet om højere involvering og ejerskab for sikkerhedsarbejdet blandt universiteternes ledelse. Yderligere vil dette også betyde, at universiteterne underlægges den tilsynsmodel, som skal sikre overholdelse af direktivets krav, samt de sanktioner som også følger af direktivet.

Ud over at være direkte omfattet, som nogle universiteter muligvis er, vil hovedparten af universiteterne nok opleve, at deres samarbejdspartnere kan begynde at stille sikkerhedsmæssige krav, som bunder i direktivets krav til sikkerhed.

Det er nemlig sådan, at direktivet stiller krav til forsyningskædesikkerhed. Så alle de virksomheder, der selv er omfattet af direktivets krav, vil skulle kigge på deres samarbejdspartnere og leverandører og stille krav til disse.

Vi så det faktisk også med GDPR. Her begyndte samarbejdspartnere at stille krav til og spørge ind til universiteternes compliance med databeskyttelsesreglerne, hvilket gjorde, at universiteterne blev underlagt mange forskellige krav fra forskellige aktører, hvis samarbejdet skulle fortsætte. Især inden for forskning var dette tydeligt, hvor flere store fonde ligefrem gjorde dokumenteret compliance til en forudsætning for at kunne udbetale midler til forskning.

**Gensyn med udbredelse a la GDPR**

Hvis det samme kommer til at gøre sig gældende for NIS2-direktivets krav, vil universiteterne blive mødt med en bred vifte af krav fra forskellige samarbejdspartnere. Disse har alle deres egen forståelse og fortolkning af kravene fra direktivet, som de forventer, at samarbejdspartnere kan leve op til. Dét bliver ikke nogen nem opgave for universiteterne at efterkomme.

At direktivets krav har til formål at sikre, at de vigtige tjenester fortsat er tilgængelige for samfundet, hvilket også gør sig gældende for universiteternes egne tjenester, ændrer ikke ved, at sikkerhed og compliance koster penge og ressourcer. NIS2 kommer så yderligere til at kræve mange kompetente medarbejdere med sikkerhedserfaring. Noget, der allerede nu er mangel på i Danmark og også i resten af EU.

Som en pudsig lille eftertanke, så skal regeringen faktisk også i den nationale strategi beskrive, hvordan man vil fremme uddannelse i cybersikkerhed, cybersikkerhedsfærdigheder og -forskning. Det vil sandsynligvis også vil involvere universiteterne i nogen grad, og denne involvering vil igen kunne stille krav til universiteternes egen sikkerhed med udgangspunkt i kravene fra NIS2-direktivet.

Det hele skal være på plads i oktober 2024, og selvom universiteterne ikke bliver omfattet, fordi de er universiteter, så bør de alle allerede nu kigge på direktivets krav, fordi de alle alligevel risikerer at blive indirekte omfattet, og dermed alligevel skulle overholde direktivets krav.

# 5. Eksterne bidrag

## 5.2 ÆNDRINGER I ISO/IEC 27000-STANDARDERNE SKAL GØRE DEM NEMMERE AT ANVENDE

**Cybertruslen får flere og flere til at søge mod sikkerhedsstandarder. Det har gjort behovet for mere tilgængelige standarder større.**

AF BERIT AADAL,
SENIORKONSULENT, DANSK STANDARD

I takt med den stigende cybertrussel vælger flere og flere virksomheder at følge de internationale standarder for informationssikkerhed i ISO/IEC 27000-serien. ISO/IEC 27000-serien indeholder nogle af verdens mest udbredte standarder for informationssikkerhed. Den mest anvendte er ISO/IEC 27001, der er en ledelsesstandard for informationssikkerhed. Standarden indeholder krav til blandt andet risikostyring, dokumentation af processer og fordeling af roller og ansvar for informationssikkerhed.[46]

ISO/IEC 27001 er tæt koblet med standarden ISO/IEC 27002, der er en vejledende standard. ISO/IEC 27002 indeholder foranstaltninger, der kan hjælpe virksomheder med at kvalificere og udpege handlinger, der anses som nødvendige ift. at beskytte informationer. Foranstaltningerne, der er beskrevet i ISO/IEC 27002, fremgår også af anneks A i ISO/IEC 27001.[47]

Det overordnede formål med standarderne er at give virksomheder og organisationer et værktøj til at beskytte forretningskritiske aktiver på en struktureret og systematisk måde. Begge standarder er udkommet i nye versioner i 2022, da der har været behov for at opdatere standarderne i tråd med den teknologiske udvikling. Samtidig har det været et mål at gøre standarderne mere brugervenlige.

### De nye ændringer i standarderne ISO/IEC 27001 og ISO/IEC 27002

De største ændringer ser vi i standarden ISO/IEC 27002. Det ses bl.a. ved antallet af foranstaltninger, der er skåret ned fra 114 til 93. Foranstaltningerne omfatter anbefalinger til både politikker, processer, procedurer, organisationsstrukturer samt software- og hardware-funktioner. Nogle foranstaltninger er lagt sammen inden for den samme livscyklus, andre er kommet til som følge af de teknologiske udviklinger, der er sket gennem de sidste år. Eksempler på nye foranstaltninger er datamaskering og webfiltrering.

Tidligere har standarden været inddelt i 14 kapitler, men her er også sket en gennemgribende ændring. Standarden er nu bygget op over en helt ny struktur baseret på fire temaer, der kategoriserer foranstaltningerne:

- Personrelaterede foranstaltninger vedrører individuelle personer (distancearbejde, ansættelse, uddannelse mv.)
- Fysiske foranstaltninger handler om de fysiske objekter (bygninger, områder, hardware mv.)
- Teknologiske foranstaltninger fokuserer på teknologi (kryptografi, konfigurationsstyring, netværk mv.)
- De organisatoriske foranstaltninger er mere eller mindre 'alt andet' (politikker, ansvar, leverandørforhold mv.).

Princippet bag den nye inddeling er at placere foranstaltningerne dér, hvor de har størst forklaringskraft. Det betyder også, at nogle foranstaltninger kan dække flere temaer på én gang. F.eks. kan foranstaltningen om awareness, uddannelse og træning siges både at være en organisatorisk og en personrelateret foranstaltning. Men den er kategoriseret som en personalerelateret foranstaltning, da det er det, der handler om de individuelle personer, der vejer tungest.

