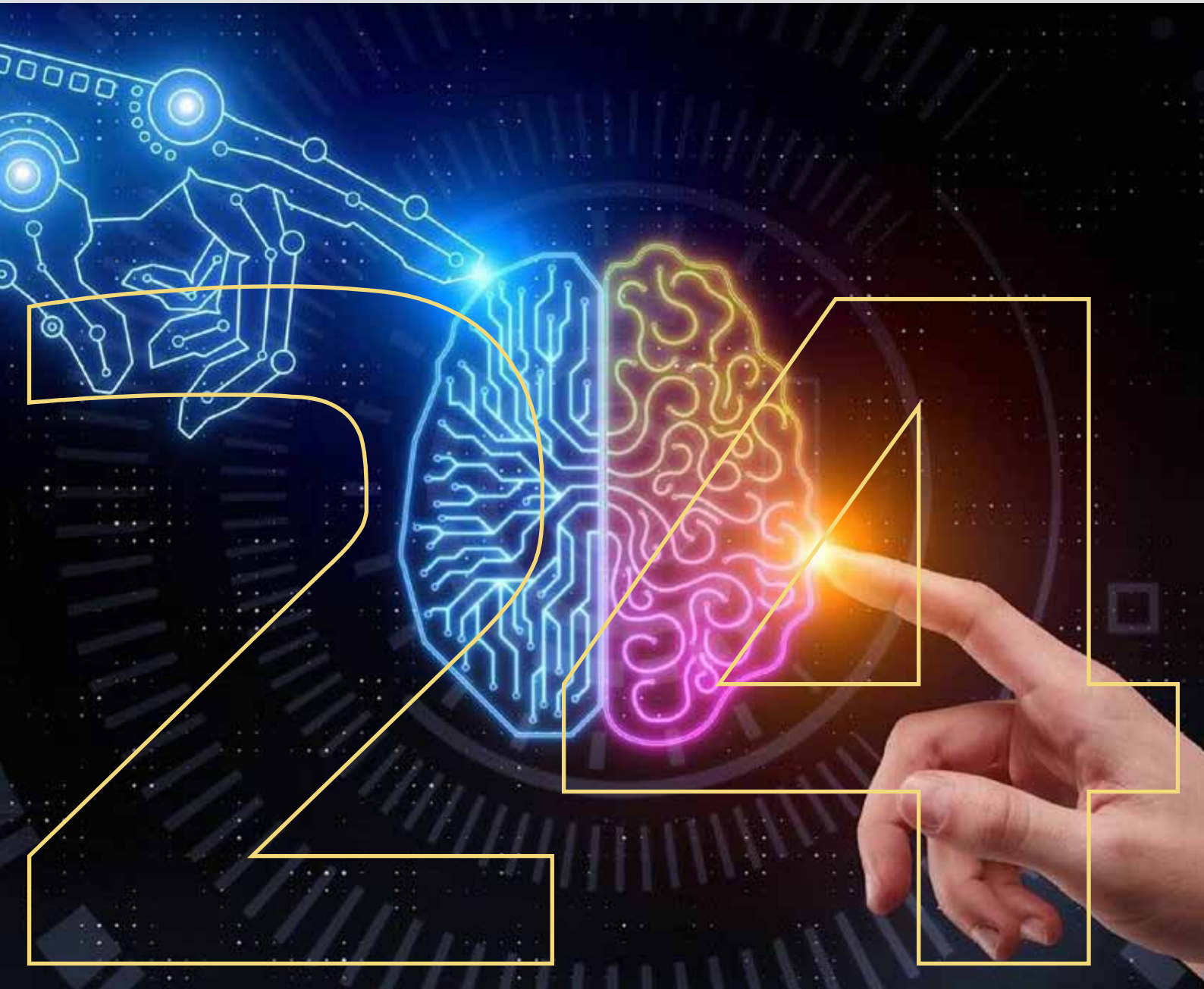
DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed



Kolofon

DKCERT TRENDRAPPORT 2024

Redaktion: Eskil Sørensen og Martin Bech, DKCERT
Redaktionen afsluttet 1. april 2024

Tak til vores bidragydere:
Claudia Zöllner, projektleder, Dansk IT
Laura Kocksch, M.A. Post-Doctoral Researcher in The Techno-Anthropology Lab, Aalborg University
Torben Elgaard Jensen, PhD, professor of Techno-Anthropology and Science & Technology Studies, Aalborg University
DCIS-UFM, Uddannelses- og Forskningsministeriets decentrale cyber- og informationssikkerhedsenhed
Medarbejdere ved DKCERT

Grafisk design:
Kiberg & Gormsen

Trusselsvurdering og redaktionelle bidrag:
Henrik Larsen, sikkerhedskonsulent, Henrik Larsen Informationssikkerhed

Illustrationer:
Jon Skræntskov

DeiC-journalnummer:
DeiC-JS 22/1005735-1

DKCERT - en del af DeiC
DTU, Produktionstorvet, Bygn. 426
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.

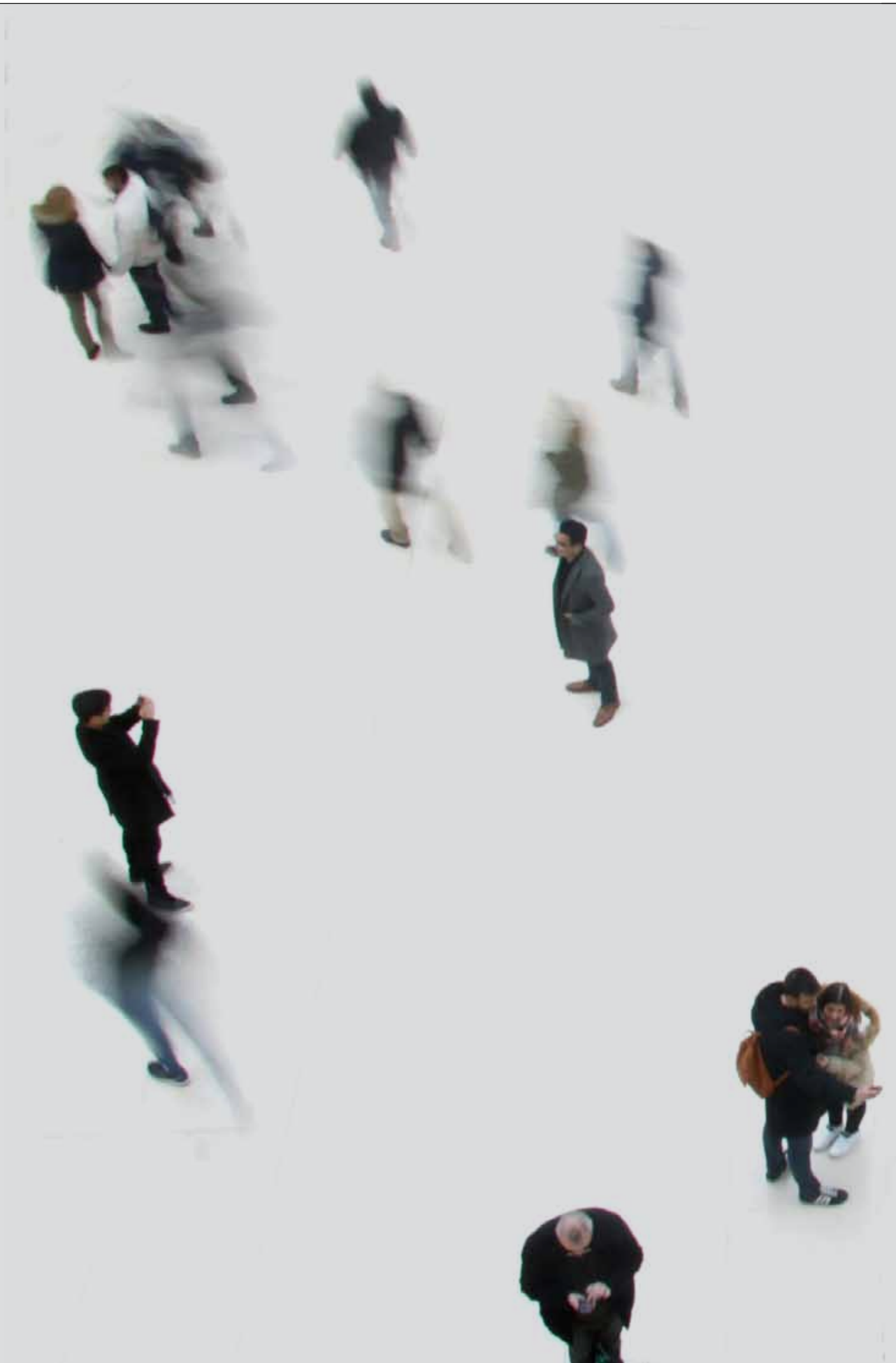
DKCERT overvåger det danske forskningsnet for uønskede aktiviteter, sender varsler ud til uddannelsesinstitutionerne, indsamler oplysninger om sårbarheder og foretager sårbarhedsscanninger af uddannelses- og forskningsinstitutioner.

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 er en del af DeiC, Danish e-Infrastructure Consortium. DeiC er det nationale samarbejde med og mellem universiteterne om levering af digital forskningsinfrastruktur. DeiCs hovedopgaver er levering af Forskningsnettet og tilhørende tjenester, datalagring og data managementtjenester, supercomputere og kvanteinfrastruktur. DeiC koordinerer den nationale infrastruktur og repræsenterer samarbejdet i internationale organisationer. DeiCs opgave er defineret i bekendtgørelse 615-2024 udgivet af Uddannelses- og Forskningsstyrelsen.

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 februar 2024 certificeret medlem af Trusted Introducer og TF-CSIRT (Task Force Computer Security Incident Response Team)[1].

[1] Se referenceliste i afsnit 6.



Indholdsfortegnelse

1. Velkommen

Velkommen til DKCERTs TRENDRAPPORT 2024.

I 2023 introducerede vi undervisere, forskere samt teknisk-administrativt personale ved uddannelsesinstitutionerne som ny målgruppe for trendrapporten. Med udvidelsen af målgruppen markerede vi, at informationssikkerhed i vores sektor vedrører dem, der arbejder med informationer i sektoren. Det gør vi alle.

Hele indholdet i denne trendrapport, der bl.a. omfatter en trusselsvurdering og en gennemgang af DKCERTs opgaver det forgangne år, er ikke nødvendigvis relevant for alle i uddannelsesinstitutionerne at læse, men alligevel vigtig at orientere sig i for at forstå trusselsbilledet. Forstår man trusselsbilledet, er der større incitament til at kende regler og politikker for sikkerhedsadfærd i ens organisation og dermed også til efterlevelse af regler og politikker. For det er i efterlevelsen, at vi ser, om indsatsen til at øge sikkerheden har en effekt.

Men hvordan måler man i det hele taget efterlevelsen og effekten?

Til at svare på de spørgsmål har vi inviteret tre af DKCERTs samarbejdspartnere for at fortælle om, hvordan de arbejder med målinger af informationssikkerhed.

En svær og ressourcekrævende disciplin på et område, som alle gerne vil have et ja-nej svar på. For hvornår er man sikker (nok)? Og hvilke målemetoder er bedst egnet til både analyse og formidling?

Netop det er temaet for årets rapport. Målemetoder af informationssikkerhed. Vi giver ordet til vigtige aktører på denne dagsorden: Vores egen sektors decentrale cyber- og informationssikkerhedsenhed, Dansk IT og Aalborg Universitets TANTlab. Alt dette for at inspirere sikkerheds-miljøet til at blive dyg-

1. Velkomst

tigere til at arbejde med målinger af informationssikkerhed og bruge målinger aktivt til at forstå, hvad der virker, og hvad der ikke gør. Kun ved at dele erfaringer kan vi opnå den nødvendige styrkelse af sikkerhedsniveauet.

Trendrapportens opbygning
Trendrapporten 2024 er bygget op med udgangspunkt i trusselsvurderingen, som gennemgår de trusler, vi ser på baggrund af vores kilder, hændelser og materiale fra vores samarbejdspartnere.

Trusselsvurderingen fremgår af kapitel 2, og i kapitel 3 gennemgår vi de opgaver, som DKCERT har løftet i 2023 og de tjenester, vi stiller til rådighed for sektoren. Vores data fra sårbarhedsscanningerne viser bl.a., at der er fundet flere kritiske sårbarheder end tidligere.

I kapitel 4 har vi bidrag fra vores eksterne samarbejdspartnere, som vi har stillet spørgsmålet: Hvordan arbejder I med målinger af informationssikkerhed?

I kapitel 5 gennemgår vi de trends, vi ser inden for databeskyttelses- og cyber- og informationssikkerhedsområdet, og vi formidler de anbefalinger, vi anser for at være de vigtigste at implementere for vores sektor. Kapitel 6 indeholder en liste over alle de aktører, som DKCERT nationalt og internationalt har berøring med.

Rigtig god fornøjelse med læsningen.

DKCERT

2. Trusselsvurdering 2024

Cybertruslen mod den danske uddannelses- og forskningssektor

2.1. INDLEDNING

Dette er den femte årlige trusselsvurdering for uddannelses- og forskningssektoren, udarbejdet af DKCERT.

Den første blev offentliggjort i Trendrapporten 2020, hvor det bl.a. hedder: 'Trusselsvurderingen er udarbejdet efter samme metode som trusselsvurderingerne fra Center for Cybersikkerhed og har til formål at hjælpe institutionerne med at kende og forstå deres modstandere i cyberspace, så de bedre kan vurdere den risiko, som aktørerne udgør, og så de bedre kan forsvare sig mod dem.'

Trusselsvurderingen anvender fortsat den samme skabelon som hidtil, men det kildemateriale, der er lagt til grund for de årlige vurderinger, har ændret sig lidt gennem årene, bl.a. er udvalget af andre myndigheders trusselsvurderinger blevet større.

Senest er Uddannelses- og Forskningsministeriets decentrale cyber- og informationssikkerhedsenhed (DCIS-UFM) blevet etableret som en nær samarbejdspartner for DKCERT. DCIS-UFM har som en del af sine definerede opgaver i efteråret 2023 udarbejdet en trusselvurdering, der opsummerer tendenser i cybertruslen og gennemgår truslen mod de danske universiteter og særligt udsatte forskningsområder, ligesom det beskrives, hvordan kvanteteknologi vil påvirke cybersikkerheden offensivt og defensivt.

Denne vurdering er imidlertid ikke offentliggjort for en bredere kreds, men er inddraget som baggrundsmateriale for DKCERTs trusselsvurdering.

DKCERTs trusselsvurderinger er de eneste, der specifikt dækker den danske uddannelses- og forskningssektor, og som regelmæssigt bliver offentliggjort (Center for Cybersikkerhed har således ikke udsendt en trusselsvurdering for sektoren siden efteråret 2021); det er fortsat DKCERTs intention hvert forår at udgive trusselsvurderinger som en del af årets Trendrapport.

I det følgende beskriver vi DKCERTs hovedvurderinger, udviklingen, trusler og risici og situationsbilledet for sektoren. Til sidst uddyber vi de enkelte trusselskategorier hver for sig og begrunder vurderingerne af trusselsniveauet for de enkelte kategorier.

DKCERT anvender de samme trusselskategorier, som Center for Cybersikkerhed bruger i sine trusselsvurderinger – den seneste overordnede er '*Cybertruslen mod Danmark 2023*', udgivet 8. maj 2023.[2] Ligeledes anvender DKCERT samme skala for trusselsniveau (se *Trusselsniveauer ifølge Forsvarets Efterretningstjeneste på* side 9) i vurderingen som FE og CFCS. Men skalaen, som har været anvendt i mange år, har den svaghed, at den ikke er i stand til at afspejle et stadigt stigende trusselsniveau. Derfor giver vi sidst i afsnit 2.2 en vurdering af udviklingen inden for trusselskategorierne.

2.2. HOVEDVURDERINGER

DKCERT vurderer ud fra kriterierne i FE's skala, at truslen mod uddannelses- og forskningssektoren fra:

> Cyberspionage er **MEGET HØJ**
> Cyberkriminalitet er **MEGET HØJ**
> Cyberaktivisme er **MEGET HØJ**
> Destruktive cyberangreb er **LAV**
> Cyberterror er **INGEN**

Endvidere vurderer DKCERT, at truslen mod uddannelses- og forskningssektoren fra:

> Misinformation og desinformation er **HØJ**

Trusselskategorierne skal ikke opfattes som isolerede områder, ligesom det ikke udelukkende er separate og specialiserede trusselsaktører, der står bag hver kategori.[3]

Grundlæggende er vurderingen af et trusselsniveau betinget af fire kriterier: kapacitet, hensigt, planlægning og (mulig) iværksættelse. Hvis det konstateres, at alle fire kriterier er til stede, må niveauet for den pågældende trusselskategori sættes til MEGET HØJ. Dette har været niveauet for *cyberkriminalitet* i CFCS' vurdering i en del år. Fra 2020 har DKCERT og efterfølgende også CFCS vurderet truslen fra cyberspionage som ligeledes MEGET HØJ.

[2] https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2023.pdf

[3] Særligt FEs årlige såkaldte risikovurdering, 'Udsyn 2023', der er udgivet 14. december 2023, fremhæver sammenhængene mellem truslerne. ('Udsyn' er en beskrivelse af det efterretningsmæssige trusselsbillede og ikke en afvejning af sandsynligheder og konsekvenser, hvorfor betegnelsen 'risikovurdering' ikke er informationssikkerhedsfagligt helt præcis, jf. nedenfor om trusler og risici).

2. Trusselsvurdering 2024

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.

Fra i år er også *cyberaktivisme* blevet vurderet som MEGET HØJ. Det er næppe en lige så potent trussel som den fra cyberkriminalitet – i det mindste vil risikoscoren (se afsnit 2.3 om trusler og risici) være lavere – og omfanget af *cyberkriminelle* angreb har kun været stigende over årene.

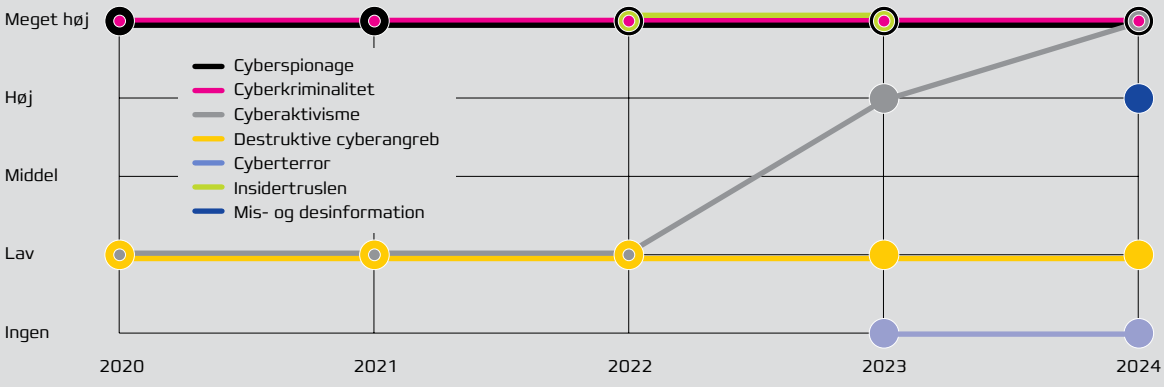
Ligeledes må det vurderes, at truslen fra cyberspionage ligger på et noget højere niveau i 2024, end den gjorde i 2020, men det kan skalaens niveauer ikke afspejle. Det kan derfor give mening at supplere vurderingen af trusselsniveauet med en vurdering af udviklingstendensen i trusselsniveauet for den enkelte trusselkategori.

DKCERT vurderer på baggrund af den hidtidige udvikling, at udviklingen af trusselsniveauet mod uddannelses- og forskningssektoren for:

> *Cyberspionage og cyberkriminalitet* er **STIGENDE**
> *Cyberaktivisme* er **STÆRKT STIGENDE**
> *Destruktive cyberangreb* er **UÆNDRET** på kort sigt, men med en sandsynlighed for at den kan være stigende på mellemlangt sigt
> For *Cyberterror* er udviklingen **UÆNDRET**
> For misinformation og desinformation er udviklingen **STIGENDE**.

Figur 1 Trusselsudviklingen i den periode, DKCERT har udarbejdet trusselsvurderinger.

DKCERT gik i 2023 bort fra begrebet insidertruslen, se *Trusselsaktørers udnyttelse af den menneskelige sårbarhed* på side 10.11.



Trusselsaktørers udnyttelse af den menneskelige sårbarhed

Trusselsaktører arbejder dagligt på at fremprovokere og udnytte menneskelige bevidste og ubevidste fejl, fx ved social engineering som phishing eller spearphishing eller ved udnyttelse af andre kilder som forskningssamarbejder, optagelse af patenter, tyveri mv.

Menneskelige fejl kan også skyldes fejlkonfigurationer eller være fx datalæk mv, som kan have baggrund i manglende kompetencer, uagtsomhed eller bevidste handlinger udført af hhv. ubevidste, uagtsomme eller uvederhæftige/ondsindede medarbejdere hos organisationen selv eller hos leverandører eller samarbejdspartnere.

DKCERT betragter ikke ubevidste, uagtsomme og uvederhæftige/ondsindede medarbejdere som trusler på linje med de øvrige, men som en sårbarhed eller angrebsvektor, som kan udnyttes af en trussel. Men det er naturligvis nødvendigt, at institutionerne er bevidste om og har fokus på dette i både deres tekniske og organisatoriske cyber- og informationssikkerhedsarbejde.[4]

Det kan fx ske ved at stille spørgsmål om, hvordan en trusselsaktør inden for cyberspionage kan mobilisere eller rekruttere en medarbejder til ondsindede handlinger og give aktøren adgang til fortrolig forskningsviden. Hvilke greb kan en cyberkriminel eller spionageaktør anvende for at få en uagtsom medarbejder til at give adgang til infrastrukturen? Hvordan kan en aktivist bruge ubevidste medarbejdere til at sprede aktivistiske budskaber? Hvilken tendenser ses ift. desinformation, som påvirker vores medarbejdere og studerende? (Se vurderingen af mis- og desinformation i afsnit 2.5).

Uvederhæftige/ondsindede medarbejdere vil oftest findes i forbindelse med cyberspionage, hvor de pågældende for personlig vindings skyld, af overbevisning eller med andre motiver hjælper en udefrakommende trusselsaktør til at opnå sit mål, mens ubevidste og uagtsomme medarbejdere vil typisk kunne anvendes af trusselsaktører fra alle kategorier til at angribe organisationen.

Medarbejderne og de studerende er således mere en angrebsvektor, end de er en egentlig trusselkategori. Men når trusselsniveauet er så højt som i dag, vil den generelle sandsynlighed for trusselsaktørers misbrug af medarbejderne også være meget høj.

[4] PET har i januar 2024 igangsat en informationskampagne for at sætte fokus på beskyttelse af dansk forskning, hvor medarbejderaspektet spiller en central rolle. Se i øvrigt afsnit 2.5.1.

De tre karaktertyper og de menneskelige fejl

DKCERT opererer med tre karaktertyper, som både kan være ansatte, studerende eller gæsteforelæsere m.fl.

> Den ubevidste

Er en person, som på grund af fx uklare/manglende sikkerhedspolitikker eller manglende uddannelse ubevidst bryder organisationens sikkerhedspolitikker.

> Den uagtsomme

Er en person, der bevidst bryder reglerne, selv om han eller hun har kendskab til dem. Årsagen kan være, at sikkerhedsreglerne opleves at umuliggøre udførelsen af arbejdet. Det kan også være skødesløshed som følge af, at reglerne opleves at gøre arbejdet mindre effektivt. Den uagtsomme bryder ikke nødvendigvis reglerne af ond mening.

Handlinger fra de uagtsomme og ubevidste kan være skadelige – ikke mindst fordi disse medarbejdertyper sjældent vil være opmærksomme på at anmelde sikkerhedsbrud i organisationen. Menneskelige fejl kan aldrig undgås, men sikkerhedspolitikker, retningslinjer, løbende uddannelse og vedligeholdelse af en sikkerhedskultur er metoder til nedbringelse af menneskelige fejl. De ubevidste og de uagtsomme er ubetinget årsag til de fleste sikkerhedsbrud.

> Den uvederhæftige/ondsindede

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 eller afsløres med funktionsadskillelse, bruger/rettighedsstyring og logs.

2. Trusselsvurdering 2024

2.3. HVAD ER TRUSLER, OG HVAD ER RISICI?

Standarder og regulering tilsiger en risikobaseret tilgang til arbejdet med cyber- og informationssikkerhed. Det stiller krav om, at hver ansvarlig enhed udarbejder konkrete risikovurderinger for deres aktiviteter. Nærværende trusselsvurdering er ikke en risikovurdering, men et input til institutionernes risikoarbejde.

Hvad er en cybertrussel?
Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester.[5]

Den tilsvarende tjeneste i USA, Cyber Security and Infrastructre Security Agency (CISA) taler om, at avancerede cyberaktører og nationalstater udnytter sårbarheder til at stjæle information og penge og udvikler kapaciteter til at forstyrre, ødelægge eller true leveringen af væsentlige tjenester.[6]

CISA definerer cybertrusler således (i DKCERTs oversættelse):
'En cybertrussel er et forsøg på at beskadige eller forstyrre et computernetværk eller system. Cybertrusler kan blive en realitet, hvis der er sårbarheder i et netværk, hardware eller software, som gør det muligt for en angriber at reducere et systems informationssikkerhed. De fleste cybersikkerhedsvejledninger omhandler adgangskontrol, konfigurationer og ansvarlighed, men virksomheder kan ikke vurdere risikoen eller vide, hvor de skal investere i sikkerhed, før de kender trusselsbilledet, som deres organisation står over for.'[7]

Man kan med andre ord ikke udarbejde de påkrævede risikovurderinger for forretningsprocesser og aktiver, hvis man ikke kender trusselslandskabet.

Hvordan kan man anvende denne – og andre - trusselsvurderinger i sit arbejde med at udarbejde risikovurderinger?
DKCERT gennemgik i Trendrapport 2021 processen for risikohåndtering, og hvordan trusselsvurderinger indgår i dette arbejde.[8]

En risikovurdering bygger på kendskabet til egne forretningsprocesser og til de systemer og andre aktiver, organisationen anvender til at gennemføre processerne. Det fører frem til, at man kan estimere de konsekvenser, et brud på fortrolighed, dataintegritet og tilgængelighed, fx et cyberangreb eller en anden informationssikkerhedshændelse, vil kunne medføre for organisationen i form af økonomiske tab, begrænsning af muligheden for at kunne udføre sine forretningsprocesser, tab af omdømme, bøde- eller erstatningskrav osv.

Heroverfor stiller man sandsynligheden for, at en sådan hændelse vil kunne indtræffe. Estimering af sandsynligheden bygger dels på (egne og andres) erfaringer med tidligere hændelser, dels på en analyse af, hvilke sårbarheder, organisationens processer og aktiver indeholder, samt endelig på en vurdering af hvilke eksterne og interne trusler, der vil kunne udnytte disse sårbarheder og føre til en sikkerhedshændelse.

Ved at stille de mulige trusler over for de identificerede sårbarheder kan man få et udtryk for sandsynligheden for sikkerhedsbrud. Multiplicerer man derefter dette udtryk for sandsynligheden med den estimerede konsekvens, får man et udtryk for den risiko, man står over for. Det kan fx være udtryk på en pointskala eller i kroner og ører, alt efter hvilken risikovurderingsmetode, man har valgt at anvende.

5 https://www.fmn.dk/da/arbejdsomraader/cybersikkerhed/om-cybersikkerhed/
6 https://www.cisa.gov/topics/cyber-threats-and-advisories
7 CISA: Understanding the Threat Landscape (https://www.cisa.gov/sites/default/files/c3vp/smb/Understanding_the_Threat_Landscape.pdf)
8 DKCERT Trendrapport 2021, s. 17. (https://cert.dk/sites/default/files/uploads/PDF/DKCERT_Trendrapport_2021_END.pdf)

2. Trusselsvurdering 2024

2.4. SITUATIONSBILLEDET FOR UDDANNELSES- OG FORSKNINGSSEKTOREN

Antallet af cyber- og informationssikkerhedshændelser i uddannelses- og forskningssektoren på verdensplan ser ud til fortsat at stige betydeligt.

DKCERT citerede i Trendrapport 2023 den tyske cyber- og informationssikkerhedsanalytiker Bert Kondruss, der havde optalt 66 medieomtaler af diverse sikkerhedshændelser på universiteter verden over i 2022 mod 32 i 2022.[9] En sammentælling af hans oplistning af hændelsesomtaler i 2023[10] viser 145 – men tallet er ikke en-til-en et udtryk for endnu en fordobling, og det er næppe heller helt dækkende.

Således er der i 2022 ikke rapporteret danske universitetshændelser, og i 2023 er der kun én på hans liste, nemlig hændelsen på Aalborg Universitet, der blev rapporteret 9. januar 2023. Både DTU-hændelsen i august 2022 og angrebene fra gruppen Vice Society mod Professionshøjskolerne Absalon i januar og VIA i april 2023 mangler, mens i det mindste nogle af de tilsvarende angreb fra samme gruppe mod bl.a. tyske professionshøjskoler er på listen.

106 af hændelserne på Bert Kondruss' liste blev rapporteret i første halvår 2023 og heraf var fx seks hændelser den 4. april samtidige DoS-angreb mod seks forskellige israelske universiteters websider, mens 42 hændelser (41 i USA og en i UK), rapporteret 31. maj, var udnyttelse af MoveIT Transfer-sårbarheden.[11]

Fratrækker man disse multiplicerede hændelser, viser tallene alligevel en væsentlig stigning, en tendens, der også bekræftes af andre undersøgelser.

Således skriver Orange Cyberdefense i deres '*Security Navigator 2024*', der er publiceret 30. november 2023 og bygger på data fra 1. oktober 2022 til 30. september 2023, at 'cyberafpresning' (økonomisk cyberkriminalitet) mod uddannelsessektoren (alle niveauer bredt) er steget med 115% fra 2022 til 2023, således at sektoren nu er den fjerdemest angrebne sektor mod tidligere en ottendeplads.[12]

Blandt hovedkonklusionerne i '*Security Navigator 2024*' er desuden, at Orange Cyberdefense ser:

- Et dynamisk økosystem for cyberkriminalitet, der udvider sine operationsmetoder ved direkte at rette dem mod virksomhedens personale for at kunne trænge ind i systemerne ad den vej.
- En stigning i cyberangreb mod mobile enheder, hvor vores personlige og forretningsmæssige data er stadig mere koncentreret.
- Fortsat målretning mod videnskabelig og teknisk ophavsret, den finansielle sektor, og især industri- og fremstillingsinfrastruktur.
- En eksplosion i cyberhacktivisme gennem de seneste to år for at støtte politiske eller sociale krav.

9 https://cert.dk/sites/default/files/uploads/PDF/DKCERT_Trendrapport_2023_END.pdf, s. 10.
10 https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html
11 Se fx: https://cert.dk/da/news/2023-07-03/MOVEit-angreb-ramt-over-130 og https://cert.dk/da/news/2023-06-26/Udlover-dusoer-paa-10-mio-dollar
12 https://www4.orangecyberdefense.com/security-navigator-2024, s. 63 og s. 86

2. Trusselsvurdering 2024

Flere af rapportens data er citeret nedenfor under gennemgangen af truslen fra cyberaktivisme.

ENISA, European Union Agency for Cybersecurity har 19. oktober 2023 udgivet 11. udgave af sin årlige rapport *'Threat Landscape'*.[13] Rapporten bygger på data fra andet halvår 2022 og første halvår 2023. Overordnet har ENISA i denne periode set en betydelig stigning i både bredden og mængden af cyberangreb og deres konsekvenser. Krigen mod Ukranie vedblev at præge trusselslandskabet, og 'hacktivisme' eller cyberaktivisme voksede med nye grupper, der dukkede op. Ransomwarehændelser toppede i første halvår 2023 (sidste del af undersøgelsesperioden) og viser ingen tegn på at bremse ned.

[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

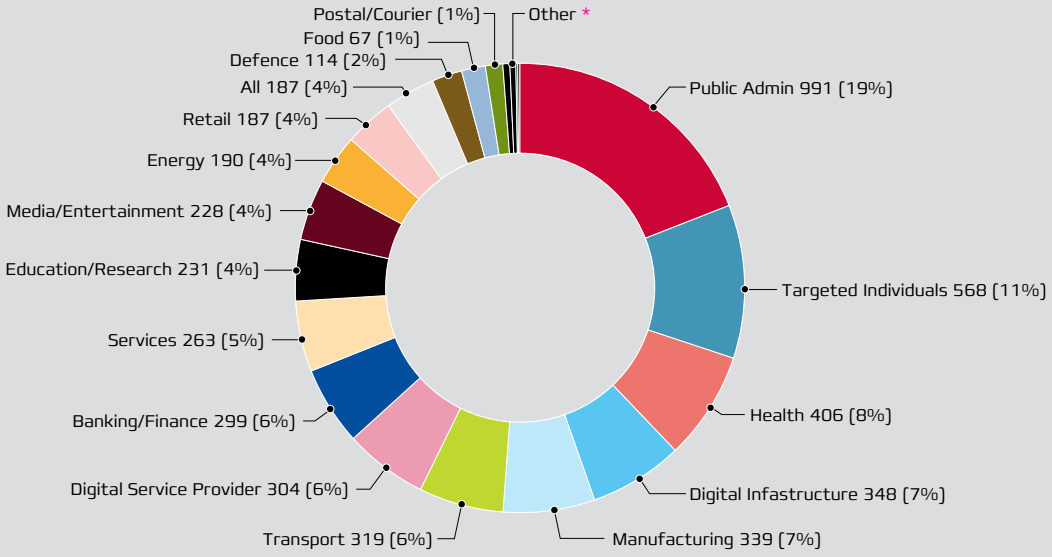
Rapporten udpeger og analyserer de primære trusler:

- ransomware
- malware
- social engineering
- trusler mod data i form af datalæk, datatab og manipulation, fx 'poisining' mod AI/ML-data
- trusler mod tilgængeligheden i form af dels
  - overbelastningsangreb, dels
  - 'internet-trusler'
- manipulation af informationer og påvirkning samt
- supply chain attacks (leverandørangreb)

Det fremgår, at uddannelses- og forskningssektoren er den 10. mest udsatte sektor for cyberangreb, men med flere rapporterede angreb end fx energisektoren eller forsvarssektoren og kun lidt færre end finanssektoren. Offentlig administration er den mest udsatte sektor, fulgt af målrettede angreb mod enkeltpersoner ('civilsamfundet') og af sundhedssektoren.

Figur 2 ENISA Threat Landscape 2022 - 2023

Targeted sectors per number of incidents (Juli 2022 - juni 2023).
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, s. 13



* Chemicals, Political, parties, Postal/Courier, Space, Unknown, Waste Management, Water

2. Trusselsvurdering 2024

2.5. CYBERTRUSLEN MOD DANSK FORSKNING OG VIDEREGÅENDE UDDANNELSE - UDDYBNING

2.5.1. Cyberspionage

Dansk forskning er i verdensklasse, og derfor er det attraktivt at få fat i forskningsresultater inden for en lang række forskningsområder. Det gælder særligt inden for kvanteteknologi, energiteknologi, bioteknologi, rumteknologi, robotteknologi, forsvarsindustrielle produkter og produkter omfattet af eksportkontrol.

Truslen fra cyberspionage gennemgås særligt i PETs rapport '*Vurdering af Spionagetruslen mod Danmark, Færøerne og Grønland*', udgivet 2. maj 2023.[14]

Rapporten vurderer, at fremmede efterretningstjenester bl.a. forsøger at opbygge kontakter til visse studerende, forskere og virksomheder, der vil kunne udlevere produkter og konkret viden om den ønskede teknologi og viden.

Om Rusland konkluderes det, at de russiske efterretningstjenester - udenrigsefterretningstjenesten, SVR, den militære efterretningstjeneste, GRU, og indenrigsefterretningstjenesten, FSB, der alle er involveret i efterretningstjeneste uden for Rusland - til stadighed forsøger at indhente oplysninger om dansk teknologi og forskning på områder, hvor danske virksomheder og forskningsinstitutioner er førende.

Det gælder bl.a. oplysninger om teknologisk specialiserede produkter og komponenter, som Rusland ikke selv er i stand til at fremstille. Det gælder også forskning i grønne teknologier og vedvarende energi. Rusland har samtidig behov for udenlandsk teknologi for at opretholde og udvikle landets militære kapacitet.

Kina ønsker at øge sin politiske, økonomiske og militære indflydelse i verden og at blive teknologisk selvforsynende og førende. PET vurderer, at den kinesiske stat er villig til at gå meget langt for at forfølge sine strategiske interesser på det videnskabelige og teknologiske område, og at der er en risiko for ulovlig eller uønsket kinesisk overførsel af viden og teknologi på især de områder, som Kina prioriterer strategisk.

Det gælder bl.a. kvanteforskning, kunstig intelligens, robotteknologi, bio- og medicoteknologi,

Figur 3
Med et opslag på LinkedIn igangsatte PET i januar 2024 en kampagne for at skabe debat om beskyttelse af dansk forskning. Kampagnen affødte dog kritik og protester fra bl.a. 182 medarbejdere på Niels Bohr Instituttet:
https://uniavisen.dk/havner-dit-arbejde-i-teheran-182-ku-forskere-kalder-ny-pet-kampagne-racistisk/
https://videnskab.dk/kultur-samfund/pet-advarer-forskere-mod-spioner-i-ironisk-kampagne/

[14] https://pet.dk/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vsd_2023_dk_web.pdf

2. Trusselsvurdering 2024

maritim teknologi, rumteknologi samt grøn teknologi. Ulovlig eller uønsket kinesisk vidensoverførsel kan efter PET's vurdering bl.a. ske i forbindelse med forskellige former for kinesisk forskningssamarbejde med danske forskningsinstitutioner, herunder ph.d.- og talentprogrammer samt statslige kinesiske stipendiater og ved virksomhedssamarbejder.

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.

DKCERT anbefaler, at institutionerne følger anbefalingerne fra Uddannelses- og Forskningsministeriets Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde (URIS) fra maj 2022[15] og i publikationen '*Er jeres forskning i fare?*', udgivet af PET, Uddannelses- og Forskningsstyrelsen og Erhvervsstyrelsen i august 2023.[16]

2.5.2. Cyberkriminalitet

Cyberangreb, der er motiveret af økonomisk vinding, forekommer dagligt og rammer hele samfundet. Angrebene udføres både af enkelte småsvindlere, af organiserede kriminelle grupper og af statsstøttede aktører. Både Ruslands krig mod Ukraine og krigen mellem Hamas og Israel har medført en yderligere stigning i det i forvejen meget høje antal angreb, da en af motivationsfaktorerne for cyberkriminalitet kan være finansiering af krigsførelsen.

Bl.a. de tidligere nævnte rapporter Orange Cyberdefense 'Security Navigator 2024'[17] og ENISA Threat Landscape 2023[18] dokumenterer et stadig stigende omfang af cyberkriminelle angreb. Også World Economic Forums 'The Global Risks Report 2024' fremhæver, hvad de kalder 'cyber insecurity' – herunder i høj grad cyberkriminalitet, blandt de væsentlige trusler mod verdensøkonomien generelt.

Det generelle situationsbillede for uddannelses- og forskningssektoren (jvf. afsnit 2.4) viser, at der løbende er en stadig voksende mængde af cyberkriminelle angreb mod sektoren.

Dette gør, at forudsætningerne for cyberkriminalitet i meget høj grad er til stede, hvorfor truslen mod uddannelses- og forskningssektoren vurderes at være er MEGET HØJ.

2.5.3. Cyberaktivisme

Cyberaktivismens karakter gør, at en pludseligt opstået opmærksomhed mod sektoren eller enkeltforskere kan medføre en eller flere former for aktivistiske angreb fra cyberaktivister, der ønsker at få opmærksomhed for deres sag. Anonymous Sudans bebudede DoS-angreb[19] 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, blot det skaber opmærksomhed.

Truslen fra cyberaktivisme har frem mod 2022 været LAV, men krigen mellem Rusland og Ukraine såvel som krigen mellem Israel og Hamas med afledte hændelser har skabt ændringer, som hæver niveauet, ligesom cyberaktivister har oplevet, at deres aktioner medfører den omtale, de søger, og givetvist også har inspireret andre.

Forud for konflikten var truslen fra cyberaktivister mod Danmark lav, men både pro-russiske og pro-ukrainske hackere blev hurtigt meget aktive efter krigens udbrud. De pro-russiske cyberaktivister udgør nu den primære trussel mod danske virksomheder og myndigheder, som løbende er blevet ramt af DoS-angreb.

Angriberne rammer oftest symbolske mål i lande, der støtter Ukraine i krigen mod Rusland. De pro-russiske cyberaktivister har siden konfliktens start udviklet deres metoder og forøget deres kapacitet til at udføre DoS-angreb, i takt med at flere har støttet op om deres sag.

[15] https://ufm.dk/aktuelt/pressemeddelelser/2022/ny-rapport-behov-for-skaerpet-tilgang-til-forskningssamarbejde-med-blandt-andre-kina og https://ufm.dk/publikationer/2023/statusrapport-for-implementering-af-uris

[16] https://ufm.dk/publikationer/2023/er-jeres-forskning-i-fare

[17] Orange Cyberdefense: Security Navigator 2024, 30. november 2023

[18] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[19] Overbelastningsangreb, Denial-of-Service eller DoS, kan udføres på en række forskellige måder. Ofte sker det i form af Distributed Denial of Service (DDoS), hvor angribene benytter sig af et såkaldt botnet. Det består af en lang række inficerede computere som styres af en command-and-control-server (C2), som simultant sender forespørgsler til angrebsmålet (en webadresse eller et IP-nummer), som dermed overbelastes og enten helt stopper med at svare eller svarer meget langsomt på reelle opslag.
Se også https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks

2. Trusselsvurdering 2024

Alligevel har den type DoS-angreb, som aktivisterne udfører, stadig ikke store konsekvenser for det enkelte offer, men de kan bidrage til at skabe frygt og usikkerhed og dermed have en destabiliserende effekt. Mediernes fokus på disse 'hackerangreb', som de oftest kaldes, giver netop cyberaktivisterne den opmærksomhed, de ønsker at opnå.

Fremtiden kan bringe nye former for cyberaktivisme med sig

Cyberaktivister benytter sig også af andre typer cyberangreb ved siden af de mange DoS-angreb. De lækker eksempelvis stjålne oplysninger eller laver såkaldte 'defacement-angreb', hvor det originale indhold på en hjemmeside erstattes med politiske budskaber fra aktivisterne.

Sådanne angreb har særligt fundet sted i Ukraine og Rusland ifølge FE, mens DKCERT ikke har set defacement-angreb mod uddannelses- og forskningssektoren i større omfang siden tegningekrisen i 2005-06 og 2008. Og især efter 2017-18 er defacement-angreb i Danmark generelt blevet sjældne[20] – muligvis fordi vi er blevet bedre til at beskytte integriteten af hjemmesiderne.