### Attributter og to nye annekser

En anden ændring er brugen af de såkaldte attributter. Brugen af attributter har til formål at give flere perspektiver på de enkelte foranstaltningers egenskaber. Hver foranstaltning har således fem attributter, der kan anvendes til at filtrere, sortere eller præsentere foranstaltningerne i forskellige fremstillinger til forskellige målgrupper og dermed være en hjælp til at kvalificere deres relevans og værdi for forretningen.

46 På Dansk Standards hjemmeside findes en oversigt over de mest anvendte standarder inden for cyber- og informationssikkerhed. https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder

47 Dansk Standard har udarbejdet et whitepaper, der beskriver de største ændringer i den nye version af ISO/IEC 27002. https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder/whitepaper

# 5. Eksterne bidrag

Endelig er der tilføjet to nye annekser til ISO/IEC 27002. Annekserne skal hjælpe virksomhederne med at skabe overblik over standarden og udfolde anvendelsesmulighederne. Anneks A redegør for, hvordan de fem attributter kan benyttes, og bidrager dermed til brugervenligheden af standarden. Anneks B indeholder en mapping af foranstaltningerne fra den tidligere version af standarden til den nye. Det giver et godt overblik over ændringerne for virksomhederne og kan være en hjælp til dem, der skal gå fra den tidligere version af standarden til implementering af den nye.

Tilsammen giver standardens nye struktur, indhold og de nye perspektiver en større tilgængelighed for de virksomheder og organisationer, der skal arbejde efter den.

**Hvad betyder det, at der er kommet nye versioner af standarderne?**
Da ISO/IEC 27001 er en kravstandard, som man kan vælge at blive certificeret efter, vil der være krav om recertificeringer. Certificeringer efter den tidligere udgave af ISO/IEC 27001 (fra 2017) gælder i en overgangsperiode på tre år fra udgivelsesdagen. Dvs. at recertificering efter den nye ISO/IEC 27001:2022 skal ske senest i 2025.

Selvom man ikke er certificeret, vil det være en god idé at få implementeret de nye ændringer, så man holder trit med den teknologiske udvikling og kan imødekomme markedskrav. En implementering af de nye ændringer betyder også en opdatering af ens SoA-dokument (Statement of Applicability). ISO/IEC 27001 stiller krav om, at virksomheder udarbejder et SoA-dokument på baggrund af foranstaltningerne i anneks A i ISO/IEC 27001 (samme foranstaltninger der gennemgås i ISO/IEC 27002). Det er i SoA-dokumentet, at man begrunder sine til- og fravalg af foranstaltninger.

**Ny version af standarden for risikostyring – ISO/IEC 27005**
En tredje standard i ISO/IEC 27000-serien, der også har fået en opgradering i 2022, er ISO/IEC 27005. Standarden er en vejledning i håndtering af informationssikkerhedsrisici, der kan hjælpe organisationer med at systematisere deres arbejde med risikostyring. Den er tæt koblet med ISO/IEC 27001 og 2, da den indeholder konkret vejledning i og eksempler på, hvordan kravene til risikostyring i 27001 kan opfyldes. ISO/IEC 27005 er også blevet opdateret for at gøre den mere brugervenlig og aktuel, fx med praktiske og kontekstnære eksempler.[48]

Dansk Standard har sammen med Alexandra Instituttet i 2023 udarbejdet en guide for risikostyring ift. cyber- og informationssikkerhed. Guiden bygger på principperne fra ISO/IEC 27005 og er tænkt som en hjælp til virksomheder, der gerne vil arbejde mere systematiseret med risikostyring ift. cyber- og informationssikkerhed. Risikostyringsprocessen beskrives i guiden i et lettilgængelig sprog og er suppleret med eksempler, der skal give virksomhederne et godt udgangspunkt for at komme i gang. Guiden er primært henvendt til små og mellemstore virksomheder, men giver for alle en god introduktion til systematisk risikostyring.

Guiden kan hentes her: www.ds.dk/risikostyring.

[48] Dansk Standard har udarbejdet et whitepaper, der beskriver de største ændringer i den nye version af ISO/IEC 27005: https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder/whitepaper-27005

# 5. Eksterne bidrag

## 5.3 EN BERETNING FRA EN DCIS

**Hvordan griber man opgaven an, når en ny enhed med en forholdsvis uprøvet arbejdsmetode skal udmønte initiativer for cyber- og informationssikkerhed på tværs af en kompleks sundhedssektor? Hvad kan uddannelses- og forskningssektoren lære af sundhedssektorens decentrale cyber- og informationssikkerhedsenhed?**

AF CHRISTA WULFF SARBY,
KOMMUNIKATION & EVENT, SUNDHEDSSEKTORENS DCIS

Den danske sundhedssektor er stor og består af mange meget forskellige aktører; lige fra små selvstændige klinikker til offentlige hospitaler med over 10.000 ansatte. Modenhedsniveauet for cyber- og informationssikkerhed er derfor også meget forskelligt aktørerne imellem. Samtidig behandler sektoren store mængder følsomme personoplysninger og sundhedsdata som led i borgernes behandlingsforløb, og dette arbejde understøttes af et komplekst it-landskab med forbundne systemer og infrastruktur.

I 2018 fik sundhedssektoren sin egen delstrategi for cyber- og informationssikkerhed, ligesom uddannelses- og forskningssektoren har fået det i år.

Og i november 2018 blev den decentrale cyber- og informationssikkerhedsenhed i sundhedssektoren (DCISSund/DCIS) oprettet i Sundhedsdatastyrelsen og integreret i styrelsens afdeling for cyber- og Informationssikkerhed.

En af de første opgaver for DCIS'en var at prioritere initiativerne til den sektorspecifikke strategi for cyber- og informationssikkerhed for sundhedsvæsenet. Det skete på baggrund af en ekstern vurdering af sundhedsområdets sårbarheder i forhold til cyber- og informationssikkerhed samt en analyse og vurdering af sundhedsområdets risici i forhold til cyber- og informationssikkerhed.

**En bredt funderet styregruppe**
Den næste opgave var at få aktørerne med på ombord.

'Først og fremmest har det været vigtigt at danne sig et overblik over sektorens nøgleinteressenter og strukturer. Samtidig har det været afgørende, at sundhedssektorens cyberstrategi giver mening i en forskelligartet sektor og forpligter til handling på alle niveauer', siger Søren Bank Greenfield, afdelingsleder for Cyber- og informationssikkerhedsafdelingen i Sundhedsdatastyrelsen.