Nogle hackere eller hacktivister har ladet deres DoS-angreb ledsage af et krav om løsepenge for at få angrebet til at stoppe. Udbyttet af et sådant kriminelt element i et aktivistisk cyberangreb begrænses dog af, at mange ofre vil kunne afværge DoS-angrebet ved relativt enkle foranstaltninger. DKCERT har tidligere set eksempler på en tilsvarende fremgangsmåde fra rent kriminelle grupperinger uden et politisk eller aktivistisk formål. Dermed er det ikke cyberaktivisme, men metoden er den samme.

Derudover er der tegn på, at cyberaktivister i fremtiden vil forsøge at udføre mere alvorlige angreb for at gøre opmærksom på deres sag eller for direkte at påvirke den. Aktivister har bl.a. påstået, at de har angrebet operative systemer i eksempelvis energi- eller telesektorer i Ukraine og Rusland. Angrebene påvirkede, ifølge aktivisterne selv, den fysiske verden i form af strømafbrydelse, signalafvigelser og lignende. Uanset om de aktivistiske destruktive cyberangreb har fundet sted eller ej, er alene omtalen af den slags angreb en ny udvikling.[21]

Orange Cyberdefense skriver i den ovenfor omtalte Security Navigator 2024, at de nordiske lande – navnlig Sverige og Danmark - er et særligt mål for cyberaktivisme, idet Sverige samlet set er det land, der har været udsat for tredje flest angreb, nemlig 338, mens Danmark kommer ind på en 11. plads med 127 angreb, registreret af Orange Cyberdefense fra fjerde kvartal 2022 til tredje kvartal 2023.[22]

[20] https://cert.dk/da/news/2018-04-09/defacements
[21] FE: Udsyn 2023: https://www.fe-ddis.dk/globalassets/fe/dokumenter/2023/udsyn/-udsyn-2023-.pdf, s. 35
[22] Orange Cyberdefense: Security Navigator 2024, 30. november 2023, s. 79

2. Trusselsvurdering 2024

Både DKCERT og de svenske kolleger i Sunet CERT har konstateret, at en væsentlig del af disse cyberaktivistiske angreb har ramt den akademiske sektor. Og vi har, ligesom Orange Cyberdefense, set, at angrebene navnlig kommer fra to grupper, nemlig 'Anonymous Sudan' - som især har angrebet Sverige, men som i foråret 2023 også ramte mål i Danmark, bl.a. danske universiteter - mens de senere angrebsbølger mod Danmark og mod en række andre lande, der aktivt støtter Ukraine, er kommet fra 'NoName057(16)'[23]. Det gælder især Polen, Litauen og Tyskland, der er henholdsvis nr. 2, 4 og 5 på listen over mållande.[24] Ukraine topper listen, men 80% af 639 dokumenterede angreb mod dem kom fra en gruppe, kendt som 'CyberArmyRussia'.

Cyberaktivisme er i det hele taget et europæisk fænomen, først og fremmest drevet af grupper, der enten direkte støttede af den russiske stat, eller som sympatiserer med Rusland. 3.404 ud af i alt 4.016 registrerede angreb på verdensplan i 12-måneders perioden fra 1. oktober 2022 til 30. september 2023 har ramt Europa og heraf som nævnt 127 angreb mod danske mål.[25]

Der har således i 2023 været en række cyberaktivistiske angreb – især i form af DoS-angreb mod danske mål, herunder i uddannelses- og forskningsektoren.

Forudsætningerne for cyberaktivisme (i form af parametrene kapacitet, hensigt, planlægning og iværksættelse) er med andre ord i meget høj grad til stede, hvorfor vurderingen af trusselsniveauet for cyberaktivisme mod uddannelses- og forskningssektoren øges fra LAV i 2022 og HØJ i 2023 til nu MEGET HØJ.

Imidlertid er de tekniske konsekvenser af disse angreb overskuelige, hvorfor en *risikovurdering* for de fleste ikke vil vise en lige så høj score som for cyberspionage og cyberkriminalitet, der har samme trusselsniveau.

2.5.4. Destruktive cyberangreb

Destruktive cyberangreb kommer fra statslige aktører med det formål ved at ødelægge fx kritisk eller samfundsvigtig infrastruktur. CFCS definerer destruktive cyberangreb som handlinger, 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,

Selv om krigen i Ukraine har betydet en drastisk forværring af forholdet mellem Vesten og Rusland, vurderer FE i rapporten 'Udsyn 2023', at det er mindre sandsynligt, at Rusland aktuelt har til hensigt at ramme Danmark med destruktive cyberangreb.[26]

Når Rusland skaffer sig adgang til it-systemer hos udenlandske myndigheder og virksomheder, er det dog ikke altid alene for at stjæle hemmeligheder. Det er sandsynligt, at statsstøttede hackere, særligt fra Rusland, forbereder sig på at kunne udføre destruktive cyberangreb mod Danmark og dansk kritisk infrastruktur.

Det betyder, at hvis Ruslands hensigter ændrer sig, vil truslen fra destruktive cyberangreb mod mål i Danmarks kritiske infrastruktur hurtigt kunne stige. Destruktive cyberangreb har det til fælles, at de ødelægger noget – enten datasystemer eller fysiske enheder som maskiner og apparater i eksempelvis produktionsvirksomheder. Selv om sandsynligheden for et destruktivt angreb mod Danmark fortsat er lav, er de potentielle konsekvenser store.

Et koordineret angreb i to bølger i maj 2023 med udnyttelse af en nyopdaget sårbarhed i Zyxel-firewalls kan have været en forberedelse af et destruktivt cyberangreb mod 22 mindre forsyningsselskaber. Hvis angrebet havde været succesfuldt, kunne det have ramt fjernvarme- og elforsyning til omkring 100.000 danske husstande. Der er tegn på, at en statsstøttet aktør kan stå bag i det mindste et af delangrebene.

Om målet var at lægge kritisk forsyningsinfrastruktur ned umiddelbart med et destruktivt angreb, eller om der var tale om cyberspionage med henblik på et muligt angreb på et senere tidspunkt, kan ikke afgøres.[27]

[23] https://cert.dk/da/news/2023-11-05/hackergruppe-NoName057%2816%29-slaar-til-igen
[24] Orange Cyberdefense: Security Navigator 2024, s. 78 og https://cert.dk/da/news/2023-01-17/DDoS-er-NATO-lande
[25] Orange Cyberdefense: Security Navigator 2024 s. 78.
[26] https://www.fe-ddis.dk/globalassets/fe/dokumenter/2023/udsyn/-udsyn-2023-.pdf, s. 36.
[27] https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-Angrebet-mod-dansk-kritisk-infrastruktur-TLPCLEAR.pdf

2. Trusselsvurdering 2024

Cyberspionage mod kritisk infrastruktur, især energi og forsyning, kan være en del af forberedelsen af destruktive cyberangreb. Det er mindre sandsynligt, at disse vil være rettet direkte mod uddannelses- og forskningssektoren, da hovedinteressen for statsstøttede operatører vil være at komme i besiddelse af forskningsresultater, fremfor at ødelægge eller forstyrre forskningen.

Imidlertid kan de afledte effekter af fx svigtende elforsyning eller dataforbindelser have betydelige konsekvenser for sektoren, så udviklingen på området bør følges nøje og give anledning til beredskabsplanlægning og forberedelse af modforanstaltninger, selvom truslen på kort sigt er LAV.

Det forhold, at et fjendtligtsindet lands involvering i et decideret destruktivt cyberangreb mod Danmark og danske interesser, kan blive betragtet som et angreb (med hybride virkemidler) på et NATO-land, som vil kunne udløse en artikel 5-reaktion fra alliancen, kan i sig selv afholde aktører fra destruktive angreb.[28/29]

FE udgav 19. februar 2024 en analyse, der beskriver Ruslands genopbygning af sin militære styrke og vurderer, at Rusland på kortere og mellemlangt sigt vil optræde mere selvhævdende over for NATO.[30] Herunder er forventningen, at Rusland vil anvende sine militære kapaciteter op til grænsen for, hvad de forventer, vil kunne udløse NATO-pagtens artikel 5 ('Musketereden').

Analysen nævner angreb på fysisk infrastruktur i internationalt farvand (fx søkabler) som en mulighed, men ikke cybervåben og cyberangreb. Det er imidlertid velkendt, at Ruslands militære og politiske ledelse betragter disse midler som en ligeværdig del af værkstøjskassen (hybrid krigsførelse)[31], hvorfor det efter DKCERTs vurdering ikke kan udelukkes, at man i det skærpede scenario, som analysen beskriver, vil forsøge at anvende destruktive cyberangreb af mindre omfang, i sin afprøvning af NATOs solidaritet og tolerancetærskel.

Forudsætningerne for destruktive cyberangreb vurderes kun i lav grad at være til stede, hvorfor truslen fra destruktive cyberangreb direkte mod uddannelses- og forskningssektoren må anses for at være LAV.

Truslen om afledte effekter af destruktive cyberangreb mod kritisk infrastruktur, herunder energiinfrastruktur samt tele- og it-infrastruktur vurderes inden for de næste to til fem år at være MIDDEL.

28 https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en
29 https://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/2022/-dansk-sikkerhed-og-forsvar-mod-2035-densikkerhedspolitiske-analyserapport-.pdf (side 39)
30 https://www.fe-ddis.dk/da/produkter/situations--og-trusselsvurderinger2/trusselsvurderinger/analyse---rus-landgenopbygger-sin-militare-styrke-og-vil-agere--mere-selvhavdende-overfor-nato/
31 https://www.diis.dk/publikationer/danmark-optimere-handlemuligheder-paa-hybridkrigens-sloerede-slagmark

2. Trusselsvurdering 2024

2.5.5. Cyberterror

CFCS definerer cyberterror som alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som ved konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur. På den måde har cyberterror lighed med fysisk terror, men CFCS har ikke set udførte cyberterrorangreb, der har svaret til konventionel terror.[32] Center for Cybersikkerhed vurderer på den baggrund, at det er usandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberterror inden for de næste to år.

Forudsætningerne for cyberterror, særligt rettet mod den danske uddannelses- og forskningsinstitutioner, er ikke til stede, hvorfor det fortsat er DKCERTs vurdering, at truslen fra cyberterror mod uddannelses- og forskningssektoren er INGEN.

2.5.6. Påvirkning, mis-/desinformation

DKCERT behandlede denne trusselskategori i trusselsvurderingen for 2022 og tager den op igen i år.[33]

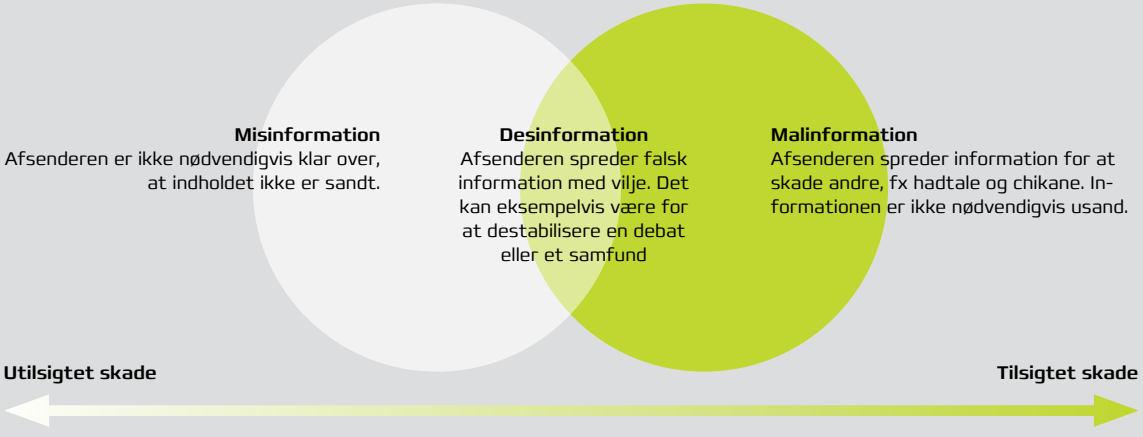
Påvirkningskampagner kan bl.a. medvirke til undergravning af tiltro til forskningsbaserede fakta og skubbe yderligere til en samfundsudvikling, hvor følelser og holdninger synes at gå forud for fakta og viden.

World Economic Forums Global Risks Report 2024[34] fremhæver truslen fra mis- og desinformation, bl.a. udført ved hjælp af kunstig intelligens, som den mest alvorlige trussel på et tidspunkt, hvor tre milliarder vælgere på verdensplan forventes at gå til stemmeurnerne over de næste to år. Mis- og desinformation kan bidrage til at undergrave tiltroen til politiske institutioner og til den generelle polarisering i samfundet. Vurderingen af truslen er i dette års undersøgelse fra World Economic Forum steget fra en 15. plads til nu at være nr. 1 som den mest alvorlige trussel på kort sigt (over to år), mens den på 10 års sigt indtager en 5. plads, overgået af ekstremt vejr, kritiske ændringer af jordens systemer, tab af biodiversitet og kollaps af økosystemer samt mangel på naturressourcer.

[32] https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2022b.pdf
[33] DKCERT Trendrapport 2022 2.2.7. s. 16
[34] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Figur 4 Misinformation, desinformation og malinformation

I dag er 'begrebet fake news smidt i skraldespanden' ifølge www.TjekDet.dk. I stedet taler man om og skelner mellem misinformation, desinformation og malinformation, afhængigt af hensigten med at dele falske informationer.



2. Trusselsvurdering 2024

ENISA Threath Landscape[35] har fulgt mis- og desinformation siden 2021 og bruger nu udtrykket 'manipulation af informationer og påvirkning' for at beskrive truslerne lidt bredere.

Bl.a. fremhæves også her (mis)brug af kunstig intelligens, ligesom rapporten gennemgår forskellige taktikker og teknikker i manipulation af information. Bl.a. finder man, at 48% af de anvendte teknikker udnytter 'breaking news-hændelser' eller igangværende kriser, hvor uklare facts og ukomplet information øger spekulationer, rygter og konspirationsteorier, som alle kan manipuleres. 36% udnytter eksisterende fortællinger og 8% verserende konspirationsteorier.

The Guardian offentliggjorde 12. februar 2024, at det franske agentur til imødegåelse af udenlandsk digital påvirkning af den offentlige mening, Virginum, har afsløret et Moskva-baseret onlinenetværk, der spreder propaganda og desinformation i Vesteuropa. Virginum vurderer, at netværket, som de kalder 'Portal Kombat', er en del af en ny bølge af russisk onlinemanipulation forud for valget til Europa-Parlamentet og andre afgørende afstemninger i 2024. Netværket, som Virginum har fulgt siden september 2023, omfatter mindst 193 websteder, der formidler pro-russisk propaganda. Desinformationen spredes gennem sociale medier og beskedapps, fx WhatsApp. [36]

Med en voksende mistillid til autoriteter - herunder til forskere og deres resultater - med udbredelsen af lukkede grupper på sociale medier som primære nyhedskilder for mange mennesker, med en voksende polarisering i samfundet samt med gennembruddet for kunstig intelligens-baserede værktøjer, der bl.a. gør tilgangen til at lave deep fake-billeder og -videoer lettere og langt mere udbredt, vurderer DKCERT, at forudsætningerne for mis- og desinformation mod uddannelses- og forskningssektoren i høj grad er til stede, ligesom der ses igangværende desinformationsaktivitet mod samfundet i øvrigt.

Påvirkningskampagner er en del af hybrid krigsførelse i det skærpede trusselsbillede (se destruktive cyberangreb ovenfor).

Truslen vurderes derfor til at være HØJ.

DKCERT anbefaler, at institutionerne forholder sig til Rådet for Digital Sikkerheds vejledning 'Sådan modstår vi falsk information. En vejledning til offentlige myndigheder og private virksomheder', fra februar 2020.[37] Endvidere henvises til TjekDet - national portal for bekæmpelse af fake news[38] og til Europa-Kommissionens strategi for bekæmpelse af desinformation på internettet.[39]

[35] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, s. 110
[36] https://www.theguardian.com/technology/2024/feb/12/french-security-experts-identify-moscow-baseddisinformation-network
[37] https://www.digitalsikkerhed.dk/wp-content/uploads/2021/03/Vejledning_Desinformation.pdf
[38] https://www.tjekdet.dk/
[39] https://digital-strategy.ec.europa.eu/da/policies/online-disinformation

Kunstig intelligens

2023 blev et gennembrudsår for udbredelsen af kunstig intelligens (artificial intelligence/AI) og den brede adgang til disse teknologier. Sikkerhedsmiljøet har i en del år anvendt teknologier som algoritmebaseret maskinlæring (ML) og mønstergenkendelse i forbindelse med bl.a. analyse af netværkstrafik og fx *intrusion detection/intrusion preventing systemer.*

Med den almindelige adgang til AI-chatbots, baseret på store sprogmodeller (Large laguage Models/LLM) som Open AI ChatGPT fra december 2022, Microsoft 365 Copilot fra februar 2023 og Google Gemini (tidligere Bard) fra marts 2023 er udbredelsen eksploderet. Således fik Open AI ChatGPT mere end en million brugere i løbet af få dage fra introduktionen. Siden er teknologien bl.a. blevet integreret i søgemaskiner, styresystemer til mobiltelefoner og meget mere.

Den almindelige adgang til meget effektive kunstig intelligens-værkstøj medfører både nye muligheder og nye trusler.[40]

Trusler mod kunstig intelligens
Kunstig intelligens og maskinlæring-teknologier anvendes bredt og i stadig stigende grad i forsknings- og uddannelsesmiljøerne. Det rejser et behov for at se på de trusler, der er rettet mod anvendelsen af disse teknologier.

Forskellige former for 'poisoning attacks', hvor data, der bruges til oplæring af algoritmerne, bliver forurenet med falske eller manipulerede data kan være ødelæggende for anvendelsen af teknologierne og for validiteten af de beslutninger og de udsagn den kunstige intelligens genererer.

Når de store sprogmodeller indsamler så store datamængder, som de har brug for til træning, stiller det store krav til den løbende kvalitetskontrol af både træningsdata og *output*.[41]

Også datalæk gennem anvendelsen af generativ kunstig intelligens og chatbots har der været flere eksempler på i 2023.

DKCERT anbefaler, at institutionerne opstiller regler for, hvilke af organisationens data, der må behandles i fx generelle chatbots, og at man overvejer muligheden for at anvende private chatbots til at imødegå denne trussel.

Trusler fra kunstig intelligens

ENISA Threat Landscape 2023 anfører fx, at *Social engineering-angreb* steg markant i 2023[42] med fremkomsten af AI og nye teknologier. Phishing er dog stadig den vigtigste angrebsvektor, men her anvendes teknologien også til udformning af endnu mere effektive angrebskampagner, herunder s*pear phishing*. Det er blevet væsentligt vanskeligere at genkende phishingsmails, når oversættelsen er foretaget af en chatbot.[43]

Deep fake i form af AI-genererede billeder og video samt stemmekloning anvendes allerede til svindelforsøg, og det må forventes, at denne trussel kun vil vokse i omfang på kort og mellemlangt sigt. AI-baseret stemmekloning udføres ud fra lydoptagelser på fx YouTube, TikTok eller andre sociale medier. Selv få sekunders lydprøve kan være nok til at skabe en nogenlunde troværdig falsk stemme.

Vi har allerede set metoden anvendt til at generere telefonopkald, hvor svindlere giver sig ud for at være fx et familiemedlem i vanskeligheder og med et akut behov for at blive hjulpet med penge. Langt mere effektivt end de tilsvarende spear phishing-kampagner, vi har set gennem adskillige år.

Også deep fake-genererede falske mødedeltagere i videokonferencer har været demonstreret.

'Security-by-obscurity', hvor man har satset på, at forskellige former for svagheder i systemer og organisatoriske sikkerhedsforanstaltninger kunne eksistere uden at blive udnyttet, er ikke længere en mulighed. En angriber kan umiddelbart kortlægge alle sårbarheder og mulige indgangsveje i et it-miljø med AI. Det gør det mere end nogensinde nødvendigt at indføre hurtig og effektiv patch mangement, grundig netværkssegmentering, MFA, always-on-VPN osv.

AI har ikke kun betydning i forbindelse med cyberkriminelle og cyberspioners manipulation. Også i forbindelse med påvirkningskampagner, mis- og desinformation udgør AI en væsentlig trussel. Falske historier underbygges med falske billeder, videoer og stemmeoptagelser.

World Economic Forum[44] har som nævnt ovenfor fremhævet denne trussel som den mest alvorlige i 2024 og 2025, hvor der afholdes afgørende valg i det meste af verden, og hvor krige og konflikter, inklusive propagandakrige, præger billedet. På 10-års sigt er mis- og desinformation nummer 5 på WEFs liste over globale trusler, rangeret efter alvorlighed. Nr. 6 på denne liste er den bredere kategori 'negative resultater af AI-teknologier'.

Center for Cybersikkerhed udgav 8. marts 2024 trusselsvurderingen *Hackere misbruger generativ AI*.[44a]

[40] Amerikanske National Institute of Standards and Technology (NIST) udgav i januar 2024 et paper, A Taxonomy and Terminology of Attacks and Mitigations, vedr. trusler fra og mod AI. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

[41] ENISA Threat Landscape 2023, s. 91

[42] ENISA Threat Landscape 2023, s. 4, s. 31, s. 74

[43] Orange Cyberdefense Security Navigator 2024, s. 167

[44] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[44a] https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/hackere-misbruger-generativ-ai/

2. Trusselsvurdering 2024

2.6. ANBEFALINGER TIL ORGANISATIONENS RISIKOVURDERINGER

Som baggrund for organisationens egen vurdering af trusselselementet i arbejdet med risikovurderinger og det videre arbejde med risikohåndtering, anbefaler DKCERT, at man orienterer sig i flere trusselsvurderinger udover denne.

Til DKCERTs trusselsvurdering har vi anvendt et udvalg af vurderinger, der er åbent tilgængelige på internettet, jf. nedenstående liste. De citeres i tekst og noter. Endvidere har der som baggrundsmateriale været anvendt et begrænset antal kilder, som ikke er offentliggjorte. Til baggrund for trusselsvurderingen tjener endvidere DKCERTs kendskab til hændelser i sektoren, se afsnit 3.1. Se endvidere afsnit. 5.1 Cybertrends 2024.

Danske efterretningsmæssige trusselsvurderinger

- CFCS: *Cybertruslen mod Danmark 2023*, 8. maj 2023[45]
- FE: *Udsyn. En efterretningsbaseret vurdering af de ydre vilkår for Danmarks sikkerhed og varetagelsen af danske interesser*, 15. dec. 2023[46]
- PET: *Vurdering af spionagetruslen mod Danmark, Færøerne og Grønland,* 2. maj 2023[47]
- FE: *Analyse - Rusland genopbygger sin militære styrke og vil agere mere selvhævdende over for NATO*, 19. februar 2024[48]
- Center for Terroranalyse, PET: *Vurdering af terrortruslen mod Danmark*, 1. marts 2023.[49] Vurderingen tager ikke stilling til truslen fra cyberterror, men henviser til CFCS: Cybertruslen mod Danmark.

CFCS udgiver endvidere en række deltrusselsvurderinger, i 2023 følgende:

- *Ransomware-truslen mod produktionsvirksomheder,* 6. december 2023[50]
- *Cybertruslen mod IoT-enheder*, 3. november 2023[51]
- *Cybertruslen mod Grønland*, 13. marts 2023[52]
- *Cybertruslen mod sundhedssektoren,* 17. februar 2023.[53]

Derudover er der anvendt en række opdaterede trusselsvurderinger af de kritiske infrastruktursektorer: *Cybertruslen mod danske havne og logistikvirksomheder; Cybertruslen mod dansk luftfart; Cybertruslen mod land- og lufttransporten; Cybertruslen mod jernbanesektoren; Cybertruslen mod telesektoren; Cybertruslen mod finanssektoren; Cybertruslen mod søfart og havne; Cybertruslen mod energisektoren.*[54]

CFCS har ikke udgivet en trusselsvurdering for uddannelses- og forskningssektoren siden *Cybertruslen mod dansk forskning og universiteter,* 3. september 2021.[55]

Andre (danske) myndigheder og aktørers trusselsvurderinger

DCIS-UFM udarbejdede i efteråret 2023 en trusselsvurdering, der ikke er offentliggjort, men inddraget som baggrundsmateriale.

SektorCERT (tidl. EnergiCERT) udgiver jævnligt en kortfattet trusselsvurdering, senest *Trusselsvurdering*, 15. januar 2024.[56A] Trusselsvurderingen skal læses sammen med den håndbog, det daværende EnergiCERT udgav i 2022.[56B]

Håndbogen forklarer de fem niveauer, som SektorCERT benytter i deres trusselsvurderinger, samt hvordan man som aktør skal forholde sig i de forskellige niveauer. Håndbogen oplister også SektorCERTs 25 anbefalinger, som det anbefales alle aktører indenfor kritisk infrastruktur at implementere.

45 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/
46 https://www.fe-ddis.dk/da/nyheder/2023/udsyn-2023/
47 FE: Udsyn. En efterretningsbaseret vurdering af de ydre vilkår for Danmarks sikkerhed og varetagelsen af danske interesser, 15. dec. 202352
48 https://www.fe-ddis.dk/da/produkter/situations--og-trusselsvurderinger2/trusselsvurderinger/analyse---rusland-genopbygger-sin-militare-styrke-og-vil-agere--mere-selvhavdende-overfor-nato/
49 https://pet.dk/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-terrortruslen-moddanmark/vurdering-af-terrortruslen-mod-danmark-2023.pdf
50 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/ransomware-truslen-mod-produktionsvirksomheder/
51 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/forskning-og-universiteter/
52 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/trusselsvurdering-cybertruslen-mod-gronland/
53 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/sundhed/
54 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/
55 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-iot-enheder/
56A https://sektorcert.dk/wp-content/uploads/2024/01/Trusselsvurdering-DK-20230115.pdf
56B https://sektorcert.dk/wp-content/uploads/2022/12/EnergiCERT-Haandbog-om-Trusselsniveauer-v1.0-1.pdf

2. Trusselsvurdering 2024

Den decentrale cybersikkerhedsenhed i Sundhedsdatastyrelsen giver årligt rapporten '*Trusselsbilledet i sundhedssektoren*'.

'*Trusselsbillederne udarbejdes på bekræftede informationer fra validerede kilder og samarbejdspartnere. Formålet er at give sundhedssektoren indblik i trusselstendenser, typer af trusler samt kritikalitet for hver kategori. Derudover skal trusselsbillederne kunne bruges til aktørernes eget risikobillede og ledelsesrapportering.*'[57]

Trusselsbilledet er ikke offentliggjort og kan derfor ikke citeres her. Det kan rekvireres af relevante aktører.

Overnationale og udenlandske myndigheders trusselsvurderinger

ENISA, European Union Agency for Cybersecurity:

> *Threat Landscape*, 11. udgave af årlig rapport, 19. oktober 2023.[57b]

ENISAs Threat Landscape (ETL) er igen i år en væsentlig kilde til DKCERTs trusselsvurdering.

> *ENISA Threat Landscape for DoS Attacks*, udgivet 6. december 2023.[57c]

ENISA har med en ny metode og et nyt klassifikationsskema systematisk analyseret 310 bekræftede DoS-angreb i perioden fra januar 2022 til august 2023. Rapporten omfatter ikke data specifikt fra uddannelses- og forskningsektoren, men bekræfter det generelle billede af stadig stigende omfang af DoS-angreb (cyberaktivisme). Den mest ramte sektor var den offentlige administration i mållandene. 46% af angrebene ramte denne sektor, og det estimeres, at 66% af alle angrebene var politisk motiverede eller havde et aktivistisk formål. 50% af hændelserne var relaterede til Ruslands angrebskrig mod Ukraine.

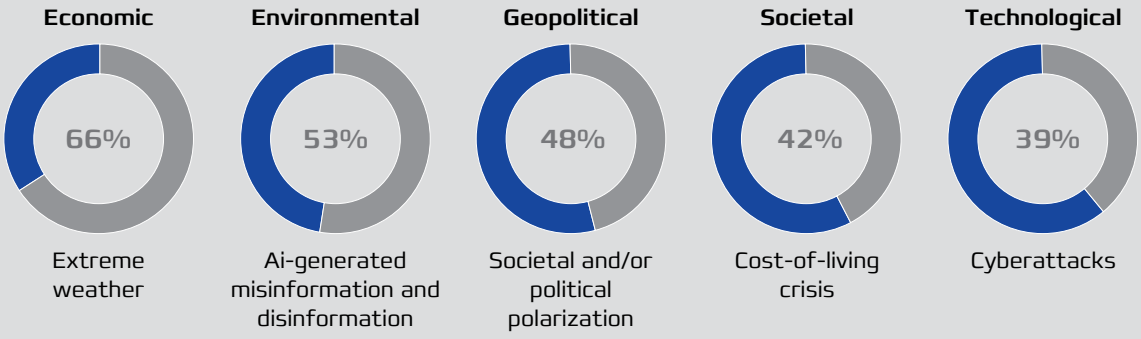
> World Economic Forum (WEF): *The Global Risks Report 2024*, 10. januar 2024.[58]

Rapporten er bygget op omkring en undersøgelse af, hvordan risiko opleves rundt omkring i verden. Mere end 11.000 offentlige og private ledere fra de fleste af verdens lande har svaret på, hvilke af 34 nærmere definerede trusler inden for ka-

[57] https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/ominformationssikkerhed/
[57b] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023] haendelser#_5d8f9579-14e6-4e97-9c0c-b9de45b33f44
[57c] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks
[58] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Figur 5 World Economic Forum Global Risks Perception Survey 2023-2024

Data til figuren kommer fra respondenternes svar på følgende spørgsmål:
'*Please select up to five risks that you believe are most likely to present a material crisis on a global scale*'



Kilde: World Economic Forum Global Risks, Perception Survey 2023-2024

2. Trusselsvurdering 2024

tegorierne økonomiske, miljømæssige, geopolitiske, samfundsmæssige og teknologiske risici, der vil kunne udløse en omfattende krise. Overordnet kommer kunstig intelligens-genereret misinformation og desinformation ind på en andenplads, mens cyberangreb opfattes som den femtestørste trussel.

Rapporten indeholder også en liste over, hvordan de 34 trusler rangeres i de enkelte lande. I Danmark ser respondenterne fordelingen, som det fremgår af figur 6. Danskerne opfatter altså cyberkriminalitet og 'cyberusikkerhed' som den tredjestørste trussel, mens angreb på kritisk infrastruktur fra kategorien geopolitiske trusler også kommer med på top-5.

'Cyberusikkerhed' dækker i undersøgelsens definition over 'Brug af cybervåben og -værktøjer til at udføre cyberkrigsførelse, cyberspionage og cyberkriminalitet for at få kontrol over en digital tilstedeværelse og/eller forårsage driftsforstyrrelser. Inkluderer: ransomware, datasvindel eller datatyveri'. Cyber Security and Infrastructure Security Agency

Figur 6 **Danske respondenters placering af truslerne ifølge World Economic Forum**

1	Economic downturn
2	Labour shortage
3	Cybercrime and cyber insecurity
4	Inflation
5	Attacks on critical infrastructure

Kilde: World Economic Forum Global Risks, Perception Survey 2023-2024

(CISA) er USAs pendant til Center for Cybersikkerhed og en del af U.S. Department of Homeland Security. Det er en kilde, vi ofte citerer i DKCERTs nyheder, ligesom et par af CISAs publikationer er nævnt i indledningen til denne trusselsvurdering.[59]

National Institute of Standards and Technology (NIST) under U.S. Department of Commerce udgiver bl.a. et Cybersecurity Framework, som er udkommet i version 2.0 26. februar 202460, og et Privacy Framework61. Disse standarder er gode supplementer til ISO/IEC 27000-serien mv. NIST er citeret ovenfor i temaboksen om kunstig intelligens.

Kommercielle rapporter

Verizon DBIR 2023[61a], Verizons Data Breach Investigations Report har tidligere været anvendt som en væsentlig kilde til Trusselvurderingen. Den fravælges i år, da den bygger på data fra 2022.

I betragtning af den hurtige udvikling på cyberområdet har vi stedet valgt Orange Cyberdefense Security Navigator 2024[62], hvis datagrundlag er fjerde kvartal 2022 og de første tre kvartaler af 2023. Rapporten er præsenteret ovenfor i afsnit 2.4. Situationsbilledet for uddannelses- og forskningssektoren.

[59] https://www.cisa.gov/topics/cyber-threats-and-advisories
[60] https://www.nist.gov/cyberframework
[61] https://www.nist.gov/privacy-framework
[61a] https://www.verizon.com/business/resources/reports/dbir/
[62] https://www4.orangecyberdefense.com/security-navigator-2024

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 tjenester, 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, TEKNISKE ANALYSER OG VIDENDELING

3.1.1 Sårbarhedsscanninger

De ca. 40 institutioner tilknyttet forskningsnettet[63] har mulighed for at få gennemført sårbarhedsscanninger af deres IT-systemer. DKCERT anvender Tenable Nessus Expert til at undersøge om institutionernes it-systemer har kendte sårbarheder, som er publiceret i National Vulnerability Database[64] (se Figur 7).

Scanningerne gennemføres på baggrund af konkrete bestillinger på ad hoc-basis eller som følge af en fast aftale om fx månedlige eller kvartårlige scanninger.

DKCERT har i 2023 gennemført 129 scanninger, hvoraf 120 var eksterne scanninger, mens ni var interne. I 2022 blev der gennemført 200 scanninger (10 interne og syv ad-hoc).

De interne scanninger gennemføres inden for institutionens firewall, hvor lokale netværk scannes. Den interne scanning giver mulighed for en mere fintmasket undersøgelse af institutionernes

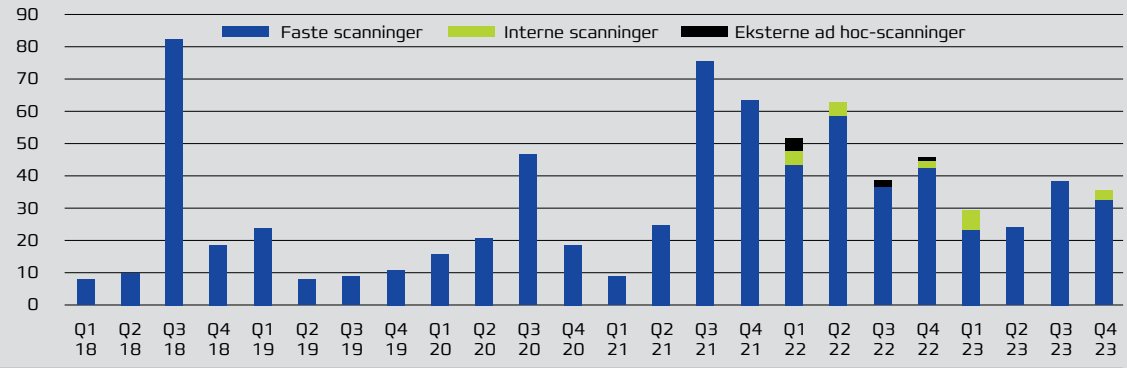
systemer, hvor der kan påvises sårbarheder, hvis man er på domænet som autoriseret bruger. Det kan pege på systemer med sårbarheder, der kan udnyttes af såvel uautoriserede som autoriserede brugere. De eksterne scanninger udføres uden for firewall'en.

DKCERT udarbejder en rapport med en prioritering af de fundne sårbarheder og anbefalinger til institutionens håndtering af disse, ud fra hvor alvorlige sårbarhederne er. På baggrund af denne træffer institutionen beslutning om håndtering af sårbarheden ud fra egen prioritering og risikotolerance.

[63] https://www.deic.dk/da/forskningsnet/basisnet/tilslutning/tilsluttede-institutioner
[64] NVD udgives og vedligeholdes af NIST, se https://nvd.nist.gov/

Figur 7 Scanninger på forskningsnettet 2018 - 2023

I 2023 udførte DKCERT 129 scanninger for institutioner på forskningsnettet.

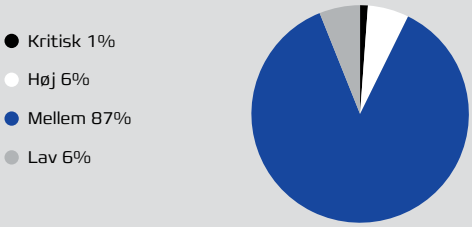


3. Året i tal og ord

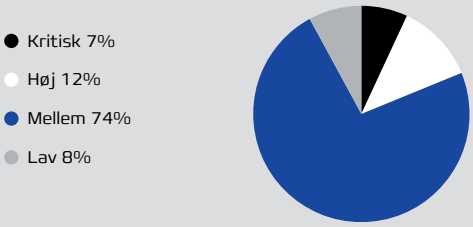
Figur 8

Diagrammerne viser sårbarhedernes fordeling på kritikalitet i 2022 og 2023. Sammenligningen peger på, at der er en stigning i antallet af sårbarheder, der ikke er 'mellem' i kritikalitet. Sårbarhedernes opdeling er baseret på OWASP TOP 10 Web Application Security Risks 2021.[65]

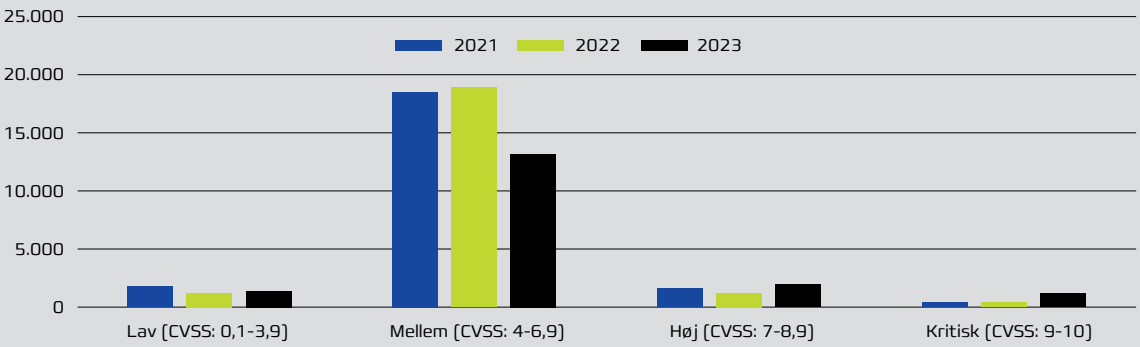
Fordelingen af de fundne sårbarheder ift. kritalitet 2022



Fordelingen af de fundne sårbarheder ift. kritalitet 2023



Udviklingen i fundne sårbarheder ift. kritikalitet 2021-23



Alvorlighedsgraden er baseret 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.

Det samlede antal scannede enheder/IP-adresser i 2023 var 437.118 IPS, hvoraf 436.618 i 'live'. Det betyder, at der er aktivitet på dem.

I 2022 var det samlede antal scannede enheder/IP-adresser 332.974 mod 115.069 i 2021. I 2020 var det samlede antal ca 300.000.

I alt er der fundet 18.026 sårbarheder, hvor langt de fleste er 'mellem' i kritikalitet. Samlet har 3.293 host-enheder i 2023 en kritisk eller høj sårbarhed, hvilket svarer til godt 18 pct. I 2022 blev der fundet 22.075 sårbarheder, mens det tilsvarende antal i 2021 var 22.549. Der er altså tale om en faldende tendens i antallet af fundne sårbarheder, som der til gengæld er flere kritiske af.

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

3. Året i tal og ord

SÅDAN KAN DU FORSTÅ EN CVSS-SCORE
CVSS er den metode og det scoringssystem, som anvendes til at finde frem til en alvorlighedsgrad af sårbarheder, der opdages i it-systemer og bl.a. bekendtgøres på National Vulnerability Database (NVD). Formålet med CVSS er at hjælpe organisationer til at vurdere og prioritere sårbarheder, der kan/skal håndteres som en del af en organisations patch managementproces – og i yderste konsekvens forsvare organisationen mod eventuelle cyberangreb, hvor udnyttelse af sårbarheder er anvendt.

Den 1. august 2023 blev ny version af Common Vulnerability Scoring System (CVSS v4.0) officielt taget i brug. I den forbindelse er der skabt et nyt nomenklaturunivers i forhold til de elementer, der indgår i beregningen af scoren.

Det er den såkaldte CVSS-SIG inden for FIRST, der har drevet processen med udviklingen af CVSS v4.0.

Elementerne er følgende:
CVSS-B: CVSS Basisscore – udgør de grundlæggende elementer i udnyttelse af sårbarhed, fx angrebsvektor, angrebskompleksitet, brugerinteraktion mv. Basisscoren er den, som almindeligvis fremgår af leverandørens advisory i forbindelse med offentliggørelse af sårbarheden.

CVSS-BT: CVSS Basisscore + Trusselsscore – her suppleres basisscoren med modenheden i evt. udnyttelse, dvs. om sårbarheden er under udnyttelse, om der er en proof-of-concept tilgængelig eller om sårbarheden har været rapporteret udnyttet. Denne score fastsættes af brugeren af systemet.

CVSS-BE: CVSS Basisscore + 'Environmental Score' – her suppleres basisscoren med elementer, som indgår i brugerens miljø, og som er afhængig af brugerens forhold, fx om adgangsvektoren er netværksbaseret, fysisk, lokal, om angrebskompleksiteten er høj eller lav, hvilke privilegier en udnyttelse kræver, brugerinteraktion mv.

CVSS-BTE: CVSS Basisscore + Trusselsscore + 'Environmental Score' – her kombineres alle tre elementer, basisscoren, trusselscoren og miljøscoren i beregningen.