Sundhedssektoren valgte fra starten at forankre arbejdet med udmøntningen af strategien i samme styregruppe, der var med til at formulere strategien. Styregruppen består af medlemmer fra hele sektoren og andre vigtige interessenter – herunder fra regionerne, KL, Digitaliseringsstyrelsen, CFCS, PLO, MedCom, Danske Regioner, Sundhedsstyrelsen, Sundhedsdatastyrelsen samt Indenrigs- og Sundhedsministeriets departement.

I arbejdet har Sundhedsdatastyrelsen haft fokus på at oprette et tillidsbaseret, formaliseret og tæt samarbejde mellem parterne og på at blive enige om en governancestruktur, som både for-

# 5. Eksterne bidrag

pligter alle parter, men som også kan modnes og udvikles undervejs.

Denne brede fundering i styregruppen har samtidig sikret enhedens legitimitet, løbende 'sanity checks' af retningen, værdien af initiativerne og spørgsmålet om det i virkeligheden også er det, som sektoren vil have og har behov for. Styregruppen har således deltaget som aktive deltagere og stillet sig kritisk an til de planer, som DCISSund har lagt for dagen.

**Hvad er lykkedes for DCIS?**
En tredje og mindst lige så vigtig opgave var at skabe grundlaget for, at enheden overhovedet kan arbejde: Medarbejderne.

'I en tid, hvor der er rift om medarbejderne i branchen, er det alligevel lykkedes vedvarende at tiltrække de rigtige kompetencer. Dette udgangspunkt gør, at der kan sikres kontinuerlig og stabil fremdrift i arbejdet', siger Søren Bank Greenfield.

Og endelig at sætte sikkerhed, Sundhedsdatastyrelsen og DCISSund-funktionen på agendaen ude i sektoren.

'Det har været vigtigt for os at komme ud og møde dem, der har en aktie i arbejdet med at sikre sektoren. Det giver både en bedre forståelse af problemstillingerne, og i hvilken sammenhæng løsninger skal virke rundt omkring i sektoren. Samtidig fremmer det jo altid samarbejdet, når man har mødt hinanden.'

Med sloganet 'Sharing is caring' har DCISSund i Sundhedsdatastyrelsen, i både nationale og internationale sammenhænge, lagt meget vægt på, at det er bedre at dele med hinanden, så alle kan tage ved lære af hinandens erfaringer, end at forsøge at gemme udfordringerne væk. Dette kræver, at der opbygges tillidsfulde samarbejdsfora, hvor man som aktør ved, at det, der bliver delt i de lukkede rum, ikke kommer videre.

**Ingen roser uden torne**
Centralt om DCIS'en arbejde har naturligvis været delstrategien, og arbejdet med udmøntning af strategien har ikke været uden bump på vejen. Men Sundhedsdatastyrelsen og sektoren har lært meget på de snart fire år, samarbejdet har eksisteret.

Tidligt i forløbet opdagede man et behov for at kommunikere et meget klart budskab til aktører, interessenter og samarbejdspartnere: Sundhedsdatastyrelsen og DCISSund agerer ikke kun på vegne af staten, men er til for hele sektoren.

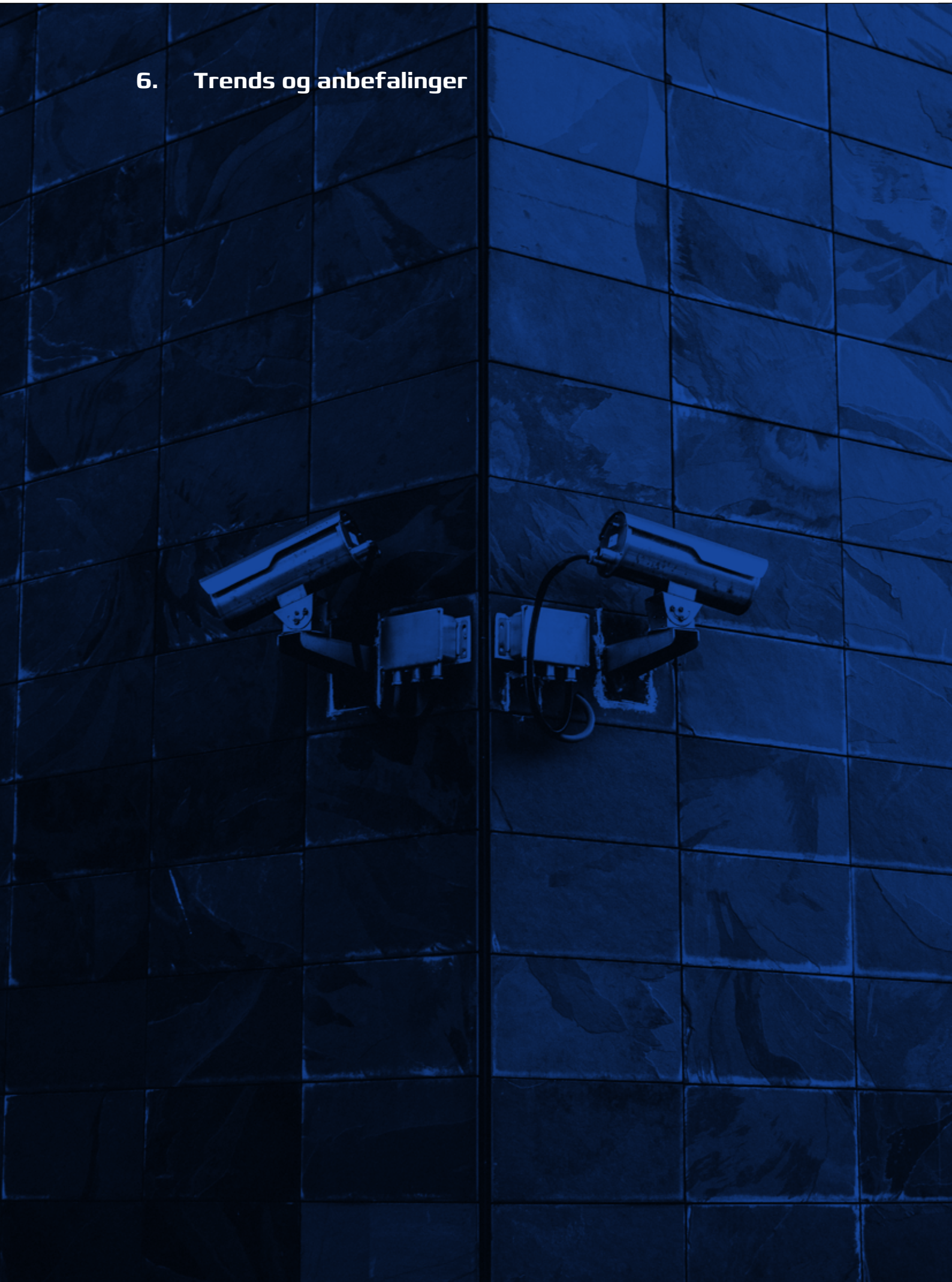
Derudover var det vigtigt at kommunikere, at Sundhedsdatastyrelsen tydeligt adskilte DCISSund-funktionen fra NIS-tilsynsfunktionen, så der ikke blev tvivl om, hvad informationer blev brugt til.