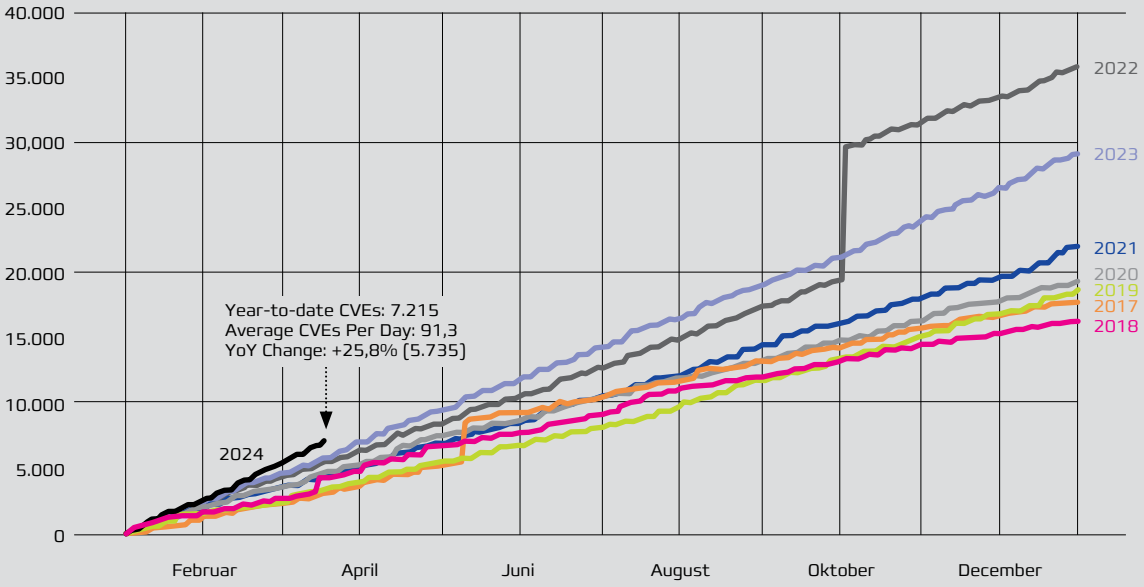
Der er udviklet et værktøj, der ud fra brugernes indtastninger kan beregne CVSS-scoren. Værktøjet findes på FIRSTs hjemmeside og giver et rigtigt godt indblik i, hvad sårbarhedens score er afhængig af, og hvad der fx. skal til for at en sårbarhed får den maksimale score på 10,0.

DKCERT anbefaler alle, der interesserer sig for sårbarheder og gerne vil forstå kompleksiteten i sårbarheder og deres udnyttelse, at anvende beregneren. Beregneren findes tilgængelig på FIRSTs hjemmeside.
https://www.first.org/cvss/calculator/4.0

3. Året i tal og ord

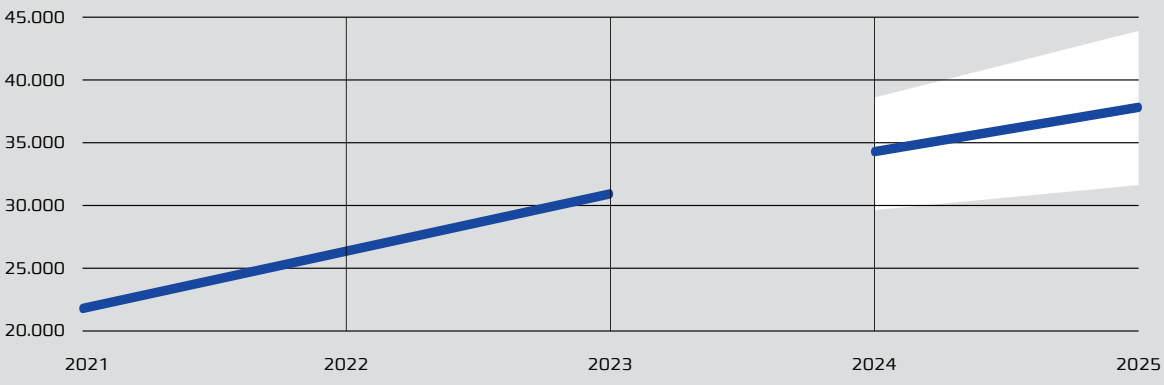
Figur 9 Udviklingen i antallet af CVE-numre

Grafen viser udviklingen i antallet af CVE-numre, der har været offentliggjort på National Vulnerability Database (https://nvd.nist.gov/) siden 2017. Det er disse CVE'er, som DKCERTs scanninger efter sårbarheder baserer sig på. Tallenes udvikling peger på, at der opdages flere og flere sårbarheder, hvorved også mulighederne for udnyttelse stiger. Modsat er offentliggørelse af sårbarheder også et signal til systemejere om behovet for løbende opdateringer. Grafen findes på FIRSTs hjemmeside https://www.first.org/epss/data_stats og opdateres løbende.



Figur 10 FIRSTs forudsigelse over udviklingen af publicerede sårbarheder 2021-2025

FIRSTs forudsigelse over udviklingen i antallet af publicerede sårbarheder på National Vulnerability Database. https://www.first.org/blog/20240109-vulnerability-forecast-2024



3. Året i tal og ord

3.1.2 Varsler fra DKCERT

Opdages der en sårbarhed med en CVSS-score på over 7, sender DKCERT et varsel ud via en mailingliste.[66] Varslerne omhandler sårbarheder og opdateringer i systemer, som forventes bredt anvendt, men DKCERT har som udgangspunkt ikke kendskab til, hvilket systemer der anvendes blandt modtagere. Derfor kan varslerne være relevante for nogen og irrelevante for andre, ligesom vores modtagere også kan finde informationen andetsteds, fx via tilmelding til andre nyhedsbreve og søgninger på 'X' (tidligere Twitter).

DKCERT modtager oplysninger og varsler fra egne kilder eller får indsigt i dem via nyhedsfeeds, opslag på X, netværk mv og sender de relevante varsler videre til modtagerne. Varslerne skrives altid i det samme 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 med mere information. I alt har DKCERT udsendt 89 varsler i 2023 mod 31 i 2022 (se figur 11).

Ud over udsendelse af egne varsler har DKCERT videresendt 21 varsler fra Center for Cybersikkerhed.

3.1.3 Formidling af varsler fra tredjeparter

I 2023 modtog og udsendte DKCERT varsler om flere forskellige typer sårbarheder, som er identificeret hos institutioner tilknyttet forskningsnettet. Denne service er baseret på automatisk indhentning og udsendelse af information, som først og fremmest kommer fra Shadowserver-projektet, der dagligt scanner forskningsnettet (og det øvrige internet) ud fra kendte og hyppigt udnyttede sårbarheder.[67]

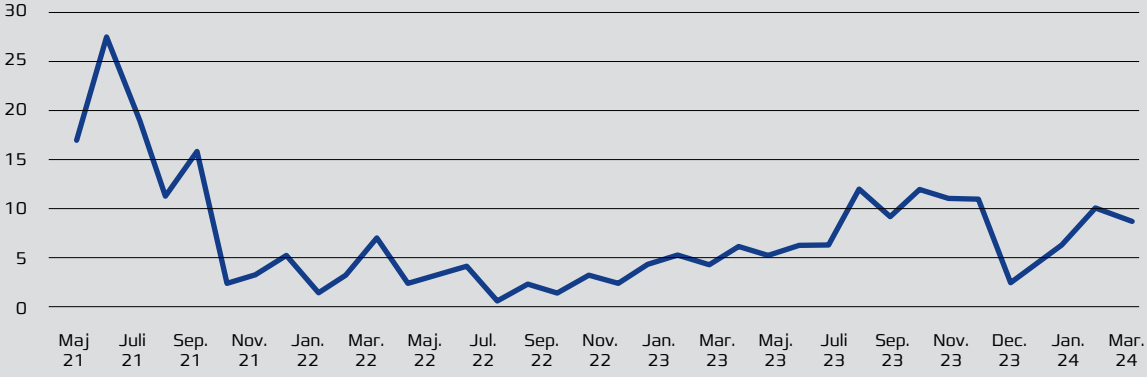
Der er således tale om en bredere scanning, end den som DKCERT udfører på bestilling for institutionerne.

[66] En CVSS-score fra 7-8,9 betegnes som 'high', mens en score fra 9-10 betegnes som 'critical'. DKCERT anvender betegnelserne 'alvorlig' for 'high', 'kritisk' og 'critical'.

[67] Shadowserver Foundation, https://www.shadowserver.org

Figur 11 Varsler udsendt af DKCERT fra maj 2021 til marts 2024

Varsler udsendt fra DKCERT siden maj 2021. Antallet af varsler er afhængig af, hvor mange alvorlige eller kritiske sårbarheder, der bliver fundet. Bortset fra december 2023 ses en tendens til stigning, hvilket matcher stigningen i antallet af publicerede CVE-numre på NVD, jf. figur 5.



3. Året i tal og ord

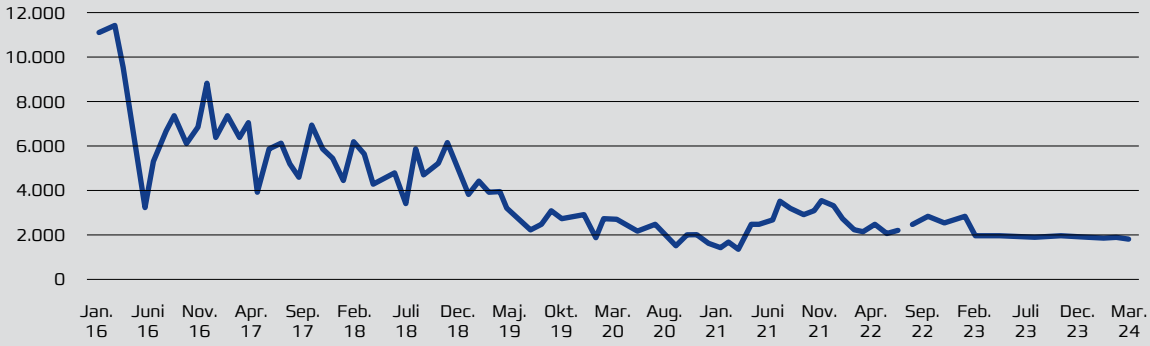
DKCERT er med i netværket af andre CERT-organisationer m.fl., der leverer data til Shadowserver. I DKCERTs tilfælde indsamler vi data om konkrete angrebsforsøg mod DKCERTs tjenester.

I 2023 er der i gennemsnit blevet udsendt ca. 172 unikke varsler pr. måned vedr. sårbarheder på forskningsnettet.

Grafen i Figur 13 (Unikke varsler) viser, at antallet af varsler sendt til det danske forskningsnet generelt er faldende fra i gennemsnit 650 pr. måned i 2016 til 172 i 2023. Dermed ser der ud til at være fundet et nogenlunde stabilt leje, som kan bekræfte tendensen om, at institutionerne er blevet bedre til at holde systemer opdateret.

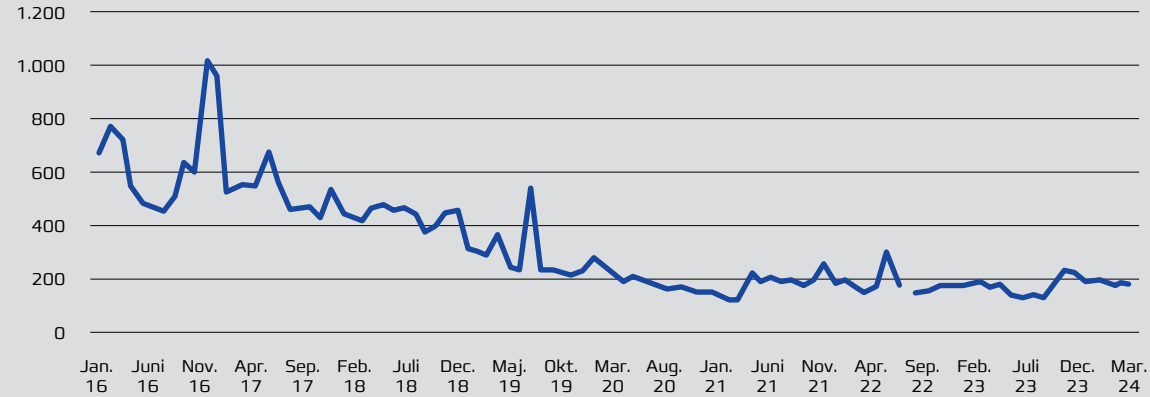
Figur 12 Varsler fra tredjeparter (2016-Q1, 2024)

Varsler fra tredjeparter fra 2016 til første kvartal 2024. 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, der ses på forskningsnettets ASN-nummer, ligesom der er kommet nye sagstyper til, hvorfor der kan ses en stabilisering. DKCERT justerer løbende udsendelsen af varsler i forhold til institutionernes ønsker og varslernes karakter.



Figur 13 Unikke varsler fra tredjeparter (2016-Q1, 2024)

Unikke varsler fra 2016 til første kvartal 2024. 'Unikke varsler' betyder at gentagelser er sorteret fra. Shadowserver sender den samme advarsel hver dag, så længe sårbarheden er åben på den pågældende IP.



3. Året i tal og ord

3.1.4 Sikkerhedshændelser i 2023

I 2023 modtog DKCERT oplysninger om 566 hændelser (2022: 629). De er samlet i 31 undersøgelser, hvor DKCERT bl.a. undersøger, om en mistanke om malware på et system kan bekræftes, giver besked til de berørte parter, og hændelserne omhandler typisk inficerede systemer på forskningsnettet. I 2022 blev der gennemført 34 undersøgelser, mens der i 2021 var tale om 67.

Denne service er automatiseret ud fra en indsamling af henvendelser fra eksterne kilder som sikkerhedsfirmaer, myndigheder eller andre CERT/CSIRT-organisationer rundt i verden, der har set uønsket adfærd fra eksempelvis IP-adresser på forskningsnettet. Med denne service filtrerer DKCERT de ikke-relevante henvendelser fra, orienterer de berørte aktører og udfører en indledende analyse/efterforskning af problemstillingen, hvis det vurderes relevant.

3.1.5 Videndeling ved større hændelser

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

I 2023 har DKCERT bistået med håndtering af hændelser på forskningsnettet i fem tilfælde. To hændelser har omhandlet ransomwareangreb og én hændelse har vedrørt udnyttelse af en sårbarhed. I to tilfælde har DKCERT bistået NC3 med sporing af nettrafik.

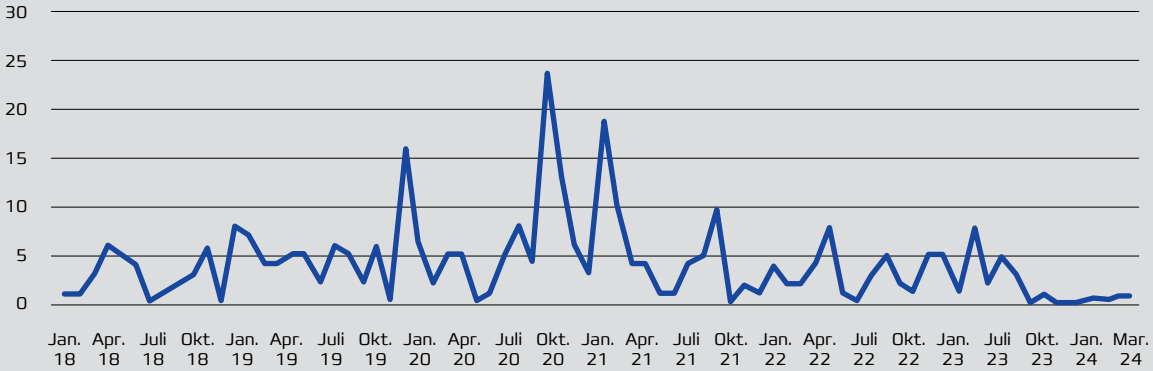
Med videndeling om hændelser kan andre institutioner forberede sig og evt. forebygge, at de rammes af samme type hændelser. Blandt cyberkriminelle er kendskab til succesfulde metoder til brud i bestemte sektorer eftertragtet viden og vil lynhurtigt brede sig, så andre vil forsøge at anvende samme metoder.

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 den fælles MISP og sekundært på CISO-niveau. Derudover udsendes varsler til alle institutioner tilknyttet forskningsnettet.

Figur 14 Undersøgelser januar 2018 - marts 2024

DKCERTs undersøgelser siden 2018. DKCERT får typisk flere rapporter, der omhandler den samme sagstype og det samme ip-nummer. De samles derfor i én undersøgelse – frem for fx 10 om det samme til den samme modtager. Antallet af rapporter og undersøgelser svinger derfor meget fra måned til måned.



3. Året i tal og ord

3.1.6 Dataanalyse

DKCERT har i 2023 gennemført 91 dataanalyser, hvoraf syv er gennemført efter henvendelse fra institutioner eller myndigheder og 84 på DKCERTs egen initiativ. Der er tale om analyse af netflow-data, dvs. netværkstrafik på forskningsnettet, som kan give ny viden om angrebsmønstre og proaktivt opdage angreb. Dataanalyse kan også anvendes reaktivt fx til efterforskning af sikkerhedshændelser for institutionerne og i forbindelse med politisager.

3.1.7 Uddannelses- og forskningssektorens MISP

I 2021 tog DKCERT uddannelses- og forskningssektorens MISP[68] i anvendelse med 13 institutioner – heraf de fleste universiteter. Der er i dag i alt 65 brugere med rettigheder til at indtaste data. Det er de enkelte institutioners ansvar at udpege brugere til at kunne registrere events i MISP'en – hvilket vil være afhængigt af, hvordan institutionerne har organiseret deres sikkerhedarbejde.

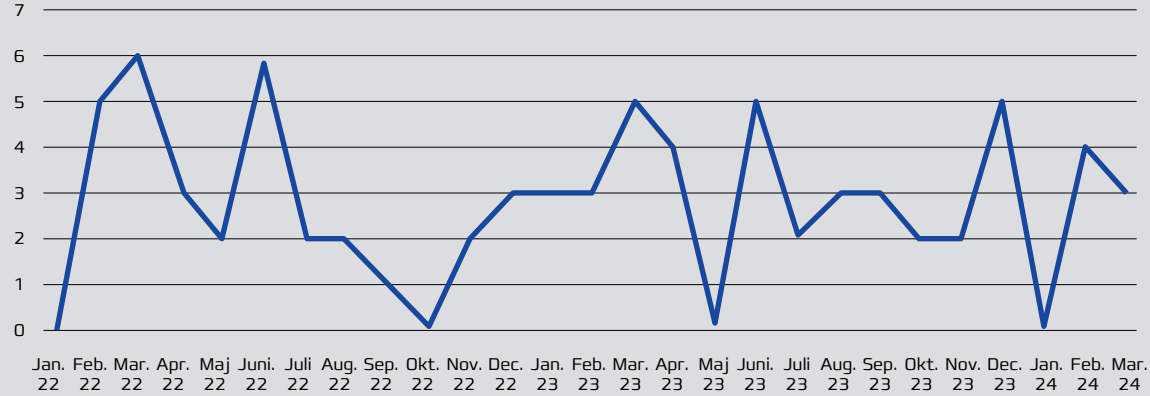
Med MISP stiller DKCERT således en platform til rådighed for uddannelses- og forskningsinstitutioner, hvor de systematisk kan dele viden om trusselsinformation sikkerhedshændelser og angreb. Delingen foregår enten manuelt eller automatisk ved integration til virksomhedens filtre eller logsystemer.

I 2023 har DKCERTs fortsat dialogen med de andre nordiske forskningsnet-CERT'er om etablere en MISP-infrastruktur for at kunne dele IoC'er regionalt i Norden.

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

Figur 15 Nyregistrede events i MISP fra januar 2022 - marts 2024

Antal hændelser i uddannelses- og forskningssektorens MISP siden januar 2022. Der har været registreret 37 nye events i 2023. Det er en stigning fra 32 events i 2022. Samlet er der pr. 1. januar 2024 registreret 581 events i MISP.



3. Året i tal og ord

3.1.8 Honeypot-projekt lukket

DKCERT etablerede i december 2022 en honeypot som et proof-of-concept mhp. at vurdere, om der kunne indsamles relevante data for uddannelses- og forskningssektoren. Honeypot'en skulle lytte til forskellige porte og dermed detektere forskellige angrebstyper, men da data ikke viste sig anvendelige, blev honeypot'en taget ud af drift i starten af 2023.

DKCERT arbejder på en ny løsning, der vil kunne indgå som analyseværktøj til en evt. kommende SOC.

3.1.9 Nyhedsformidling

I 2023 udgav DKCERT 314 artikler om forskellige aspekter af informationssikkerhed på cert.dk mod 311 i 2022 og 346 i 2021.

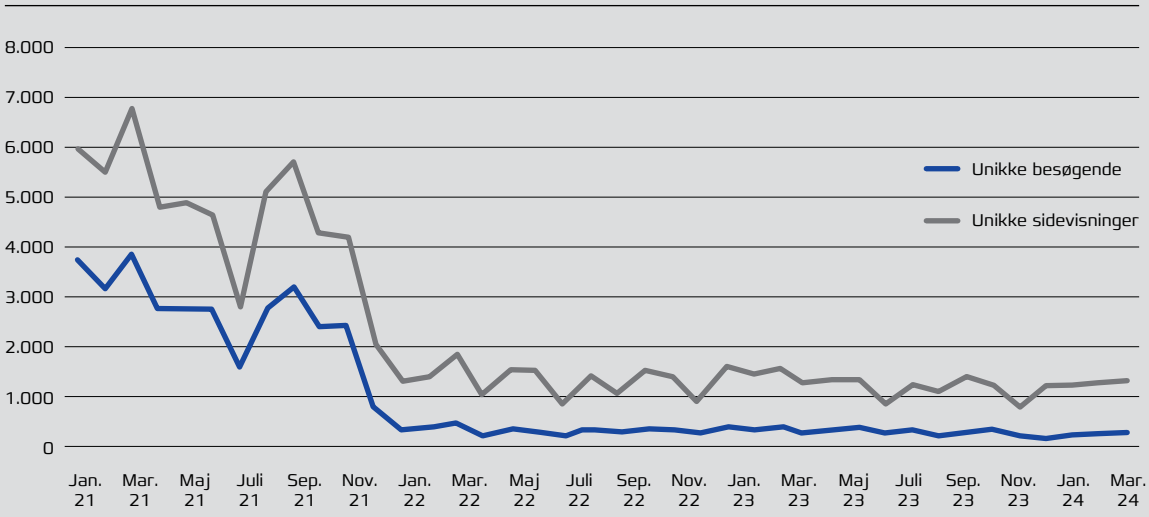
Artiklerne publiceres dagligt eller næsten dagligt på cert.dk. Artiklerne omhandler tekniske sårbarheder, nyheder om nye og gamle trusler, hændelser på universiteter og forskningsinstitutioner i verden, større databrud og cybersikkerhedspolitik fra ind- og udland.

Hver mandag samles den foregående uges nyheder i et nyhedsbrev, der udsendes til abonnenterne. Ved udgangen af 2023 abonnerede i alt 1.238 personer på DKCERTs nyhedsbrev. Hvor DKCERT tidligere sendte nyhedsbrev ud til fem målgrupper (borgere, små- og mellemstore virksomheder, ansatte ved forskningsnettet, DKCERTs interessenter og dagspressen), er alle abonnenter nu samlet i én gruppe, til hvem der sendes ét nyhedsbrev. Dette er sket i forbindelse med omlægning af nyhedsbrevssystemet, hvorved der også er slettet en række dubletter. Ved udgangen af 2022 var der 1.609 på listen over modtagere af nyhedsbrevene.

Cert.dk havde i 2023 15.094 unikke sidevisninger mod 15.764 i 2022. Dermed ser det ud til, at antallet er stabiliseret på omkring 15.000 efter det store fald fra 2021 og 2020, hvor der også var særligt fokus på cybersikkerhed, bl.a. pga. corona. Den offentlige fokus på cybersikkerhed er ikke faldet, snarere tværtimod. Dette har øget konkurrencen om opmærksomheden og også fået flere nyhedsmedier til at sætte cybersikkerhed på dagsordenen, hvorfor færre læsere søger mod cert.dk.

Denne tendens forstærkes også af, at myndighederne i de sidste år kommunikerer via sikkerdigital.dk, hvorved DKCERTs rolle som formidler af cybersikkerhed mod borgere og små og mellemstore virksomheder ikke længere er i fokus. Men øget interesse om cybersikkerhed kommer også med en pris. Der tales i dag i sikkerhedsmiljøet i højere og højere grad om risikoen for overkommunikation – altså hvor de samme nyheder og information om samme emner distribueres fra flere

Figur 16 Unikke besøgende og sidevisninger på cert.dk fra januar 2021



3. Året i tal og ord

afsendere og via flere kanaler. Det kan medføre, at de vigtigste informationer overses.

DKCERT har ved udgangen af 2023 3.387 følgere på X. Det er en stigning fra 3.369 2022. DKCERT postede tidligere alle publicerede artikler på cert.dk. For at imødegå tendensen til overkommunikation, poster DKCERT ikke i samme grad som tidligere, men gør det kun, når der publiceres nyheder af særlig og aktuel relevans for uddannelses- og forskningssektoren.

3.1.10 Mattermost

DKCERTs chatværktøj - Mattermost - er en sikker kanal til udveksling af informationer, og det bruges af sikkerhedsteknikerne til hurtig deling relevant af viden og udveksling af erfaringer. Der er pt. 29 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.

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

3.1.11 SikRef

DKCERT driver et netværk for sikkerhedsteknikere (SikRef), som er DKCERTs videndelingsforum for alle, der arbejder med sikkerhed på universiteterne. Formålet med forummet er at skabe et mødested for teknikerne, hvor de i et fortroligt rum kan udveksle erfaringer, give råd, orientere 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. Desuden understøtter netværket, at sikkerhedsmedarbejderne lærer hinanden at kende på tværs af institutionerne.

3.1.12 CISO-Forum

DKCERT er 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.

Figur 17 Antallet af følgere på DKCERTs X-profil siden januar 2020

3. Året i tal og ord

3.2 DKCERTS BRUGERBETALTE TJENESTER

3.2.1 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, som dækker hele Danmark. DPO-tjenesten blev grundlagt i 2018 og har i perioden oplevet flere skift i fokusområder. I dag har mange en højere grad af modenhed i compliance. Nogle har derfor også valgt at hjemtage DPO-opgaven. Men samtidig har DPO-tjenesten også oplevet en tilgang af nye kunder og konsultative opgavetyper, samtidig med at der har været et længerevarende vikariat. DPO-tjenesten har således i 2023 holdt samme niveau i leverancer som i 2022.

Udvidet rådgivning og fokusområder

Inden for de seneste år har der været en tendens til, at opgaven udvikler sig til også at omfatte rådgivning inden for anden lovgivning (fx sundhedsområdet). Denne tendens fortsætter, men set i lyset af det aktuelle trusselsniveau, er der også kommet øget fokus på GDPR og informationssikkerhed. Her drejer spørgsmålene sig om forhold vedr. organisatoriske- og tekniske sikkerhedsforanstaltninger, risikovurderinger o.lign. Som en udløber af dette øgede fokus faciliterer DPO-tjenesten fx et netværkssamarbejde mellem de tre kunstneriske Uddannelsesinstitutioner om 'Videndeling om informationssikkerhed og GDPR'. Netværket mødes to gange årligt hos hinanden til en åben videndeling om aktuelle forhold.

Indenfor GDPR sætter AI også en dagsorden, da AI også kan bruges til at behandle personoplysninger og derfor skal leve op til principperne. Der er en række udfordringer forbundet med at overholde GDPR, når man bruger AI-systemer. Én udfordring er, at AI-systemer kan være komplekse og vanskelige at forstå. Det kan derfor være svært at vurdere, hvordan AI-systemer overholder GDPR. En anden udfordring er, at AI-systemer kan lære og tilpasser sig over tid. Det kan gøre det vanskeligt at sikre, at AI-systemer altid overholder GDPR (Se også ovf. s. 22-23).

Efterspørgslen på vejledning inden for disse problematikker forventes at fortsætte og vokse i 2024, hvilket bl.a. også betyder løbende videreuddannelse af tjenestens medarbejdere via kurser, seminarer, konferencer o.lign.

GDPR-netværk for Uddannelse og Forskning

Netværket tog i 2023 navneforandring fra DPO-netværket, som det har heddet siden 2018, til GDPR-Netværk for Uddannelse og Forskning. Dette ud fra en erkendelse af, at der i dag deltager såvel DPO'er som andre med GDPR-funktioner i netværkets møder. Dertil er det også relevant at markere, at det er GDPR inden for forskning og uddannelse, som har netværkets særlige fokus. GDPR-netværket har til formål at sikre videndeling og erfaringsudveksling på tværs af de deltagende uddannelses- og forskningsinstitutioner under Uddannelses- og Forskningsministeriet om GDPR-problematikker, fx. om hvad andre gør, så der skabes konsensus. Ressourcerne til at løfte større problematikker er nemlig ofte små på den enkelte institution.

Netværket afholder to årlige virtuelle møder. Dertil er der mulighed for løbende udveksling via mailingliste og evt. afholdelse af ekstraordinære møder, hvis der er aktuelle forhold, som skal koordineres og løses.

Intern rådgivning

DPO-tjenesten yder også rådgivning til en række af DeiCs tjenester, fx i forbindelse med udarbejdelse af databehandleraftaler, forberedelse til certificeringer og eget tilsyn af DeiCs tjenester i forbindelse med DeiC-tjensten 'Tilsynsbussen', som er et initiativ, der har til formål at koordinere databehandlertilsyn med DeiCs tjenester.

3.2.2 Awarenesstjenesten Phish

Phishing er en altoverskyggende angrebsvektor for cyberkriminelle og dermed også en faktor for sikkerheden i uddannelses- og forskningssektoren. DKCERT har derfor i flere år stillet en tjeneste til rådighed for universiteter og andre institutioner på forskningsnettet, der bruges til

3. Året i tal og ord

udsendelse af fingerede phishingmails til ansatte og studerende mhp. at monitorere reaktionsmønstre hos brugerne.

DKCERT hjælper institutionerne med at gennemføre testen, der afsluttes med en detaljeret og anonymiseret rapport. DKCERT løser opgaven pr. medgået tid, hvilket typisk indebærer en udgift på ca. 15.000 kr. pr. kampagne.

DKCERT har ikke haft efterspørgsel på phishing-awareness-tjenesten i 2023.

3.2.3 Beredskabsøvelser

DKCERT tilbyder uddannelses- og forskningsinstitutioner på forskningsnettet at facilitere beredskabsøvelser. Medarbejdere fra DKCERT planlægger et øvelsesscenarie med udgangspunkt i institutionens beredskabsplan og udarbejder indspil, som tester deltagernes evne til at håndtere kritiske situationer, samarbejde, videndeling, inddragelse af eksterne parter og kommunikation med omverdenen. DKCERT kan deltage som øvelsesleder på dagen efter aftale.

DKCERT deltog som øvelsesplanlægger i DCIS-UFMs beredskabsøvelse for universiteterne i november 2023 og har gennemført en beredskabsøvelse for Aalborg Universitet i starten af 2024.

3. Året i tal og ord

NYE PROJEKTER PÅ DKCERT

DKCERT arbejder løbende på at videreudvikle vores services, så de møder institutionernes behov og tilpasses udviklingen i trusselsbilledet. Det foregår i formelle og uformelle projekter i samarbejde med danske og internationale kolleger. I første omgang er det projekter, der forsøger at opstille et proof-of-concept.

DNS RPZ

RPZ står for Response Policy Zones og er en filtreringsmekanisme, som enten kan forhindre brugere i at besøge på forhånd definerede internetdomæner eller omdirigere dem ved at manipulere DNS-opslag. RPZ kan hente data fra eksterne organisationer om fx skadelige domæner og derefter bruge oplysningerne til at blokere domænerne.

pDNSSOC

pDNSSOC er et værktøj, der gør det muligt at indsamle DNS-data centralt og korrelere med ondsindede domæner/IP'er fra en MISP. Ambitionen er at tilbyde universiteterne en pDNSSOC-klient på deres DNS-server, som kan sende DNS-data til DKCERTs pDNSSOC-server. Data fra pDNSSOC-serveren kan sendes til en central DNS RPZ, så filtreringen kan fange de relevante domæner.

DKCERT har indgået en aftale med CERN CERT om deling af data fra pDNSSOC. Se også SIE Europe-samarbejdet nedenfor, afsnit 3.3.3.

Netflow costum made detection tool

I samarbejde med SDU forsøger vi at opsamle unormale hændelser på Forskningsnettet. Ambitionen er at analysere Netflowdata i realtid, hvor disse data aggregeres, korreleres og filtreres ved hjælp af diverse open source-værktøjer og egenudviklede scripts, så unormale trafikmønstre kan identificeres og indgå som IoC'er i vores MISP eller i en evt. fremtidig SOC.

Nessus Expert full features

Nessus Expert er bygget direkte på fundamentet af vores nuværende scanningsenhed – Nessus Professional. Expert inkluderer alle de kendte funktionaliteter fra Nessus Professional, men har tilføjet funktioner, der gør det muligt at finde sårbarheder for flere angrebsmetoder. Med værktøjet har vi dermed et mere komplet værktøj til at vurdere sårbarheder mod en bredere vifte af angrebsvektorer. Nessus Expert giver bl.a. mulighed for at udføre eksterne 'Attack Surface Discovery'-scanninger, som scanner et topdomæne og identificerer alle sub-domæner, som er tilgængelige via internettet. Denne feature er allerede i drift og tilbydes institutioner på Forskningsnettet.

Kontakt evt. cert@cert.dk for mere information.

3. Året i tal og ord

3.3 DKCERTS DANSKE OG INTERNATIONALE SAMARBEJDER

Som en del af det internationale sikkerhedsfællesskab drager DKCERT nytte af videndelingen på nationalt, nordisk, europæisk og globalt plan. Det sker gennem samarbejder om sikkerhedsløsninger, i netværk og på konferencer.

3.3.1 Videndeling og netværk i Danmark

DKCERT er medlem af Rådet for Digital Sikkerhed med Lene Kim Dehn 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.[69]

Deltagelse i arbejdsgrupperne er med til at nuancere problemstillingerne og øge DKCERTs medarbejderes netværk og viden. DKCERT har i 2023 deltaget i en arbejdsgruppe vedrørende international overvågning.

Med udgangen af 2023 udløb mandatet for regeringens cybersikkerhedsråd, som Henrik Larsen har været medlem af. Rådet har været nedsat for at rådgive regeringen om, hvordan den digitale sikkerhed styrkes og sikre videndeling mellem myndigheder, erhvervsliv og forskningsverdenen. Rådet har i 2023 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.

3.3.2 Nordisk forskningsnet-CERT-samarbejde

DKCERT deltager i samarbejdet mellem CERT'erne for de fem nordiske forskningsnet og NORDUnet CERT. Netværket opstod omkring 2010 og kører med videomøder sammen med NORDUnet-CERT ca. hver 4-6 uge og et fysisk møde i forbindelse med NORDUnet Community Workshop.

På møderne diskuteres aktuelle sikkerhedshændelser og erfaringer med værktøjer og er med til at holde netværk etableret på fx konferencer og workshops ved lige. I 2023 afløste finske Funet norske Uninett CERT (nu eduCSC-NO) rollen som netværkets mødeleder. I 2024 varetages rollen af svenske Sunet.

3.3.3 SIE Europe (Passiv DNS)

SIE Europes mission er at gøre den europæiske digitale øknomi mere sikker ved at tilbyde en platform til indsamling, aggregering og deling af DNS-data, som løbende kan anvendes i kampen mod cyberkriminalitet. Data, som sendes fra datayderne (organisationer som har valgt at deltage i samarbejdet), stammer fra 'cache miss trafic' over den rekursive navneserver og omfatter derfor ikke data, som er personligt identificerbart.

SIE Europe er åbent for europæisk-baserede organisationer indenfor den statslige og kommercielle sektor samt højere uddannelse.

DKCERT deltager aktivt i samarbejdet om pDNS. Vi sender dels data fra forskningsnettets rekursive navneservere, og vi modtager til gengæld data fra samarbejdets partnere.[71] Data, som vi modtager er aggregeret og lagt sammen med anonymiseret DNS-data fra andre deltagere i projektet.

Formålet med samarbejdet er at højne sikkerheden for de institutioner, der er tilknyttet forskningsnettet uanset deres ekspertise, modenhed eller økonomiske ressourcer. Målet er at etablere en del af inputtet til en SOC, hvor der skal deles efterretninger (threat intilligence), som en af de vigtigste datakilder til opdagelse af potentielle hændelser og anvisning af mulig forebyggelse af hændelser.

I Danmark bidrager DKCERT, KU, SDU, AAU, CFCS og CSIS Security Group, men der er rigeligt plads til flere. Kontakt gerne DKCERT for yderligere information.

[69] https://www.digitalsikkerhed.dk
[71] https://www.sie-europe.net/

3. Året i tal og ord

3.3.4 TF-CSIRT og Trusted Introducer

DKCERT har siden 2002 været akkrediteret medlem og fik i februar 2024 certificeret medlemskab af Trusted Introducer.[72] TF-CSIRT[73] er en organisation for CERT/CSIRT'er, der oprindeligt er tilknyttet organisationer i Europa, men efterhånden er også teams fra andre verdensdele blevet optaget. Der er pt over 500 medlemsteams, hvoraf 53 er certificerede.

Netværket blev i perioden frem til 2022 faciliteret af GÉANT, men i 2022 overtog The Open CSIRT Foundation opgaven.

Open CSIRT Foundation og TF-CSIRT gennemfører til sammen fires events om året, hvor DKCERT deltager i dem alle. Den 13.-15. maj 2024 er DKCERT lokal vært for det 71. TF-CSIRT-møde.

DKCERT opnåede i februar 2024 SIM3-certificering. Det indebærer, at DKCERT som team lever op til en række krav i SIM3-modellen. SIM3 står for 'Security Incident Management Maturity Model' og er et udtryk for, hvor godt et team styrer, dokumenterer, udfører og måler sin sikkerhedsfunktion. Modellen består af 45 parametre i fire områder, som et teams modenhed måles efter. De fire områder er hhv. 'Organisation', 'Human', 'Tools' og 'Processes'. Modellen findes tilgængelig på Open CSIRT Foundations hjemmeside https://sim3-check.opencsirt.org/#/

[72] https://www.trusted-introducer.org/index.html
[73] https://tf-csirt.org/

3.3.5 GÉANT

GÉANT er det fælles-europæiske forskningsnet og forbinder de nationale forskningsnet i Europa med forskningsnet i andre verdensdele. DeiC og DKCERT er medlem af GÉANT gennem NORDUnet og deltager i en række projekter og samarbejder.

Beredskabsøvelsen CLAW

DKCERT har i flere år bidraget til planlægning af den europæiske beredskabsøvelse CLAW, der gennemføres hvert år i november eller december. I de sidste tre år er øvelserne foregået på Poznan Supercomputing and Networking Center i Polen. CLAW er finansieret af GÉANT og tilbydes alle europæiske forskningsnet.

DKCERTs deltagelse i CLAW er med til at styrke vores kompetencer inden for planlægning og gennemførelse af beredskabsøvelser, ligesom det styrker vores eget beredskab. Øvelsesscenarierne er inspireret af virkelige hændelser fra uddannelses- og forskningsmiljøer i Europa.

Siden 2021 har CLAW været tilbudt de europæiske forskningsnet i både et analogt og virtuelt format.

Øvrige projekter og arbejdsgrupper i GÉANT

> Etableringen af European R&E Security Intelligence Hub er et resultat af GÉANTs Cyber Threat intelligence subtask (GN5-1 WP8, CTI). Det er et to-årigt progtam støttet af Europa-Kommissionen. I løbet af det første år er der opbygget infrastruktur til deling af *intelligence* mellem deltagerne, profilering af trusselsaktører og udviklet en række værktøjer, der genererer og håndterer IoC'er, som kun har fokus på Academia.
> 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.

3. Året i tal og ord

3.3.6 FIRST

Siden 1993 har DKCERT været medlem af FIRST (Forum of Incident Response and Security Teams),[74] som er en organisation for 74 CERT/CSIRT/PSIRT-teams i 108 lande, heraf 11 medlemmer i Danmark (pr. 1. marts 2024). DKCERT-medarbejdere deltager i et årligt regionalt seminar for Europa samt i årskonferencen og generalforsamlingen.

I 2024 holdes årskonferencen i Fukuoka i Japan, mens den i 2025 foregår i København med Center for Cybersikkerhed som lokal vært. DKCERTs tidligere chef Henrik Larsen er udpeget som formand for programkomiteen for konferencen i 2025.

DKCERT deltager i følgende arbejdsgrupper under FIRST:

- 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 FIRSTs årskonference og en til to gange via videomøder. I 2023 blev møderne gennemført virtuelt i februar og fysisk i forbindelse med årskonferencen i juni.
- FIRST Automation SIGs formål er at dele viden om de eksisterende løsninger, som hver CERT har kørende. Gruppen skal understøtte læring og rådgivning mellem medlemmerne af gruppen. Gruppen mødes en gang årligt i forbindelse med FIRSTs årskonference og hver måned via videomøder.
- FIRST Malware Analysis SIG udvikler et framework som indeholder best practices vedr. malwareanalyse, værktøjer til forskellige funktioner, lister med IoC'er og en kommunikationskanal til drøftelse af nye teknikker og metodologier.

[74] https://www.first.org/

4. Eksterne bidrag

Hvordan måles informationssikkerhed? Fire af DKCERTs samarbejdspartnere giver deres bidrag

4.1 HACKERSTOP - EN LET MÅLING DER (OGSÅ) STYRKER MEDARBEJDERNES LÆRING

Siden 2022 har Dansk IT drevet måleværktøjet Hackerstop, der er udviklet med øje for små og mellemstore virksomheder i Danmark.

AF CLAUDIA ZÖLLNER,
DANSK IT

For størstedelen af Danmarks virksomheder – særligt de små og mellemstore – er det er svært at vurdere deres eget sikkerheds- og modenhedsniveau. Set med virksomhedernes øjne, er opgaven uoverskuelig, de ved ikke, hvor de skal starte og slutte, de har ikke ressourcerne internt, ej heller nødvendigvis økonomien til at betale konsulenttimer - eller kræfterne til at implementere tunge sikkerhedsrammeværker, som blandt andre ISO/IEC 27001 og D-mærket.

Og selvom det er alment kendt, at op imod 90 pct. af alle sikkerhedsbrud sker pga. menneskelige fejl, så er der inden for cybersikkerhed stadig størst fokus på de tekniske foranstaltninger og implementering af tunge rammeværker og processer.

Dette var udgangspunktet, da Dansk IT (en forening af it-professionelle og it-brugere) med NBI som nøglepartner og med støtte fra Industriens Fond satte sig sammen for at skabe et værktøj, som var nemt at bruge for små og mellemstore virksomheder. Værktøjet hedder HackerStop, og det repræsenterer en nytænkning inden for målinger, hvor medarbejdere er en gennemgående bestanddel i tilbagevendende målinger, og hvor det primære fokus er medarbejderne og virksomhedskulturen.

HackerStop-rammeværket er kvalificeret af frivillige eksperter i Dansk ITs fagråd for informationssikkerhed og andre stærke spillere og bygger dermed på de bedste erfaringer ift. både cybersikkerhed, adfærdsdesign og forandringsledelse. Netop dét gør HackerStop til noget ganske særligt.

Fondsmidlerne og de frivillige kræfter er årsagen til, at der for få økonomiske midler er udviklet et let og intuitivt værktøj, som både den lille og den store virksomhed kan finde ud af og har glæde af!

Åbenlyse tendenser og problematikker

Siden januar 2022, hvor HackerStop havde premiere, har organisationer målt deres medarbejderes modenhed inden for cybersikkerhedsawareness i HackerStop.