Nogle initiativer har virket gode på papiret, men gav ikke mening i forbindelse med udmøntningen: Når arbejdet skulle planlægges, kunne det efter nærmere analyse ikke lade sig gøre, eller de gav ikke den værdi, sektoren ønskede. Det har dog kunnet lade sig gøre at ændre og omforme initiativerne, fordi styregruppen har haft indblik i arbejdet, og derfor har kunne være med til at kvalificere og ændre planerne, så de igen gav den ønskede værdi.

Sundhedssektorens cyberstrategi var planlagt således, at dele af strategiens initiativer skulle finansieres efterhånden, som de blev sat i gang. Dette har vist sig svært at gøre. Derfor har styregruppen været meget opmærksom på, at holde den nye strategi inden for de faste økonomiske rammer.

**Fire gode råd til en ny DCIS**
1. Fokuser på udviklingen af håndgribelige produkter tidligt i strategien.
2. Få mere tidsmæssig frihed i strategien, så det passer til virkeligheden --> vi lægger sporene, mens vi kører.
3. Opbyg og facilitér operativt samarbejde og vidensdeling:
   a. Kortlæg de samfundsvigtige funktioner og deres IT-kritiske infrastruktur.
   b. Fastlæg et samlet cyberberedskab for sektoren og test det ved en øvelse.
   c. Opret og facilitér et fast operativt samarbejdsforum med sikkerhedschefer fra nøgleaktørerne.
   d. Fastlæg og implementer ansvars- og opgavefordeling ved varsling til og rapportering af hændelser fra nøgleaktørerne.
4. Etabler et professionelt sekretariat med kapacitet til programunderstøttelse og formidling af initiativerne, både til højere ledelse og til aktører og interessenter.

# 6. Trends og anbefalinger



# 6. Trends og anbefalinger

**2022 har været præget af Ruslands krig i Ukraine og de hybride angrebsformer. Cyberaktivisme er det nye sort, der sammen med ransomware spillede en hovedrolle i mediebilledet.**

**Med udgangspunkt i det aktuelle trusselsbillede giver vi her et bud på trends i 2023 og anbefalinger til hhv. ledelsen, til forskere og undervisere og til de it-ansvarlige på uddannelses- og forskningsinstitutionerne.**

## 6.1 CYBERTRENDS

**Flere informations- og cybersikkerhedsstrategier og DCIS'er**
Som følge af cyber- og informationssikkerhedsstrategien fra december 2021 skal der etableres 27 decentrale cyber- og informationssikkerhedsenheder (DCIS) i væsentlige og vigtige sektorer. Etableringen har været forsinket af folketingsvalget og de efterfølgende ændringer i ressortområder. Strategien medfører, at vi kommer til at se delstrategier fra hver af de mange sektorer, ligesom der i kølvandet af disse etableres en lang række videndelingsfora på strategisk, taktisk og operationelt niveau. Strategierne vil afspejle de forskellige modenhedsstadier, som sektorerne befinder sig på, og vil med tiden øge modenheden.

DKCERT opfordrer til, at aktører inden for og uden for sikkerhedsmiljøet parallellæser de forskellige sektorers strategier. At læse og forstå de forskellige tilgange til arbejdet er lærerigt.

Uddrag af uddannelses- og forskningssektorens delstrategi kan læses i kapitel 4.

https://www.cfcs.dk/da/nyheder/2023/dcis-forum-19-januar/

**Systematisk sårbarhedsudnyttelse fra statsaktører**
Phishingangreb stadig er de fleste angriberes foretrukne angrebsmetoder til kompromittering, men i kraft af at opmærksomheden på phishing bliver større og større, vil cyberkriminelle søge andre veje. Her kan systematisk udnyttelse af tekniske sårbarheder være vejen ind, hvorfor der både fra det legitime og illegitime miljø sættes flere kræfter ind på at finde sårbarheder og handle med exploit-koder. Antallet af sårbarheder på National Vulnerabilty Database har alle år været stigende og intet tyder på, at det ændrer sig.

https://cert.dk/da/news/2022-11-07/Advarer-om-udnyttelse-af-offentligt-tilgaengelige-0-dagssaarbarheder
https://cert.dk/da/news/2022-10-11/De-tyve-mest-populaere-saarbarheder-i-Kina
https://thehackernews.com/2021/07/chinas-new-law-requires-researchers-to.html

**Bedre formidling**
I midten af 2022 udkom den nyeste udgave af ISO/IEC 27002 og senere på efteråret også en ny version af selve standarden ISO/IEC 27001. Selv om standarder generelt set er svært stof, så gør reduceringen af foranstaltningerne fra 114 til 93 og opbygningen af strukturen i fire temaer standarden mere tilgængelig og dermed også lettere at arbejde med. Det peger mod en erkendelse i behovet for øget modenhed i formidlingen af cyber- og informationssikkerhed fra eksperter og arbejdsgrupper, som kan forplante sig ned mod andre lærings- og kommunikationsaktiviteter. Også en ny udgave af ISO27005 (vejledning i håndtering af informationssikkerhedsrisici) kom i 2022. En dansk udgave ventes i 2023.

https://www.ds.dk/da/nyhedsarkiv/2022/11/ny-version-af-standarden-for-informationssikkerhed-iso-iec-27001-ude-nu
https://www.ds.dk/da/nyhedsarkiv/2022/2/nu-er-den-her-ny-version-af-informationssikkerhedsstandarden-iso-iec-27002

# 6. Trends og anbefalinger

**Wiper i fremmarch**
Ligesom russisk destruktion af fysisk kritisk infrastruktur vha. raketter i krigen i Ukraine er en strategi, når fremgang på slagmarken ikke lykkes, ser destruktive cyberangreb også ud til at være på fremmarch. Statssponserede aktører har taget denne aktivitet til sig, og wipersoftware ser ud til at være fremskridende. Det kan også være en reaktion på, at flere og flere lande gør eller agter at gøre ransomwarebetalinger ulovlige.

https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.acronis.com/en-us/blog/posts/the-legal-implications-of-paying-ransomware-demands-the-evolving-state-of-ransomware/
https://cert.dk/da/news/2022-11-21/Australien-overvejer-at-forbyde-ransomware-betalinger

**Cyberaktivismen stiger**
I starten af 2023 så vi flere DDoS-angreb på danske banker, lufthavne og ministeriers websteder og til sidst også på seks af de otte universiteter i Danmark. Med dette er en tendens fra 2022 fortsat, hvor fjendtligtsindede aktører af politiske årsager angriber tjenester og services i andre lande. Cyberaktivisme er en angrebsform, der har til formål at skabe maksimal opmærksomhed fra medier og politisk niveau og 'fear, uncertainty and doubt', hvilket går hånd i hånd med misinformation. Det kan medføre tab af tillid til de bærende institutioner i samfundet.