I alt er der med udgangen af 2023 gennemført 400 virksomhedsmålinger, registreret 400 virksomheder fordelt på 79 forskellige brancher og 17.000 brugere.

Ud fra disse anonymiserede data ses tendenser og problematikker, som går på tværs af alle 79 brancher.

En af tendenserne er, at få ved, hvad de skal gøre, hvis de er udsat for sikkerhedsbrud.

På spørgsmålet: 'Har virksomheden fortalt dig, hvad den vil gøre, hvis den er udsat for hackerangreb?' svarer medarbejderne i snit 4,5 på en skala fra 1 til 10.

Adgangskoder skaber altid problemer

Der er rigelig plads til forbedring ift. at tale mere åbent på arbejdspladserne om it-sikkerhed. Generelt svarer gennemsnittet af medarbejderne lavt på følgende spørgsmål:

- Har I for nyligt på arbejdspladsen talt om, hvad en god og sikker adgangskode er?
- Har I for nyligt på arbejdspladsen talt om mistænkelige beskeder?
- Har I for nylig på din arbejdsplads talt om at beskytte smartphone/computer/tablet mod at andre kan få adgang til den?
- Taler I på arbejdspladsen ærligt om, at fejl opstår, som kan udgøre en risiko for arbejdspladsen?
- Taler I på arbejdspladsen ærligt om, at fejl opstår, som kan udgøre en risiko for arbejdspladsen?
- Taler I på arbejdspladsen om hvilke oplysninger, der er kritiske for din virksomhed?

4. Eksterne bidrag

Persondata og virksomhedsfølsomme oplysninger
Til gengæld er det positivt, at de fleste medarbejdere har rigtig godt styr på hvilke data, der er følsomme, og at man skal passe på at tale om persondata i det offentlige rum. Det skyldes sandsynligvis særligt EU's persondataforordning, som har haft stort fokus hos mange organisationer, siden den blev gennemført i 2018.

Der ligger mange devices gemt rundt omkring, som ikke bliver brugt mere: Computere, telefoner, tablets. Nogle gange bliver de smidt ud på genbrugspladsen eller ligger og samler støv hjemme hos medarbejderen eller bliver brugt af medarbejdernes børn. Og det er enhver hackers tivoli.

På spørgsmålet: 'I hvor høj grad er du opmærksom på, at devices, du ikke længere bruger, bliver renset for tidligere adgangskoder og virksomhedens følsomme oplysninger?' svarer medarbejderne i gennemsnit 6,5 på en skala fra 1 til 10.

HackerStop adskiller sig fra andre målemetoder
Det anderledes ved Hackerstop er, at det medarbejderne synes er vigtigst og mest interessant indgår i det samlede resultat, ligesom virksomhederne kan tilføje egne spørgsmål. Medarbejderne kan også give feedback, hvilket giver mulighed for anonym dialog med medarbejderne. Det giver indblik i kulturen og en indikation af, hvor der skal sættes først for at udvikle en sund sikkerhedskultur.

Endelig understøtter Hackerstop målinger over tid, så man kan se udviklingen og vurdere om de iværksatte tiltag har haft den ønskede effekt.

Rejsen til ny og mere sikker digital kultur
Hvis virksomheder skal have et stærkere forsvar mod it-kriminelle og hackere, skal der langt mere til end blot en opdateret firewall. Det kræver en adfærdsændring blandt medarbejderne, og den ændring starter allerede, når medarbejderne reflekterer over spørgsmål, som de stilles i HackerStop-målingen. Og det skaber basis for forandring.

Fakta om HackerStop
Alle kan oprette en gratis profil i HackerStop og gennemføre en personlig måling eller virksomhedsmåling.

- Værktøjet er gratis for målinger på op til 100 personer.
- Der kan sendes målinger ud på op til 10.000 personer ad gangen.
- Målingen indeholder 35 spørgsmål som kan besvares på 5-10 minutter
- Data er valide fordi brugerne svarer ærligt, da deres svar er anonyme
- En måling kan sættes op så den kører hvert år, på den måde måles udviklingen over tid
- Der mulighed for anonym feedback og dialog mellem dem som har besvaret målingen og den som har sendt målingen ud.

4. Eksterne bidrag

Figur 18 Gennemsnitlige svarscore

Skemaet viser den gennemsnitlige svarscore på en skala fra 0-10, hvor 0 repræsenterer 'slet ikke' og 10 repræsenterer 'I meget høj grad'. I afrapporteringen til virksomheden gengives scoren på en skala fra 0-100. Data i skemaet herunder er baseret på 400 virksomhedsmålinger og 17.000 brugeres svar på spørgsmål i perioden fra starten af 2022 til udgangen af 2023.

Udvalgte spørgsmål fra spørgerammen	Score (gennemsnit)
Hændelser	**64**
Har virksomheden fortalt dig, hvad den vil gøre, hvis den er udsat for hacker-angreb?	45
Hvis du mister et device, ved du så, hvad du skal gøre?	69
Hvis du modtager en mistænkelig besked, siger du det videre til en, som kan tage sig af det?	75
Taler I på arbejdspladsen ærligt om, at fejl opstår, som kan udgøre en risiko for arbejdspladsen?	56
Ved du hvem, du skal henvende dig til, hvis du kommer til at klikke på et mistænkeligt link i en besked?	74
Beskeder	**70**
Har I for nyligt på arbejdspladsen talt om mistænkelige beskeder?	49
I hvor høj grad kan du genkende en phishing besked?	68
Inden jeg klikker på et link, overvejer jeg om det er sikkert.	83
Jeg ved, at der kan være falsk afsender på en besked.	84
Kan du forklare hvad phishing er?	66
Oplysninger	**74**
I hvor høj grad føler du dig klædt på af virksomheden til at passe på følsomme oplysninger?	73
I hvor høj grad kan oplysninger i de forkerte hænder lukke din virksomhed?	59
Jeg har et klart billede af hvilke oplysninger, der er følsomme for virksomheden.	75
Når jeg taler i telefon i det offentlige rum, er jeg opmærksom på, om jeg taler om fortrolige emner.	81
Ved du, hvordan det forventes, at du behandler arbejdspladsens fortrolige informationer og data?	79
Devices	**66**
Er I på din arbejdsplads bevidste om, at fremmede ikke kan få adgang til jeres devices?	71
Har I for nylig på din arbejdsplads talt om at beskytte smartphone/computer/tablet mod at andre kan få adgang til den?	46
I hvor høj grad er du opmærksom på, at devices, du ikke længere bruger, bliver renset for tidligere adgangskoder og virksomhedens følsomme oplysninger?	65
Jeg går op i at sikre, at fremmede ikke kan gå ind fra gaden og få adgang til vores devices.	77
Når jeg går på nettet (wifi) med min computer, tablet og telefon er jeg opmærksom på, om det er et sikkert netværk.	71

4. Eksterne bidrag

4.2 NÅR VERDEN IKKE ER SORT OG HVID – EN DCIS' BERETNING OM MÅLING AF CYBER- OG INFORMATIONSSIKKERHEDSTILTAG

DCIS-UFM, UDDANNELSES- OG FORSKNINGSMINISTERIETS DECENTRALE CYBER- OG INFORMATIONSSIKKERHEDSENHED

Hvordan måler man på sikkerhedsarbejde, så både myndigheder og universiteter får et brugbart billede af sektorens modenhed over for et stadig mere alvorligt trusselsbillede? Kan man favne over kompleksitet og forskelligartethed, samtidigt med at man anvender håndfaste kriterier? Det er netop, hvad Uddannelses- og Forskningsministeriets decentrale cyber- og informationssikkerhedsenhed (DCIS-UFM) brugte en stor del af kræfterne på at afdække i 2023.

DCIS-UFM er en ny enhed, der bl.a. skal understøtte universiteterne med at højne hele sektorens robusthed på forskningsområdet og agere operativt bindeled til Center for Cybersikkerhed under alvorlige hændelser. DCIS-UFM er blevet til på baggrund af Danmarks nationale strategi for cyber- og informationssikkerhed for 2022-2024, som udvider kravene til sikkerhed både i bredden og i dybden – i erkendelse af, at cybertruslen kan ramme alle dele af samfundet og let kan sprede sig mellem sektorer. Konkret betyder det, at hvor der før var seks DCIS'er for de allermest kritiske sektorer i samfundet (energi, finans, sundhed, søfart, tele og transport), er der nu oprettet i alt 26 DCIS'er i Danmark – herunder DCIS-UFM med fokus på forsknings- og rumområdet.

Universiteterne som en del af den nationale strategi for cyber- og informationssikkerhed

Med den nationale strategi for 2022-2024 kom en række krav, som universiteterne og Uddannelses- og Forskningsministeriet skal leve op til. I strategien fremgår det af initiativ 1.1, der vedrører styrket sikkerhed af samfundsvigtige funktioner, at '*Ministerområder med ansvar for samfundsvigtige funktioner, der i væsentlig grad er it-understøttet, forpligtes til at udarbejde strategier for cyber- og informationssikkerheden samt oprette en decentral cyber- og informationssikkerhedsenhed (DCIS).*'[75] På den baggrund har Uddannelses- og Forskningsministeriet oprettet en DCIS og har i samarbejde med særligt universitetssektoren udarbejdet sektorstrategien 'Forskning i trygge rammer', der ligesom den nationale strategi gælder for perioden 2022-2024. Sektorstrategien har fokus på at skabe rammer for at beskytte universiteter og forskning mod cybertrusler, men omfatter også kortlægning af cybertrusler på rumområdet, hvor Uddannelses- og Forskningsministeriet er den koordinerende rummyndighed i Danmark.[76]

Samarbejdet med sektoren: En styregruppe sikrer fremdriften

Universitetssektorens arbejde med sektorstrategien 'Forskning i trygge rammer' understøttes af en styregruppe med repræsentanter fra universitetssektoren, som følger sektorstrategiens implementering. Styregruppen drøfter løbende, hvordan strategien kan implementeres i praksis. Dermed understøtter styregruppen i fællesskab, at sikkerheden bliver løftet, samtidigt med at der tages hensyn til sektorens særlige kendetegn så som bl.a. åbenhed og forskningsfrihed. Universiteterne er selvejende institutioner og DCIS-UFM har derfor langt hen ad vejen en faciliterende rolle og understøtter universitetssektoren med at udarbejde målbare metoder for at følge op på strategiens implementering.

Ledelsesforankring og modenhed: Hvordan måles niveauet?

Sektorstrategien 'Forskning i trygge rammer' har fokus på at styrke universitetssektorens resiliens over for cybertrusler på forskningsområdet. Sektorstrategien indeholder bl.a. initiativer om, at cybersikkerhed forankres i topledelsen, at der løbende tages stilling til det ønskede modenhedsniveau, samt at sikkerhedstiltag har en målbar effekt, som kan sammenlignes på tværs af sektoren. Sidstnævnte er beskrevet under strategiens initiativ 1.3.[77]

DCIS-UFM har efter en dialog med styregruppen

[75] National strategi for cyber- og informationssikkerhed 2022 – 2024, side 44, udgivet 2021, link: https://fm.dk/media/25359/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf

[76] Forskning i trygge rammer, Delstrategi for Cyber og Informationssikkerhed 2022 – 2024, side 6ff, udgivet 2023, link: https://ufm.dk/publikationer/2023/filer/forskning-i-trygge-rammer-delstrategi-for-cyber-og-informationssikkerhed-2022-2024.pdf

[77] Forskning i trygge rammer, Delstrategi for Cyber og Informationssikkerhed 2022 – 2024, side 16, udgivet 2023, link: https://ufm.dk/publikationer/2023/filer/forskning-i-trygge-rammer-delstrategi-for-cyber-og-informationssikkerhed-2022-2024.pdf

4. Eksterne bidrag

taget udgangspunkt i standardiserede metoder fra bl.a. Digitaliseringsstyrelsen, herunder deres model for at målemodenheden hos ministerierne i forhold til ISO 27001-standarden for informationssikkerhed, for at følge op på ledelsesforankringen og de enkelte universiteters cyber- og informationssikkerhedsmæssige modenhed.

Initiativ 1.3:
Øget strategisk målbarhed på sikkerheds- og modenhedsniveauet
For at sørge for at cyber- og informationssikkerhedsmæssige tiltag i universitetssektoren opnår de ønskede mål, er det nødvendigt med et fokus på målbarhed af effekt. For at kunne opbygge det mest retvisende billede af hele sektoren, er det vigtig at tiltag på de enkelte universiteter måles på baggrund af ens kriterier på tværs.

Standarderne bruges som et redskab til at skabe et sammenligneligt, anonymiseret overblik over universiteternes modenhed, som dels hjælper universiteterne med at fastlægge deres ønskede niveau, dels hjælper DCIS-UFM med at få et overblik over, hvor sektoren som helhed befinder sig sikkerhedsmæssigt. Efter den første runde af besvarelser fra universiteterne i 2023 er der nu skabt et meget overordnet billede af sektorens modenhed, som skaber grobund for dialog og løbende vil blive forfinet i de kommende år.

Foruden målbare metoder vedr. ledelsesforankringen følger DCIS-UFM sammen med styregruppen også op på sektorstrategiens øvrige overordnede mål om bl.a. at understøtte og udvikle den risikobaserede tilgang og styrke samarbejdet og koordineringen på tværs af sektoren med strategisk målbarhed og koordination for øje. Det er således ambitionen at skabe målbare resultater på tværs af hele sektorstrategien, hvor DCIS-UFM også trækker på erfaringer fra andre DCIS'er

På sigt er det håbet, at de drøftelser, der løbende er i DCIS-styregruppen om måling kan føre til en fælles forståelse af, hvor sektoren som helhed skal hen. Det har været et gavnligt første skridt hen imod, at universiteterne agerer så åbent som muligt og så sikkert som nødvendigt over for de avancerede trusselsaktører, som kan ramme samfundsvigtige funktioner eller banebrydende forskning.

4. Eksterne bidrag

4.3 MOVING BEYOND METRICS – USING ETHNOGRAPHIC STUDIES TO UNDERSTAND THE 'GOOD' ORGANIZATIONAL REASONS FOR 'BAD' CYBERSECURITY COMPLIANCE IN SMES.

AF LAURA KOCKSCH & TORBEN ELGAARD JENSEN
THE TECHNO-ANTHROPOLOGY LAB, AALBORG UNIVERSITY

Regulatory efforts such as ISO 27001 and NIS 1 and 2 demand that organizations of various sizes and purposes monitor and measure their security controls. While technical applications can be tested and monitored, measuring user's or administrator's compliance – their correct and regular deployment of security techniques - is considerably more challenging. CISOs and compliance managers are left with abstract metrics such as response rates to awareness lectures or phishing exercises.

In this short piece, we argue that compliance not only evades metric assessment but that it requires an alternative thinking and method to ascertain the quality of cybersecurity practices. This alternative way of thinking must be rooted in an understanding of organizational structures and everyday arrangements. By pointing to 'good' organizational reasons for 'bad' cybersecurity compliance, we aim to supplement the metric understanding of compliance with the sense of practical everyday concerns that one may gain by conducting in-depth ethnographic observations.

In our perspective, incidents of incompliance may indicate a lack of awareness or skill, but they may just as well be indicative of complex organizational and practical dilemmas. So rather than condemning incompliance, we argue that these incidents should be seen as valuable occasions to understand how organizational formats and practices compete with regulatory and abstract cybersecurity ideals.

A good place to start understanding cybersecurity practices on the ground is to look at how organizations structure and delegate responsibil-

4. Eksterne bidrag

ity for their cybersecurity work. Large organizations such as law enforcement agencies or large corporate have strict hierarchical structures and are therefore able to enforce compliance to cybersecurity in a top-down manner. But many other organizations work in quite different ways: Universities, for example, only respond reluctantly to a central command structure; hierarchies are within research groups, departments, and disciplines. And despite the best efforts of eager IT support (that are often supplemented by local IT gurus), cybersecurity compliance cannot be prescribed in a top-down way.

In our ethnographic study of 30 small- and medium-sized enterprises in Denmark (Kocksch & Elgaard Jensen 2023), we also encountered additional organizational patterns worth considering; we saw cases where the primary responsible for cybersecurity was a communication person, an IT-manager or accountant, and we saw a plethora of different ways in which cybersecurity knowledge was communicated and shared. All of this may of course sound like rare exceptions, where it not for the fact that SMEs actually account for 98,7% of Danish companies![78]

Most of the companies in our study had no more than 50 employees, no designated cybersecurity unit and organizational functions that often overlapped or were temporary. The management of such companies takes place through collegial exchanges and face-to-face contacts while IT systems are procured task-based and pragmatic. SMEs tend to be organized in flat hierarchies; they work without top-down oversight and management. As a consequence, cybersecurity cannot be prescribed from above, nor advocated for by IT departments or local gurus. Rather it emerges bottom-up, deeply embedded in the day-to-day handling of IT systems.

When confronted with metric measurements, SMEs provided us with various good local explanations why an update was not rolled out (everywhere) or an authentication mechanism was not useful (in some work routines). Rather than simply being incompliant, SMEs demonstrated situated competencies and mitigation strategies. Some for example explained to us the tedious work that goes into keeping their fragile legacy technology set-ups afloat, knowing full well that they might not comply with current cybersecurity regulations.

While we could have condemned these instances as incompliance, we saw them as results of intricate practical dilemmas as well as 'good' local reasons for 'breaking things a little' (quote from an IT manager). Therefore, it is essential to understand incompliance not as a metric indicator for better or worse security, but rather as an occasion to understand SMEs' practical realities. As such, 'bad' results are not easily eradicated, and, possibly more importantly, when attempting to eradicate them we may end up throwing good local practices out with the bathwater.

During our visits, we discovered that SMEs flat hierarchies, local practices and skillful compromising was a resource rather than a hindrance for cybersecurity, something to further nurture rather than overwrite. Pursuing pure metric measurement, and by shaming 'bad' cybersecurity practices, we fear that SMEs will be discouraged from engaging in cybersecurity conversations. By using ethnography to emphasize the good local reasons, our hope is to facilitate a frank and open conversation about cybersecurity rooted in the everyday realities of Danish SMEs.[79]

Going forward, we suggest four principles for assessing cybersecurity in SMEs:

- Assessment of the maturity of cybersecurity in SMEs requires a substantial rethinking of parameters established in military or large organizational contexts.
- Mechanisms for enforcing cybersecurity must be suitable and realistic for decentralized or flat organizations.
- Instances of incompliance must not be condemned but rather seen as opportunities for examining competing local and abstract goals and practices.
- More curiosity about locally 'good' cybersecurity is needed to generate more realistic and practice-based cybersecurity assurance.

[78] OECD (2022), Financing SMEs and Entrepreneurs 2022: An OECD Scoreboard, OECD Publishing, Paris, https://doi.org/10.1787/e9073a0f-en.

[79] Kocksch, L., & Elgaard Jensen, T. (2023). 'Good' Organizational Reasons for 'Bad' Cybersecurity: Ethnographic Study of 30 Danish SMEs. Aalborg Universitet. https://doi.org/10.54337/aau513432435

5. Trends og anbefalinger

5. Trends og anbefalinger

2023 har været præget af krige i verden, kunstig intelligens og den fortsatte anvendelse af hybride angrebsformer, cyberaktivisme og endnu mere fokus på cyberspionage.

Med udgangspunkt i det aktuelle trusselsbillede og dagsordenen giver vi her et bud på trends i 2024 for henholdsvis cyber- og informationssikkerhed og på GDPR-området.

På baggrund af det giver DKCERT en række anbefalinger til hhv. ledelsen, forskere og undervisere og it-ansvarlige på uddannelses- og forskningsinstitutionerne.

5.1 CYBERTRENDS 2024

Udnyttelse af 0-dagssårbarheder breder sig

Der opdages flere og flere sårbarheder. I 2023 var det over 30.000 og i 2024 bliver tallet måske over 40.000. Det vil føre til mere handel med 0-dagssårbarheder og flere udnyttelser af sårbarheder i vinduet mellem offentliggørelse og organisationernes patch. Selv om forskellige instanser forsøger at udsende varsler om sårbarheder og gøre opmærksom på kendte udnyttede sårbarheder, så er forretningsmodellen for såvel statssponseret som ikke-sponseret cyberspionage og -kriminalitet så attraktiv, at vi formentlig kommer til at se, at udnyttelser af hoved- og biprodukter øges.

Passwordless' gennembrud

I slutningen af 2023 havde Microsoft, Google og Apple alle implementeret 'passwordless' i deres portefølje af produkter. Passwordless er pseudonym for kodeordsfrit login og indebærer, at man med en passkey kan logge ind på apps og websteder med en pinkode eller biometrisk sensor uden behov for kodeord. Det kræver blot en hardwareenhed som fx en telefon, et ur, en FIDO-nøgle eller lignende, hvorfra adgang til passkey'ens økosystem er tilgængeligt.

Det er forventningen, at tjenester i de kommende år løbende vil implementere teknologien, som dermed vil udvide sin anvendelse og blive best practice for såvel professionelle som private.

Påvirkningsoperationer

Påvirkningsoperationer har bl.a. til formål at destabilisere lande og de bærende institutioner i samfundet. Det kan også bruges mod enkeltstående sektorer, fx uddannelse og forskning. Dette vil være relevant i en videnssikkerhedskontekst, hvor længerevarende strategiske indsatser fra fremmede stater kan have indflydelse på forskere, studerende og ansattes holdninger og meninger og dermed også arbejde og forskningsområder.

4. Eksterne bidrag

AI i cybersikkerhed
Mulighederne for brug af kunstig intelligens i cybersikkerhed er med fx. ChatGPT og andre AI-værktøjer blevet lettere tilgængelige for såvel cybersikkerhedsfolk som cyberkriminelle. AI udvider puljen af aktører, der kan udføre kriminelle aktiviteter, som ellers hidtil har været de mere vidensbaserede aktører forundt. AI kan fx effektivisere kriminelles social engineering-arbejde og gøre det nemmere og billigere at iværksætte fx spearphishingangreb mod særligt attraktive mål i uddannelses- og forskningssektoren. Deep fake-teknologien er allerede langt fremme og vil også kunne indgå i værktøjskassen i forhold til målrettede angreb og påvirkningsoperationer.

På den anden side giver AI- og ML-baserede værktøjer flere muligheder i bekæmpelsen af cyberkriminalitet, bl.a. ved automatiseret netværksovervågning og dataanalyse.

Supply Chain-angreb
Der er en stigende opmærksomhed på at udnytte sårbarheder i værdikæderne. Værdikæder er forholdet mellem kunder og en eller flere leverandører og underleverandører. Det gælder fx it-systemer og -produkter, der hænger sammen i et produktionsmiljø, hvor fx en it-leverandør yder en bestemt it-service, mens en anden fx leverer indholdet. Produkternes stigende grad af forbundethed gør angrebsfladerne større og vil kræve mere af organisationernes evne til at beskytte sig og vælge og styre leverandører med omhu. I takt med at større organisationer afsætter flere ressourcer til at beskytte sig, bl.a. som følge af nye lovkrav som NIS2, vil underleverandører være eftertragtede byttedyr, hvis det kan være en nem indgang til et større.

Cyberaktivismen fortsætter
Cyberaktivismen er fremherskende og bliver ved med at være det, men der kan være håb om, at medier og aktører kan blive enige om at tie det ihjel. DKCERT har truffet beslutning om ikke offentligt at omtale DDoS-angreb på egne tjenester og har opfordret uddannelses- og forskningsinstitutioner til det samme.

Selv om cyberaktivisme er et våben i hybridkrigen, som næppe forsvinder foreløbigt, er ønsket, at aktører beslutter at betragte overbelastningsangreb som en driftshændelse og dermed ignorerer cyberaktivisternes ambitioner om at bruge DoS-angreb som et forsøg på destabilisering. Inden for sportens verden er der konsensus blandt producenter af større sportsbegivenheder om at undlade at vise TV-billeder af aktivister, der obstruerer cykelløb, fodboldkampe mv. Herved mister aktivismen sin gennemslagskraft og kan flade ud.

5. Trends og anbefalinger

De klassiske metoder går igen
I betragtning af, hvor hurtig udviklingen inden for cybersikkerhed og cyberusikkerhed løber, kan man undre sig over, at angrebsmetoderne grundlæggende er de samme. Vi ser stadig DoS-angreb, phishingangreb er fortsat de cyberkriminelles foretrukne angrebsmetode, cross site scripting på websider og DNS spoofing, hvor brugere omdirigeres til falske hjemmesider, sker i stor stil, mens ransomware vedbliver med at være en stor økonomisk driver. Forventningen er, at metoderne fortsætter deres ridt, men til gengæld kan de bagvedliggende strukturer med kriminalitetssyndikater, spionageringe og aktivistgrene i højere grad manifestere sig inden for de forskellige trusselskategorier.

5.2 TRENDS I EU-DATAREGULERING

Revision af Persondataforordningen
Persondataforordningen trådte i kraft den 18. maj 2018. I juni 2020 kom den første mindre evalueringsrapport om Persondataforordningen fra Europa-kommissionen. Rapporten fandt, at det ville være 'forhastet' at overveje eventuelle ændringer, navnlig i betragtning af Persondataforordningens succes '..som et centralt referencepunkt på internationalt plan, hvor den fungerede som katalysator for at mange lande rundt om i verden begyndte at overveje at indføre moderne regler om privatlivets fred'.[81]

I maj 2024 forventes den første større revision af Persondataforordningen foretaget af Kommissionen. Spørgsmålet er, om det denne gang vil føre til en revidering af Persondataforordningen og i givet fald på hvilket område. Flere emner har været diskuteret, bl.a. dataforordningens byrde for små og mellemstore organisationer.

[81] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

5. Trends og anbefalinger

Harmoniseringsspørgsmålet i forhold til, hvordan de forskellige EU-lande fortolker og implementerer databeskyttelse, har også længe været til debat. I 2020 besluttede Det Europæiske Databeskyttelsesråd (EDPB) derfor at nedsætte et udvalg til udarbejdelse af en koordineret håndhævelsesramme. Udvalgets sidste rapport kom den 16. januar 2024 og omhandlede databeskyttelsesrådgiverens (DPO) udpegning og funktion i de forskellige lande.

Rapportens konklusion var, at de nationale datatilsyn blev anbefalet en række tiltag for at opfylde den rolle databeskyttelsesrådgiveren oprindeligt var tiltænkt i Persondataforordningen. Eksempelvis blev det anbefalet at indføre kontroller for at sikre, at der bliver udnævnt en DPO, at DPO'er bliver givet tilstrækkeligt ressourcer til udførelse af deres opgaver, at DPO'er får den nødvendige uddannelse og træning, og at de nationale datatilsyn giver den nødvendige rådgivning.

Der er mange måder at opnå harmonisering, men en af de første opgaver er at sikre, at der er en ensartet fortolkning af lovgivningen hos samtlige instanser. EDPB opfordrer EU-lovgiverne og EU-Kommissionen til at arbejde hen imod større klarhed og ensartethed med hensyn til de nye roller og beføjelser, som tilsynsmyndighederne og EDPB har fået tildelt i henhold til ny lovgivning. EDPB opfordrer også til, at der træffes de nødvendige foranstaltninger for at sikre, at tilsynsmyndighederne og EDPB har tilstrækkelige ressourcer.[82]

AI-implikationer for databeskyttelse
Den 8. december 2023 indgik Europa-parlamentet og lovgivere en aftale om reglerne for kunstig intelligens. Aftalen skal føre til en AI-forordning (AI Act), som er det første regelsæt i verden, der regulerer reglerne for kunstig intelligens.

Den foreløbige politiske aftale skal i den kommende tid konkretiseres og justeres yderligere, før den overgår til lovgivningsmæssig behandling og vedtagelse af Ministerrådet og Europa-parlamentet.

Den midlertidige aftale fastslår, at AI-forordningen skal træde i kraft to år efter vedtagelsen, med visse undtagelser for specifikke bestemmelser, der vil gælde allerede efter seks måneder. Dette omfatter bl.a. reglerne om forbud mod visse AI-systemer, der vurderes til at have uacceptable risici. Det gælder fx AI-applikationer, der er uforenelige med EU's værdier og grundlæggende rettigheder, fx systemer der arbejder med følelsesgenkendelse.[83]

I forhold til databeskyttelse har Datatilsynet allerede udarbejdet den første vejledning i emnet i forhold til offentlige myndigheders brug af AI. I vejledningen behandles bl.a. spørgsmål om behandlingsgrundlag, oplysningspligt og konsekvensanalyse.[84]

Hvor de første reaktioner på AI-systemerne har været en blanding mellem begejstring og frygt/bekymring, er forventningen, at fremtiden vil byde på nye måder, hvorpå AI i praksis kan anvendes. Dette vil også omfatte de muligheder, AI kan give for at fremme databeskyttelse.

Et umiddelbart eksempel på, at AI kunne fremme databeskyttelse, er i forhold til opgaven med at forbedre og administrere data ved nøjagtigt at identificere følsomme data. Denne opgave starter med at finde, katalogisere og beskytte variationer af meget følsomme, begrænsede og unikt identificerbare data på tværs af fx en organisation. Traditionelle tilgange til dataopdagelse, filanalyse og klassificering kan være støjende, fuld af falske positiver, siloer og svære at skalere. Måske kan AI blive det værktøj, der kan gøre processen lettere i stedet for alene den trussel mod databeskyttelse, der har været meget fokus på.

82 https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en
83 https://dm.dk/akademikerbladet/aktuelt/ai/2023/eu-vil-forbyde-kunstig-intelligens-der-manipulerer-med-din-hjerne/
84 https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/okt/ny-vejledning-om-offentlige-myndigheders-brug-af-ai-og-kortlaegning-af-ai-paa-tvaers-af-den-offentlige-sektor

5. Trends og anbefalinger

Dataoverførelser og tilstrækkelighedsafgørelser
Kommissionen har udstedt 15 tilstrækkelighedsafgørelser. Den 15. januar 2024 meddelte Kommissionen, at 11 har været underlagt tilsyn, og at de opretholder deres tilstrækkelighedsafgørelse. Der kan således frit overføres data fra EU/EØS til Andorra, Argentina, Canada, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz og Uruguay, da de fortsat er sikret et tilstrækkeligt beskyttelsesniveau.[85]

Dataoverførsel til USA vil forsat være et tema i 2024. Kommissionen har allerede bestemt, at tilstrækkelighedsafgørelsen fra 10. juli 2023, bedre kendt som The EU-US Data Privacy Framework, skal evalueres til sommer.[86] Tilstrækkelighedsafgørelsen og den planlagte evaluering forventes ikke at ville stoppe Max Schreems i at indbringe tilstrækkelighedsafgørelsens lovlighed for EU-domstolen.[87]

Ny digital lovgivning
Den 11. januar 2024 trådte EU Data Act i kraft, men vil først blive håndhævet fra 12. september 2025. Lovgivningen har fået mindre mediebevågenhed end AI Act, men er ikke desto mindre endnu et eksempel på den stadige strøm af ny lovgivning, der er på området.

Formålet med loven er at sikre forbedring af adgangen til data på EU-markedet for enkeltpersoner og virksomheder. I de senere år har Internet of Things (IoT) givet næring til hurtig vækst i mængden af data derude. De nye regler tilskynder til anvendelse af data og sikrer, at de deles, lagres og behandles under fuld overholdelse af EU-reglerne.

Udviklingen af den digitale lovgivning har flere retninger. Indtil videre har der været et fokus på lovgivning i forhold til borgers (den registreredes) eller forbrugers rettigheder og beskyttelse. Det forventes, at den fremtidige digitale lovgivning også vil udvikle sit scope, således at lovgivning om teknologiens miljøpåvirkning eller mere sektorafgrænset lovgivning kunne blive aktuel.[88]

[85] https://www.datatilsynet.dk/internationalt/tredjelandsoverfoersler
[86] https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
[87] Max Schreems er grundlægger af NOYB (My privacy is 'Non of your business') og kendt for at kæmpe mod overførsel af data fra Facebooks europæiske brugere til USA.
[88] https://www.trail-ml.com/eu-ai-act-readiness?gclid=CjOKCQiAtaOtBhCwARIsAN_x-3I75zDy1giVjEeVautyBLsqSeGmtm-51Bo-DbROFfCKkFpLTahTyAdMaAiKnEALw_wcB

5. Trends og anbefalinger

5.3 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. Integrér 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 en læringsstrategi for studerende og ansatte, før studiestart og ansættelse.
6. Evaluér læringsstrategien og monitorér efterlevelsen af retningslinjer for informationssikkerhed i organisationen.
7. Tag stilling til risikoen for, at ansatte, studerende mv. bliver udsat for påvirkningskampagner og rekrutteret til fx. cyberspionage. Iværksæt 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 og prioritér at deltage i beredskabsøvelser.
10. Hav opmærksomhed på, at værdikædeangreb ikke nødvendigvis har med it at gøre. Særligt i forhold til spionagetruslen vil der altid være et element, der ikke kan beskyttes vha. tekniske it- og cybersikkerhedsmæssige foranstaltninger.

5. Trends og anbefalinger

5.4 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 følgende:

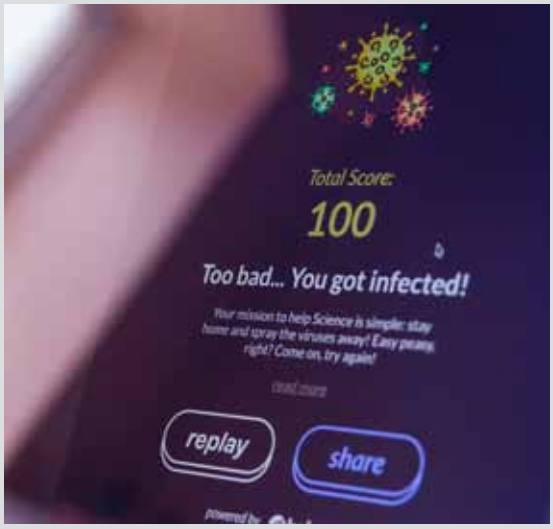
1. Lær informationssikkerhedspolitikken og lokale retningslinjer at kende.
2. Vær bevidst om værdien af arbejdet og konsekvenserne ved kompromittering af fortrolighed, integritet og tilgængelighed.
3. Tænk på om arbejdsområder er tilstrækkeligt beskyttet i forhold til værdien – både digitalt og fysisk.
4. Vær opmærksom på påvirkningskampagner og italesæt, hvordan det påvirker jeres arbejde.
5. Hjælp dine kolleger med høj informationssikkerhed og understøt dialog om informationssikkerhed som en del af hverdagen.

5.5 ANBEFALINGER TIL IT-ANSVARLIGE PÅ UDDANNELSES- OG FORSKNINGSINSTITUTIONERNE

DKCERT anbefaler, at institutionens informationssikkerhedsansvarlige sammen med ledelsen og repræsentanter for forretningen udarbejder risikovurderinger af alle processer og anskaffelser som grundlag for 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. Få hjælp af kommunikationseksperter til læringsrettede tiltag på sikkerhedsområdet og til målinger af tiltagenes virkning.
3. Tænk sikkerhed ind i forholdet til leverandører og samarbejdspartnere og følg op med regelmæssige kontroller.
4. Hav fokus på sikkerheden ved udvikling af applikationer og tjenester samt tilretninger af eksisterende systemer, 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 og undgå i muligt omfang anvendelsen af passwords, dvs. implementer passwordless indlogningsmetoder.
6. Tilbyd en passwordmanager til de ansatte og studerende i det omfang, der stadig anvendes passwords som autentifikationsfaktor.
7. Vær bevidst om at et vellykket angreb på én uddannelses- og forskningsinstitution sandsynligvis vil blive prøvet på en anden instution.
8. Overvej nødvendigheden af brug af persondata og beskyttelse af disse ved implementering af nye systemer. Vær opmærksom på princippet om dataminimering, jf. GDPR.
9. Afsæt ressourcer til deltagelse i og anvendelse af sektorens fælles tjenester, herunder beredskabsøvelser.
10. Overvej om 'antag kompromittering'-tilgangen skal indgå i organisationens sikkerhedstænkning og om der skal udarbejdes en strategi, der adresserer det.

6. Referenceliste



Academic Security SIG
Academic Security SIG er et netværk for den akademiske verden organiseret under FIRST. Academic Security SIG sigter mod at være en platform for samarbejde mellem akademiske sikkerhedsteams mhp. deling af erfaringer om aktuelle sikkerhedsproblemer. Netværket 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.

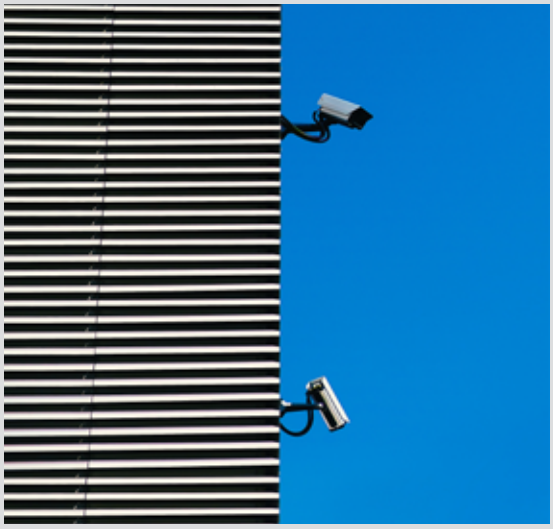
DKCERT har fra grundlæggelsen i 1991 som sikkerhedsteam for Forskningsnettet – siden 2012 en del af DeiC - været autoriseret til at kalde sig CERT. DKCERTs officielle navn er Danish Computer Security Incident Response Team.

Der er CSIRT-teams i over 100 lande i verden over (se FIRST 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
Center for Cybersikkerhed blev etableret i 2012 som en del af Forsvarets Efterretningstjeneste. Organisatorisk er Center for Cybersikkerhed en af seks sektorer i Forsvarets Efterretningstjeneste.

6. Referenceliste



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 Center for Cybersikkerhed i Danmark.

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. CISO-forum har til formål at koordinere og udveksle viden og erfaringer om aktuelle udfordringer for sikkerheden på forskningsnettet og universiteterne mellem universiteternes informationssikkerhedschefer og -koordinatorer.
Chefen for DKCERT har hidtil haft observatørstatus i CISO-forum.

DCIS
Den Nationale Strategi for Cyber- og Informationssikkerhed 2022-2024 beskriver bl.a., at der skal udarbejdes sektorstrategier og oprettes decentrale cyber- og informationssikkerhedsenheder (DCIS) for alle samfundsvigtige funktioner, der er digitalt understøttet.

En 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 nu 26 DCIS'er, der koordineres af CFCS, herunder en i Uddannelses- og Forskningsstyrelsen (DCIS-UFM). Internationalt kan det danske begreb DCIS nærmest sammenlignes med et 'ISAC', et 'Information Sharing and Analysis Center's.'

6. Referenceliste

DeiC
DeiC står for Danish e-Infrastructure Consortium. DeiC udvikler og koordinerer samarbejdet om digital forskningsinfrastruktur mellem universiteter, der er omfattet af universitetsloven. DeiCs vision er, at forskere ved de danske universiteter skal have adgang til en digital infrastruktur, der muliggør forskning og uddannelse på højt internationalt niveau. Øvrige relevante institutioner med uddannelses- og forskningsaktiviteter kan deltage i samarbejdet efter godkendelse af DeiCs bestyrelse.

DeiCs juridiske grundlag er beskrevet i bekendgørelse BEK 615 af 26. maj 2023, som bl.a. bestemmer, at DeiC træffer beslutning om udvikling og drift af fælles forskningsnetværk, fælles digitale infrastrukturtjenester, fælles cyber- og informationssikkerhedsydelser samt fælles beregnings- og lagringsfaciliteter for de danske universiteter og øvrige relevante institutioner.

ENISA
ENISA er Den Europæiske Unions Agentur for Cybersikkerhed. ENISA bidrager til EU's 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.

FIRST
FIRST står for Forum for Incident Response and Security Team og er en organisation, der organiserer en lang række CERT/CSIRT/PSIRT-teams fra det meste af verden. Pr. 1. marts 2024 er 718 medlemsteams fra 108 lande, heraf 11 fra Danmark. FIRSTs sekretariat er hjemmehørende i USA. DKCERT blev i 1993 som et af de første teams uden for USA medlem af FIRST.

Forskningsnettet
Forskningsnettet er et højhastighedsnetværk, grundlagt 1987, der forbinder danske universiteter og forskningsinstitutioner. Siden 2012 drives det af DeiC.

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

6. Referenceliste

internet. DeiC er medlem af GÉANT gennem NORDUnet og deltager i en række projekter og samarbejder under GÉANT.

NREN
NREN står for National Research and Education Network. DeiC Forskningsnettet er den danske NREN.

NORDUnet
NORDUnet er et fællesnordisk samarbejde om drift af nordisk og international e-infrastruktur og tjenester mellem forsknings- og uddannelsesnetværk i Danmark, Finland, Island, Norge og Sverige.

Nordisk forskningsnet-CERT-samarbejdet
Samarbejdet er et netværk af CERT'erne for de fem nordiske forskningsnet: Sunet (Sverige), Funet (Finland), SIKT (Norge), RHnet (Island) og DeiC Foskningsnettet samt NORDUnet CERT. Netværket mødes til onlinemøder ca. en gang hver 4.-6. uge samt til et årligt fysisk møde.

Open CSIRT Foundation
Open CSIRT Foundation (OGF) er en uafhængig NGO, grundlagt i 2016. OCFs mission er at forbedre cybermodstandskraften på verdensplan. Siden juli 2022 har OCF koordineret TF-CSIRT, som består af medlemmer af Trusted Introducer.

SIE Europe
SIE Europe er et europæisk samarbejde, der har til formål at bekæmpe cyberkriminalitet og dermed gøre den digitale økonomi mere stabil og sikker. SIE Europe driver et delingshub, som modtager passive DNS-data i realtid fra de deltagende organisationers pDNS-sensorer, hvorved de får adgang til aggregerede data fra alle øvrige deltagere.

SIG-ISM (GÉANT)
SIG-ISM er GÉANTs 'special interest group' for CISO'er og tilsvarende for de nationale forskningsnet (NREN). 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 fire-seks gange om året.

TF-CSIRT
TF-CSIRT (Task Force Computer Security Incident Response Teams) er et forum for sik-

6. Referenceliste

kerhedsteams, der står i Trusted Introducers database. Oprindeligt, dvs. fra 2000-2022, var TF-CSIRT organiseret under de europæiske forskningsnetværks paraplyorganisation GÉANT. Fra juli 2022 koordineres TF-CSIRT af The Open CSIRT Foundation.

De nu mere end 500 medlemmer er organisationer, der håndterer sikkerhedshændelser. I regi af TF-CSIRT mødes medlemmerne med ligesindede og diskuterer 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 hændelser, med at samarbejde dermed forbedre sikkerheden gennem hurtigere respons 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 (SIM-3), 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 2024 certificeret medlem. 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.

DKCERT/DeiC
DTU, Produktionstorvet
Bygn. 426
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