Offermålene for cyberaktivisme har tidligere været mere offentligt kendte tjenester og hjemmesider fra politiske, aktivistiske miljøer, men metoden indgår i dag i højere grad i statssponserede aktørers strategier som en del af hybridkrigen. Men i takt med at beskyttelsen stiger og nyhedsværdien falder, forsøges overbelastningsangreb på mindre kritisk infrastruktur som fx uddannelsesinstitutioner og andre, i offentligheden mindre fremtrædende institutioner.

https://cert.dk/da/news/2022-05-18/CFCS-haever-trusselsniveauet
https://cert.dk/da/news/2022-05-23/Massive-boelger-af-DDoS-angreb-mod-russisk-storbank
https://cert.dk/da/news/2022-06-02/Advarer-organisationer-om-at-forberede-sig-paa-DDoS-angreb
https://cert.dk/da/news/2023-02-23/Advarer-om-DDOS-angreb-mod-danske-universiteter
https://cert.dk/da/news/2023-01-31/CFCS-haever-trusselsniveauet-for-cyberaktivisme
https://arstechnica.com/information-technology/2022/01/hactivists-say-they-hacked-belarus-rail-system-to-stop-russian-military-buildup/

**Mangel på arbejdskraft blandt cyberkriminelle**
Det er måske udtryk for ønsketænkning, men det kan ikke udelukkes, at efterspørgsel efter it-tekniske kompetencer også er et issue blandt cyberkriminelle grupperinger, ligeså vel som det er blandt legitime virksomheder, organisationer og myndigheder. Høje lønninger og bonusordninger præger givetvis miljøet, hvor kriminelle grupper konkurrerer hårdt om at tiltrække de største talenter for at udvikle produkter og bevare markedsandele. Både kriminelle grupperinger, statssponserede aktører og stater har behov for arbejdskraft til at løse deres opgaver. I takt med at aktiviteterne stiger i antal, stiger også behovet for arbejdskraft. Der er også spekuleret i, at Ruslands mobilisering til krigen i Ukraine og hjerneflugt fra Rusland kan have gjort et indhug i arbejdskraften.

https://www.bleepingcomputer.com/news/security/cybercrime-job-ads-on-the-dark-web-pay-up-to-20k-per-month/
https://securelist.com/darknet-it-headhunting/108526/
https://www.computerworld.dk/art/256992/hackergruppen-conti-er-drevet-som-en-virksomhed-men-produktet-er-ransomware-saadan-er-en-af-verdens-stoerste-hackergrupper-bygget-op

# 6. Trends og anbefalinger

## 6.2 GDPR-TRENDS

**Overførsel til tredjelande**
Overførsel til USA har været vanskeliggjort siden Schrems II-dommen i 2020, hvor Privacy Shield-grundlaget som overførselsgrundlag blev ugyldigt.

En hensigtserklæringsaftale mellem EU og USA om principperne om genetablering af et rammeværk for transatlantisk dataoverførsel i marts 2022 resulterede i et nyt rammeværk: EU-US Data Privacy Framework (DPF)[49]. Baseret på dette har EU-Kommissionen udarbejdet et udkast til en tilstrækkelighedsafgørelse vedrørende beskyttelsesniveauet for overførsel af personoplysninger til USA, som blev offentliggjort i december 2022.

Udkastet blev sendt i høring til European Data Protection Board (EDPB) og EU-Parlamentet, som skal komme med en ikke-bindende udtalelse. Herefter kan EU-Kommissionen forelægge udkastet til tilstrækkelighedsafgørelse for godkendelseskomiteen (som består af repræsentanter for medlemsstaternes regeringer), før tilstrækkelighedsafgørelsen kan vedtages. Processen kan tage tre til seks måneder, og vedtagelsen kan formentlig forventes i sommeren 2023.

I skrivende stund har EDPB udtalt sig positivt over for DPF, dog med en række bekymringer.[50]

Max Schrems' organisation NOYB (akronym for 'none of your business') har allerede udtalt sig skeptisk. Denne mener, at der ikke er grundlag for, at det nye DPF vil beskytte EU-borgernes data tilstrækkeligt og ønsker, at den Europæiske Unions Domstol skal efterprøve dette hurtigst muligt.

Overførelser har fyldt meget og i den brede offentlighed været det dominerende tema. Men et andet tema er, hvorvidt de store tech-giganter indsamler data til egne formål.

[49] EU's hjemmeside om EU – US Data Privacy Framework: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632
[50] Datatilsynets hjemmeside om EDPB's udtalelse om EU-US Data Privacy Framework: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/nyt-om-overfoersel-af-personoplysninger-til-usa

# 6. Trends og anbefalinger

**Tech-giganternes indsamling af data til egne formål**
Ved nærmere eftersyn af eksempelvis Chromebook-sagen i Helsingør Kommune, hvor problemet i første omgang var en utilstrækkelig risikovurdering, der ikke evnede at vise et behov for en konsekvensanalyse, så handler sagen i sin essens også om, at Google indsamler data til egne formål, og at Helsingør Kommune har ikke lovhjemlen på plads til den videregivelse.[51]

Det samme gør sig gældende, når de 18 tyske datatilsyn i en rapport konkluderer, at offentlige myndigheder ikke kan anvende Microsoft 365.[52]

Sager som disse viser, at det ikke alene er tredjelandsoverførsler, der er problemet med de store tech-giganter. Det kan være, at DPF kan løse tredjelandsoverførselsproblematikken i forhold til de amerikanske tech-giganter, men de skal også tage fat i deres omfattende dataindsamlinger som dataansvarlige. For hvilken lovhjemmel baseres deres behandlinger på?

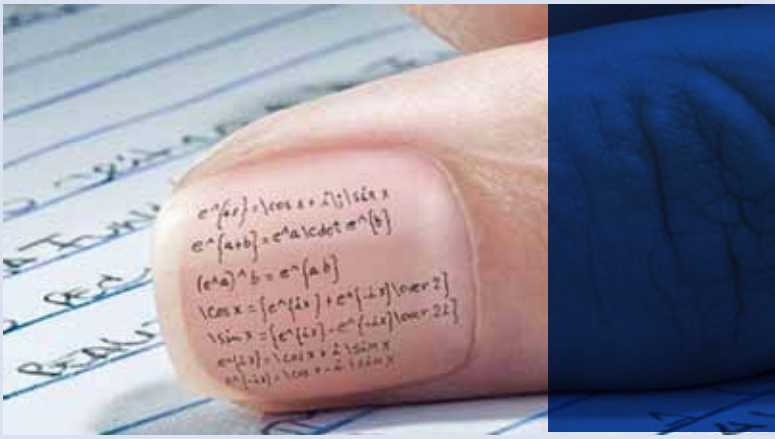
Det Europæiske Databeskyttelsesråd (EDPB) har truffet tre bindende afgørelser i såkaldte tvistbilæggelsessager indbragt af det irske datatilsyn mod Metas behandling af personoplysninger på henholdsvis Facebook, Instagram og WhatsApp.[53]

Sagerne handlede om, hvorvidt behandling af personoplysninger af hensyn til opfyldelse af en kontrakt er en passende behandlingshjemmel, når formålet med behandlingen er adfærdsbaseret markedsføring eller forbedring af services.

På baggrund af EDPBs bindende afgørelser har det irske datatilsyn nu udstedt en samlet bøde på 390 mio. Euro i januar 2023. Tidligere i 2022 udstedte det irske datatilsyn en bøde 405 mio. euro til Meta, som handlede om Instagrams offentliggørelse af e-mailadresser og telefonnumre på mindreårige, der havde Instagram Business-konti, og en 'public-by-default'-indstilling for mindreåriges personlige Instagram-profiler.[54] Instagram har efterfølgende standset sin praksis på området.

Om disse høje bøder vil få en påvirkning på bødefastsættelsen i Danmark, vil tiden vise.

[51] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag
[52] https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf
[53] https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/dec/edpb-traeffer-afgoerelse-i-tre-sager-vedroerende-facebook-instagram-og-whatsapp
[54] https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/sep/det-irske-datatilsyn-udsteder-boede-til-instagram-paa-405-millioner-euro



# 6. Trends og anbefalinger

**NIS2 og GDPR**
Med vedtagelse af NIS2-direktivet i december 2022 er der nu sket tilpasning af cybersikkerhedsforpligtelser og -arbejde i forhold til GDPR.[55] Læs evt. mere om NIS2 i afsnit 5.1.

Først og fremmest findes lovhjemlen til behandling af personoplysninger i forbindelse med NIS2 i GDPR, artikel 6, hvor behandlingen baseres på myndighedsudøvelse for offentlige myndigheder eller retlig forpligtelse eller legitim interesse for private virksomheder.[56]

Og ved overførsel til tredjelande i den forbindelse skal overførselsgrundlaget findes i undtagelsesreglerne i GDPR, artikel 49, hvor overførslen kan ske af hensyn til vigtige samfundsinteresser uden indgåelse af Standard Contractual Clauses (standardbestemmelser om databeskyttelse vedtaget af EU-Kommissionen).[57]

Ved overtrædelser, der også medfører brud på persondatasikkerheden, som de kompetente myndigheder bliver opmærksom på i forbindelse med deres tilsyn, skal de underrette Datatilsynet.

Hvis dette medfører administrative bøder efter GDPR, må der ikke samtidig udstedes bøder efter NIS2 – dvs. man bliver fri for dobbelt bøde.

NIS2 indeholder krav om risikobaseret tilgang, hvor risikovurderinger udføres med vinklingen risiko for samfundet. De virksomheder, der er omfattet af GDPR og NIS2, har nu tre overordnede dimensioner i deres risikovurdering:

- GDPR-mæssigt - risici i forhold til de registrerede (de personer, som data drejer sig om)
- Informationssikkerhedsmæssigt - risici i forhold til informationssikkerhed (it-sikkerhed, fysisk sikkerhed, medarbejdersikkerhed osv.)
- Cybersikkerhedsmæssigt - risici for samfundet

Cybersikkerhedshændelser skal indberettes, og en central sårbarhedsdatabase i EU skal oprettes - den udpegede, nationale CSIRT skal koordinere national rapportering af væsentlige hændelser inden for 24 timer, ajourføre oplysninger inden for 72 timer efter hændelsen, og en endelig rapport indgives senest en måned efter underretningen eller en måned efter håndteringen af den væsentlige hændelse. Rapporteringsprocessen minder om GDPR's underretning af brud på persondatasikkerhed samt håndtering af incidents og eskaleringsproces i forbindelse med informationssikkerhed.

[55] Om NIS2 på EU's hjemmeside: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[56] NIS2-direktivet, artikel 14 og præambelbetragtning nr. 121: https://eur-lex.europa.eu/eli/dir/2022/2555
[57] NIS2-direktivet, præambelbetragtning nr. 45
[58] NIS2-direktiv, artikel 3

# 5. Trends og anbefalinger

## 6.3 ANBEFALINGER TIL LEDELSEN PÅ UDDANNELSES- OG FORSKNINGSINSTITUTIONERNE

Informationssikkerhed er ledelsens ansvar. Brud på sikkerheden og brud på databeskyttelseslovgivningen kan koste dyrt i form af økonomisk tab, dårlig omtale og udgifter til oprydning. DKCERT anbefaler, at institutionens ledelse afsætter de fornødne ressourcer til at løfte opgaven.

Desuden anbefaler DKCERT følgende:

1. Gør det tydeligt, at ledelsen er aktivt og løbende involveret i arbejdet med informationssikkerhed.
2. Samtænk og integrer i videst muligt omfang de processer og procedurer (risikovurdering, implementering af standarder, tilsynsførelse og underretning om sikkerhedshændelser), hvor cyber, it- og informationssikkerhed og GDPR har snitflader med hinanden.
3. Understøt en kultur, hvor dialog om informationssikkerhed er en del af dagligdagen, og hvor risiko og sikkerhed er tænkt ind fra starten i udviklingen af produkter og tjenester.
4. Del viden og erfaringer og bidrag til den fælles styrkelse af informationssikkerheden i sektoren ved at anvende de tjenester, som DKCERT stiller til rådighed.
5. Adressér informationssikkerhed i den langsigtede strategiske planlægning og udarbejd i tilknytning til det en strategi for kommunikations- og læringsindsatsen i forhold til cyber- og informationssikkerhed, som også indtænker studerende og ansatte, før de får tilknytning til institutionen.
6. Sørg for løbende at adressere behovet for at efterleve retningslinjer for informationssikkerhed i organisationen og monitorer efterlevelsen. Det er ikke nok, at medarbejderne undervises.
7. Tag stilling til risikoen for, at ansatte, studerende mv. bliver rekrutteret til uvederhæftige handlinger og overvej tiltag mod dette.
8. Overvej evt. disciplinære forholdsregler og mulige konsekvenser ved overtrædelse af sikkerhedspolitikken ved fejl begået som følge af ubevidsthed eller uagtsomhed.
9. Efterspørg beredskabsplaner, test og øvelser.
10. Synliggør risikostyring gennem løbende risikovurderinger af forretningskritiske systemer – også ved hændelser, der rammer lignende institutioner.

# 5. Trends og anbefalinger

## 6.4 ANBEFALINGER TIL FORSKERE, UNDERVISERE OG TEKNISK-ADMINISTRATIVT PERSONALE PÅ UDDANNELSES- OG FORSKNINGSINSTITUTIONERNE

Mellemledere, forskere, undervisere, andre ansatte og tilknyttede samarbejdspartnere har en væsentlig rolle som aktivt udførende personer i forhold til opretholdelse af informationssikkerheden og beskyttelse af værdien af det udførte arbejde. Denne rolle bør alle på en uddannelses- og forskningsinstitution være bevidst om.

Derudover anbefaler DKCERT forskere, undervisere og teknisk-administrativt personale følgende:

1. Lær informationssikkerhedspolitikken og lokale retningslinjer at kende.
2. Vær bevidst om værdien af arbejdet og konsekvenserne ved kompromittering af fortrolighed, integritet og tilgængelighed.
3. Tænk på, om arbejdsområder er tilstrækkeligt beskyttet i forhold til værdien – fx. ift. dataindsamlende apps på såvel arbejds- som private enheder.
4. Vurder i hvilken grad jeres samarbejdsparterne og interessenter stiller krav til en forøgelse af jeres informationssikkerhedsniveau.
5. Understøt en kultur i områderne og blandt kolleger, hvor dialog om informationssikkerhed er en del af hverdagen.

## 6.5 ANBEFALINGER TIL IT-ANSVARLIGE PÅ UDDANNELSES- OG FORSKNINGSINSTITUTIONERNE

DKCERT anbefaler, at institutionens informationssikkerhedsansvarlige sammen med ledelsen og repræsentanter for forretningen udarbejder en risikovurdering som grundlag for alle sikkerhedstiltag. En risikobaseret tilgang er et krav både i ISO 27001 og i GDPR. En risikovurdering kan med fordel udarbejdes ud fra anbefalingerne i ISO 27005 eller et rammeværk som fx Octave Allegro.

Derudover anbefaler DKCERT følgende:

1. Beton vigtigheden af at gennemføre regelmæssige sårbarhedsscanninger.
2. Anvend kommunikationshjælp til at gennemføre læringsrettede tiltag, og indarbejd det i planlægning af året.
3. Tænk sikkerhed ind i relationen til leverandører og samarbejdspartnere og følg op med kontrol.
4. Hav fokus på sikkerheden ved udvikling af applikationer og tjenester samt tilretninger af eksisterende systemer, eksempelvis med udgangspunkt i principperne om security og privacy by design.
5. Anvend single sign-on suppleret med to-faktor-autentifikation. Overvej de forskellige typer to-faktorløsninger.
6. Tilbyd en passwordmanager til brugerne.
7. Hold øje for initiativer som følge af sektorens cyber- og informationssikkerhedsstrategi.
8. Vær bevidst om at et vellykket angreb på én uddannelses- og forskningsinstitution sandsynligvis vil blive prøvet på en anden.
9. Overvej brugen af persondata og beskyttelse af disse ved implementering af nye systemer. Vær opmærksom på princippet om dataminimering jf. GDPR.
10. Afsæt ressourcer til deltagelse i og anvendelse af sektorens fælles tjenester.

# 7. Referenceliste

**Academic Security SIG**
Academic Security SIG er et diskussionsforum, organiseret under FIRST. Academic Security SIG sigter mod at understøtte samarbejdet mellem akademiske sikkerhedsteams mhp. deling af erfaringer om aktuelle sikkerhedsproblemer. Det er primært etableret for at skabe forudsætningerne for samarbejde om forbedring af sikkerheden i akademiske miljøer, herunder forsknings- og uddannelsesnetværk, universitets-CSIRT'er og videnskabs- og forskningsinfrastrukturer. SIG står for Special Interest Group. Under FIRST er der en lang række SIG'er.

**CERT /CSIRT**
Et CSIRT (Computer Security Incident Response Team) er et 'team af eksperter, der reagerer på computerhændelser, koordinerer deres løsning, underretter sine medlemmer eller kunder, udveksler information med andre og hjælper med at afhjælpe hændelsen' (definition fra Internet Governance Forum).

CERT® var fra 1997 til 2021 et registreret varemærke og stod oprindeligt for Computer Emergency Response Team. Det krævede autorisation fra Software Engineering Institute på Carnegie Mellon University at anvende betegnelsen. I stedet kan alle den type teams kalde sig CSIRT.

DKCERT - har fra grundlæggelsen i 1991 som sikkerhedsteam for Forskningsnettet – siden 2012 en del af DeiC - været autoriseret til at kalde sig CERT. DKCERTs officielle navn er Danish Computer Security Incident Response Team.

Der er CSIRT-teams i 104 lande verden over (se FIRST.org og Trusted Introducer.)

Iht. NIS-direktivet skal EUs medlemsstater sørge for etableringen af CSIRT'er i alle relevante sektorer og udpege en national CSIRT, som skal være kontaktpunkt for medlemsstaten i EU-sammenhæng. I Danmark er CFCS national CSIRT.

**CFCS**
CFCS blev etableret i 2012 som en del af Forsvarets Efterretningstjeneste. Organisatorisk er CFCS en af seks sektorer i Forsvarets Efterretningstjeneste. Centerets organisatoriske placering har været under evaluering i 2022-23, men forbliver uændret.

**CISA**
CISA står for Cybersecurity and Infrastructure Agency og er et føderalt agentur, hjemmehørende under det amerikanske Departement of Homeland Security. CISA løser opgaver med henblik på minimering af risici i forhold til cybersikkerhed og fysisk infrastruktur. CISA svarer til CFCS i Danmark.

**DCIS**
Den Nationale Strategi for Cyber- og Informationssikkerhed 2022-2024 fra december 2021 forudsætter, at der udarbejdes sektorstrategier og oprettes decentrale cyber- og informationssikkerhedsenheder (DCIS) for alle samfundsvigtige funktioner, der er digitalt understøttet.

# 7. Referenceliste

DCIS skal sikre videndeling, koordinere tværgående hændelser, deltage i øvelser og sikre at der årligt planlægges og gennemføres beredskabsøvelser for ministerområdet. Mens der under National Strategi for Cyber- og Informationssikkerhed 2018 blev etableret seks DCIS'er for de såkaldt kritiske infrastruktursektorer, er der fra 2023 27 DCIS'er, der koordineres af CFCS, herunder en i Uddannelses- og Forskningsstyrelsen.

Internationalt kan det danske begreb DCIS nærmest sammenlignes med et 'ISAC', et 'Information Sharing and Analysis Center'.

**CIO-gruppen**
CIO-gruppen består af universiteternes it-chefer. CIO-gruppen har til opgave at fremme universiteternes samarbejde og erfaringsudveksling om anskaffelse, drift og opgradering af it-strukturer, der kan understøtte universiteternes faglige og administrative opgaveløsning.

**CISO-forum**
CISO-forum er en arbejdsgruppe under CIO-gruppen og består af universiteternes informationssikkerhedschefer og -koordinatorer. Chefen for DKCERT er associeret medlem.

**DeiC**
Danish e-infrastructure Cooperation er samarbejdet med og mellem de danske universiteter, etableret i 2012. DeiC koordinerer leverancen og udviklingen af den nationale digitale forskningsinfrastruktur. DeiCs formål er at sikre regnekraft, datalagring og netværksinfrastruktur til dansk forskning og uddannelse. DeiC er en virtuel enhed under Uddannelses- og Forskningsministeriet og resultatet af en aftale indgået mellem de otte universiteter og Uddannelses- og Forskningsstyrelsen. DKCERT leveres gennem DeiC.

**ENISA**
ENISA er Den Europæiske Unions Agentur for Cybersikkerhed. ENISA bidrager til EUs cyberpolitik og samarbejder med organisationer og virksomheder om at øge tilliden til den digitale økonomi og styrke EU-infrastrukturens modstandsdygtighed, bl.a. ved at udarbejde cybersikkerhedscertificeringsordninger, dele viden, uddanne personale, opbygge strukturer og øge bevidstheden om cybersikkerhed.

**Forskningsnettet**
Forskningsnettet er et højhastighedsnetværk, grundlagt 1987, der forbinder danske universiteter og forskningsinstitutioner. Siden 2012 drives det af DeiC. Ud over det fysiske netværk forsyner DeiC forskningsinstitutionerne med en række tjenester til e-infrastruktur og eScience, herunder DKCERT etableret 1991.

**GÉANT**
GÉANT er det fælles-europæiske forskningsnet. GÉANT forbinder de nationale forskningsnet (NRENs) i Europa med hinanden, med forskningsnet i andre verdensdele og med det kommercielle internet. DeiC er medlem af GÉANT gennem NORDUnet og deltager i en række projekter og samarbejder under GÉANT.

# 7. Referenceliste


**NREN**
NREN står for National Research and Education Network. Forskningsnettet er det danske NREN.

**NORDUnet**
NORDUnet er et fællesnordisk samarbejde mellem de nationale forsknings- og uddannelsesnetværk i Danmark, Finland, Island, Norge og Sverige.

**SIG-ISM (GÉANT)**
SIG-ISM er GÉANTs 'special interest group' for CISO'er m.fl. for nationale forskningsnet (NRENs). Der findes en række SIG'er under GÉANT.

**SikRef**
SikRef står for sikkerhedsreferencegruppe og er et netværk for sikkerhedsteknikere ved universiteter og forskningsinstitutioner. DKCERT driver netværket, der mødes 4-6 gange årligt.

**TF-CSIRT**
TF-CSIRT (Task Force Computer Security Incident Response Teams) er et forum, fra 2000-2022 under de europæiske forskningsnetværks paraplyorganisation GÉANT, men koordineres fra juli 2022 lige som Trusted Introducer af the Open CSIRT Foundation.

De nu ca. 500 medlemmer er organisationer, der håndterer sikkerhedshændelser (CERT/CSIRT/PSIRTs), hovedsageligt fra det europæiske område. Under TF-CSIRT kan medlemsorganisationerne mødes med andre teams af samme type og diskutere emner af fælles interesse. TF-CSIRT arrangerer også kurser og fremmer brugen af fælles standarder og procedurer for håndtering af sikkerhedshændelser.

**Trusted introducer**
Trusted Introducer (TI) blev etableret som en tjeneste i Europa i 2000. Formålet er at hjælpe teams, der håndterer sikkerhedshændelser, med at samarbejde og dermed forbedre sikkerheden gennem hurtigere reaktion på angreb og nye trusler. TI har oprettet og vedligeholder en database over teams med en oversigt over deres modenheds- og kompetenceniveau. Til det formål er der etableret en akkrediterings- og certificeringsmetode, baseret på bedste praksis, som er blevet udviklet og anvendt i mange år inden for TI-samarbejdet. Medlemmer af Trusted introducer mødes i regi af TF-CSIRT.

DKCERT var blandt grundlæggerne af Trusted Introducer og er akkrediteret siden 2002 – fra marts 2023 kandidat til certificering. Der er i alt ni danske medlemsteams.

**WISE Community**
WISE er et globalt fællesskab, hvor sikkerhedseksperter deler information og skaber samarbejde mellem forskellige e-infrastrukturer inden for forskningsområdet som fx CERN. WISE leverer en ramme af standarder, retningslinjer og praksis for at fremme beskyttelsen af kritisk infrastruktur. WISE holder en-to gange om året fælles møde med GÉANTs SIG-ISM.

**DKCERT/DeiC**
DTU, Asmussens Allé
Bygning 305
2800 Kgs. Lyngby

t 35 88 82 55
m cert@cert.dk
w www.cert.dk

# Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed