DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed

Kolofon

DKCERT Trendrapport 2022

Redaktion: Henrik Larsen og Eskil Sørensen, DKCERT.

Tak til vores bidragydere:
Henrik Kramselund Jereminsen, adjunkt, KEA – Københavns Erhvervsakademi
Mikkel Nilsson, Chef for produkt, Cyber, Tryg
Linda Mostrup Pedersen, Founding Partner, Happy42
Jens Myrup Petersen, professor, Aalborg Universitet
Christian Damsgaard Jensen, lektor, Danmarks Tekniske Universitet
Jan Kaastrup, Chief Technology Officer, CSIS Security
Jack Glenn Hjortholm, DKCERT
Henrik Jensen, DKCERT
Carina Lis Lamb, DKCERT

Design og layout: Kiberg & Gormsen

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

Om DKCERT

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

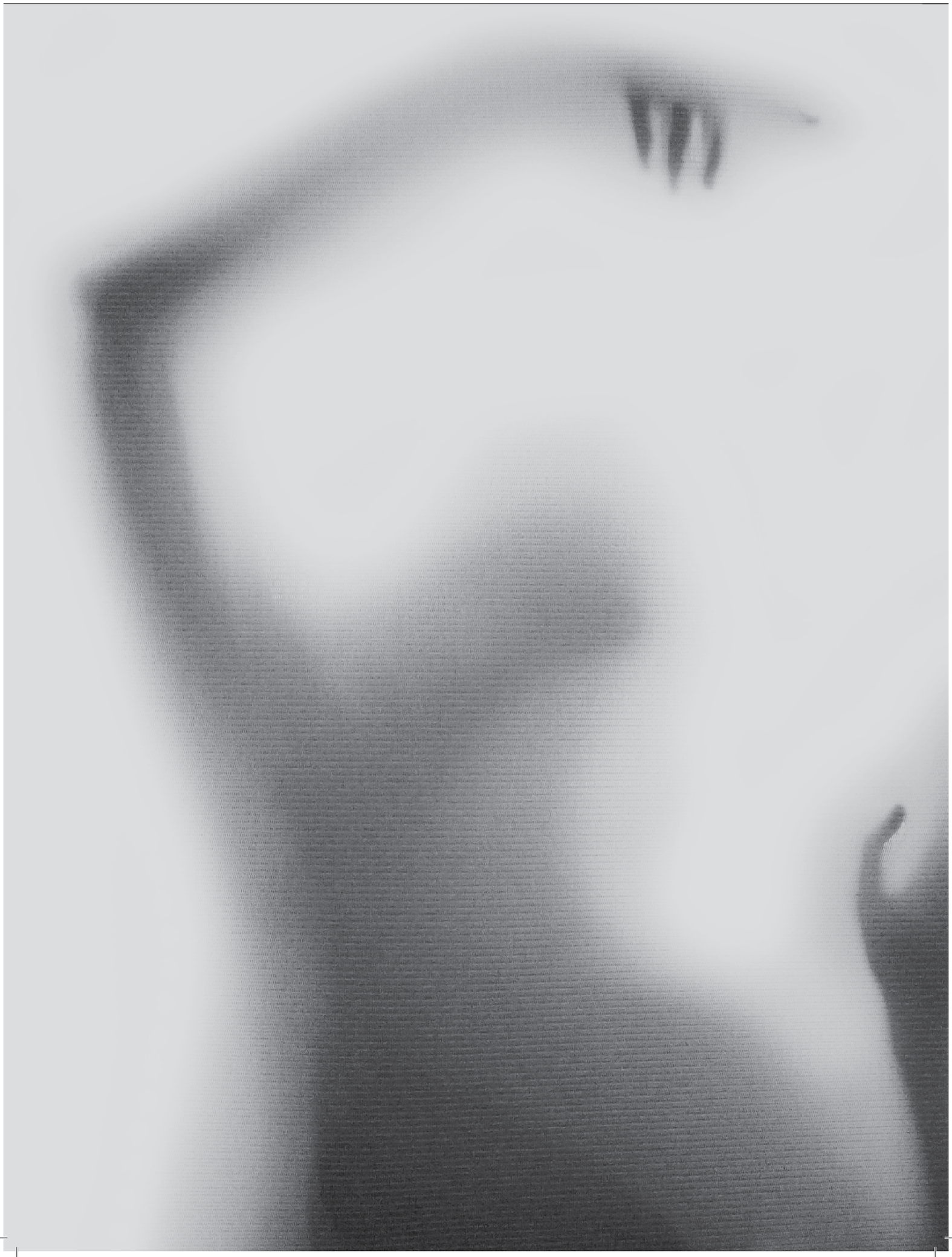
Det er DKCERTs mission at skabe øget fokus på informationssikkerhed i uddannelses- og forskningssektoren ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DKCERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DKCERT overvåger det danske forskningsnet for uønskede aktiviteter, sender advarsler ud til uddannelsesinstitutionerne, indsamler oplysninger om sårbarheder og foretager sårbarhedsscanninger af forskningsnettet og 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 Cooperation. DeiC understøtter Danmark som e-science-nation gennem levering af e-infrastruktur (computing, datalagring og netværk) til forskning og forskningsbaseret undervisning. DeiC er en enhed under Uddannelses- og Forskningsministeriet etableret ved aktstykke 70 fra den 19. april 2012.

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, samt siden 2002 akkrediteret medlem af Trusted Introducer og TF-CSIRT (Task Force Computer Security Incident Response Team) under GÉANT.



Indholdsfortegnelse

1. Velkomst

Velkommen til DKCERTs TRENDRAPPORT 2022.

Manglen på arbejdskraft med it- og sikkerhedskompetencer er stor. Ikke kun i et digitaliseringsforegangsland som Danmark. Også i resten af verden har der i flere år været efterspurgt arbejdskraft, der kan være med til at løse udfordringerne med cyber-, it- og informationssikkerhed.

Udfordringer, som dels er opstået som følge af en hastigt voksende digitalisering af både offentlig og privat sektor, dels som følge af et kriminalitetsmarked, der har set store forretningsmuligheder i at finde, bearbejde, forarbejde og sælge ulovligt fremskaffet data. Udfordringerne er i endnu højere grad blevet aktualiseret af den tragiske krig i Ukraine, som akut har medført et endnu større pres på kompetencepuljen. Dette pres vil utvivlsomt blive forstærket yderligere i kraft af det Nationale Kompromis om dansk sikkerhedspolitik fra marts 2022, der givetvis også vil medføre ekstra investeringer i cybersikkerhed.

I årets trendrapport har vi valgt at sætte fokus på uddannelse og kompetencer. Vi bringer indlæg fra eksterne eksperter, der er ansvarlige for eller har gennemført uddannelser inden for cyber-, it- og informationssikkerhed. Vi går fra masteruddannelsen på DTU til en indsats, der søger at skabe nogle faglige miljøer og fællesskaber mellem de unge, der tager en cybersikkerhedsuddannelse. Og vi ser også et et nyt tiltag, der henvender sig til medarbejdere uden uddannelsesmæssig faglighed inden for cybersikkerhed, som kan være ambassadører i virksomheder.

Viden og forskning som samfundsvigtig funktion
Regeringen adresserer netop styrkelse af samfundets adgang til it-sikkerhedskompetencer som en strategisk indsats i den nye nationale cyber- og informationssikkerhedsstrategi, der udkom kort før jul .[1] Fastholdelse og rekruttering af kompetencer er ikke alene en udfordring, som myndigheder og virksomheder møder dagligt. Det kan også være et problem i forhold til ønsket om robust beskyttelse af de såkaldte samfundsvigtige funktioner, som det hedder i strategien.

Introduktionen af samfundsvigtige funktioner som et centralt element markerer et skifte i forhold til den tidligere strategi. Den havde de samfundskritiske infrastruktursektorer, energi, sundhed, trans-

[1] https://digst.dk/strategier/cyber-og-informationssikkerhed/

1. Velkomst

port, søfart, finans og tele i fokus, men nu er det mere den brede betegnelse i samfundsvigtige funktioner, der lægges vægt på. Ifølge strategien skal hvert ministerområde kortlægge, hvilke funktioner inden for ministerområdet, der er samfundsvigtige og digitalt understøttede. Ministerområderne skal ydermere etablere en decentral cybersikkerhedsenhed, der skal koordinere cybersikkerheden i disse områder og udarbejde en cyber- og informationssikkerhedsstrategi herfor. Pointen med dette er, at det skal sikres, at funktionerne kan opretholdes i en krisesituation, hvor fx kritisk it-infrastruktur sættes ud af kraft i kortere eller længere tid. Viden og forskning inden for en lang række emner kan ses som samfundsvigtige funktioner, som dermed får en langt større bevågenhed end tidligere. Vi har netop i coronakrisen erfaret, hvor vigtig forskning er for et samfund i en krisesituation. Uden egen forskning i og dataindsamling om corona havde Danmark næppe klaret sig så godt igennem krisen, som der er almindelig enighed om.

At være en samfundsvigtig funktion betyder til gengæld også langt større krav til sikkerheden end tidligere, fx efterlevelse af ISO27001 og tekniske minimumskrav, som den øvrige statslige sektor også er underlagt. Det bliver et arbejde, som sektoren skal i gang med allerede her i 2022 – og et arbejde som DKCERT forventer at blive inddraget i. Ikke mindst fordi vi har som opgave at understøtte sektorens informationssikkerhed. Hvordan, vi gør det og har gjort i 2021, fortæller vi om i trendrapporten.

Trendrapportens opbygning
Trendrapporten 2022 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 2021 og de tjenester, vi stiller til rådighed for sektoren. Vi giver bl.a. en status på sektorens MISP og de observationer, vi kan se ud fra vores sårbarhedsscanninger. I kapitel 4 fortæller vores eksterne bidragydere om deres uddannelser til de forskellige målgrupper, de henvender sig til, mens vi i kapitel 5 gennemgår vi trends, vi ser inden for databeskyttelses- og cyber- og informationssikkerhedsområdet og de anbefalinger, vi anser for at være de vigtigste at bringe videre til sektoren.

Rigtig god fornøjelse med læsningen.

Henrik Larsen
Chef for DKCERT

2. Trusselsvurdering 2022

2. Trusselsvurdering 2022

Cybertruslen mod den danske uddannelses- og forskningssektor

Danmark har generelt et højt niveau inden for it, teknologi og forskning. Denne position gør os dels sårbare overfor cyberkriminelle angreb, dels kan den udnyttes af uautoriserede til at få indsigt i danske forskningsresultater. I kraft af dette, det sikkerhedspolitiske billede og DKCERTs vidensindsamling vurderes den generelle cybertrussel mod sektoren til at være MEGET HØJ.[2]

Angreb eller forsøg på angreb mod danske universiteter og forskningsinstitutioner registreres dels gennem oprettede sager hos DKCERT og dels gennem DKCERTs fælles platform til registrering af sikkerhedsmæssige hændelser, som baserer sig på anvendelsen af MISP[3]. I de registrerede hændelser på universitetsområdet ser DKCERT blandt andet tendenser til, at der i høj grad prøves at opnå uautoriseret adgang til universiteterne og forskningsinstitutioners digitale løsninger.

Ifølge PET[4] er der set eksempler på, at '..fremmede stater uretmæssigt anskaffer sig viden om teknologi og produkter, som Danmark skal leve af på sigt, eller som kan have en negativ indflydelse sikkerhedspolitisk.' Truslen er reel, og gennem de senere år har der været eksempler på spionage og anden udenlandsk indblanding, ligesom vi på daglig basis ser diverse former for cyberkriminelle angreb.

Covid-19 epidemien og krigen i Ukraine har forstærket opmærksomheden på betydningen af forskning og viden.

2.1. HOVEDVURDERINGER

- Truslen fra cyberspionage mod den danske uddannelses- og forskningssektor er MEGET HØJ. Fremmede stater og kriminelle har stor interesse i at stjæle forskningsdata og intellektuel ejendom fra sektoren.
- Truslen fra cyberkriminalitet er MEGET HØJ. Der er meget sandsynligt, at cyberkriminelle angreb kan forstyrre den daglige drift eller skade forskningsdata.
- Truslen fra cyberaktivisme er LAV. Truslen er ofte motiveret af enkeltsager, og truslen mod sektoren kan derfor stige uden eller med kort varsel.
- Truslen for at fremmede stater vil rette destruktive cyberangreb mod dansk samfundsvigtig infrastruktur, herunder uddannelses- og forskningssektoren er LAV. Som følge af krigen i Ukraine kan truslen mod uddannelses- og forskningssektoren stige uden eller med kort varsel.
- Truslen fra menneskelige fejl mod uddannelses- og forskningssektoren er MEGET HØJ.[5] Der er manglede opmærksomhed på truslen og konsekvenserne heraf, hvilket øger sandsynligheden for menneskelige fejl, uanset om disse er begået af ubevidste, uagtsomme eller uvederhæftige medarbejdere.

Disse konklusioner bygger på indsamlede oplysninger fra både eksterne kilder og egne kilder, herunder oplysninger fra institutioner og samarbejdspartnere. DKCERTs vurdering baserer sig på en samlet analyse af disse oplysninger. For sammenlignelighedens skyld er anvendt samme skala og definitioner, som benyttes af Center for Cybersikkerhed (CFCS) der i publikationen 'Cybertruslen mod dansk forskning og universiteter' giver tilsvarende vurderinger.[6]

Til denne trusselsvurdering har DKCERT yderligere anvendt Data Breach Investigations report fra Verizon[7] og data fra European Union Agency for Cybersecurity (ENISA), der bl.a. analyserer cyber- og informationssikkerheden inden for EU.

2 Cybertrusler defineres som trusler, der påvirker stabiliteten (tilgængelighed, fortrolighed og integritet) af de digitale tjenester, der stilles til rådighed af de danske universiteter og forskningsinstitutioner.

3 Open Source Threat Intelligence and Sharing Platform, tidligere kendt som Malware Information Sharing Platform. Se afsnit 3.3.5

4 https://www.pet.dk/Nyheder/2021/~/media/Publikationer/PETpublikationforskningDKdigitalversionpdf.ashx

5 Se afsnit 2.2.8

6 https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/forskning-og-universiteter/

7 https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

2. Trusselsvurdering 2022

2.2. TRUSLER

ENISA udgiver jævnligt publikationer, som belyser de aktuelle cyber- og informationssikkerhedsmæssige trusler med relevans for EU. I den seneste rapport fra oktober 2021, som dækker perioden april 2020 til midtjuli 2021, refereres til et trusselslandskab (ETL - ENISA Threat Landscape),[8] hvor de identificerede primære cyber- og informationssikkerhedsmæssige trusler er:

- Ransomware
- Malware
- Cryptojacking
- E-mailrelaterede trusler
- Trusler mod data
- Trusler mod tilgængelighed og integritet
- Disinformation – misinformation
- Ikke-ondsindede trusler
- Supply chain-angreb

Hvad angår tendenser, fremhæver rapporten følgende:

- Ransomware er blevet vurderet som den primære trussel for 2020-2021
- Statslige aktører har optrappet aktiviteterne på både nationalt og internationalt plan
- Cyberkriminelle motiveres i stigende grad af økonomiske motiver, som fx ransomware kan understøtte
- Kryptovaluta er fortsat den mest almindelige udbetalingsmetode for trusselsaktører
- Faldet i mængden af malware fortsætter, men er stadig en trussel
- Mængden af cryptojacking-infektioner nåede rekordhøjder i første kvartal af 2021 sammenlignet med de seneste år
- COVID-19 er stadig det dominerende lokkemiddel i kampagner for e-mailangreb (phishing)
- Traditionelle DDoS-kampagner (Distributed Denial of Service) i 2021 er mere målrettede, mere vedholdende og i stigende grad baseret på flere forskellige angrebsvektorer (multivektor).

At forstå tendenserne relateret til trusselsaktørerne, deres motiver og deres mål, kan i høj grad hjælpe til med planlægningen af et robust cyber- og informationssikkerhedsforsvar. Oftest er metoderne fra trusselsaktørerne de samme uagtet motiv. Fx kan et brud på fortroligheden af personlige data bruges til afpresning. Det kan også bruges til identitetstyveri og gemmes til senere brug, fx til spearphishingangreb.

I det efterfølgende har vi tegnet et billede af, hvordan de nævnte angreb anvendes.

2.2.1. Ransomware

Ransomware er en form for ondsindet angreb, hvor angribere krypterer en organisations data og kræver betaling for at gendanne adgang til filer og/eller diskdrev. I nogle tilfælde kan angribere også stjæle en organisations oplysninger og kræve yderligere betaling for ikke at videregive oplysningerne til konkurrenter eller offentligheden. NIST har udarbejdet et udkast til at profilere ransomwareangreb. Profilen identificerer og understøtter forebyggelse, reaktion på og gendannelse efter ransomwarehændelser. Profilen kan bruges som en guide til at håndtere ransomwarehændelser. Det inkluderer hjælp til at måle en organisations niveau af parathed til at imødegå ransomware og til at håndtere de potentielle konsekvenser af begivenheder.[9]

Phishing e-mails og bruteforce på Remote Desktop Protocol (RDP) tjenester udgør de to mest almindelige angrebsvektorer. En række hackergrupper som fx Conti og REvil leverer ransomware-as-a-service (RaaS), hvorigennem betalende kunder kan iværksætte deres angreb. Forretningsmodeller af denne type er stærkt stigende. Motivet er udelukkende økonomisk.

2.2.2. Malware

Malware er et paraplyudtryk, der beskriver enhver software, firmware eller kode, der er beregnet til at udføre en skadelig handling eller uautoriseret proces, som vil have en negativ indvirkning på et systems fortrolighed, integritet eller tilgængelighed.

Eksempler på malware kan være en virus, orm, trojansk hest eller andre kodebaserede enheder, der inficerer en vært. Spyware og nogle former

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[9] https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf

2. Trusselsvurdering 2022

for adware er også en del af malware-termen. Malware kan have forskellige formål, alt efter hvad angriberen havde tænkt sig med malwaren. For eksempel er RAT (Remote Access Trojan) en malware, der kan foretage fjernstyring af et inficeret system. 'Infostealere' eller 'skimmere' er designet til at fange kreditkortoplysninger. Botnets er et robotnetværk af computere inficeret med malware og kontrolleret af Comand and Control (C&C eller C2)-servere. Trojanere, som enten kan være en banktrojaner eller en mobil trojaner, igen afhængigt af målet, er malware, der ofte er forklædt som legitim software.

Truslen fra malware er en konstant med nye familier og stammer, der dukker op hvert år på trods af forskellige indsatser for at fjerne dem. Tendensen for truslen fra andet malware end ransomware er dog faldende.[10] Årsagen til dette kan være, at angribere flytter deres fokus til mere diskrete infektioner gennem IoT og e-mail.

2.2.3. Cryptojacking

Cryptojacking eller skjult kryptomining er en form for cyberkriminalitet, hvor en kriminel i al hemmelighed bruger et offers computer til at generere kryptovaluta. Dette sker normalt, når offeret uforvarende har installeret et program med ondsindede scripts, der giver hackeren adgang til en computer eller andre internetforbundne enheder, fx ved at klikke på et link i en e-mail eller ved besøg på et inficeret websted. Programmerne kaldet 'cryptominers' og bruges af den kriminelle til at udvinde kryptovalutaer.

ENISA har i sit Threatlandscape 2021 konstateret en voksende tendens inden for cryptojacking, som måske kan forbindes med en stigende volatilitet på kryptovalutamarkedet, der blev observeret i samme periode.[11] Desuden udveksles kryptovalutaer med en høj grad af anonymitet, hvilket er både attraktivt og bekvemt ved udveksling mellem cyberkriminelle. Cyberkriminelle afkræver som regel kryptovaluta som betaling i forbindelse med betaling af løsesum i forbindelse med ransomwareangreb. Cryptojacking-angreb er også set mod danske uddannelses- og forskningsinstitutioner.

[10] https://www.comparitech.com/antivirus/malware-statistics-facts/
[11] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (side 51)

2.2.4. E-mailrelaterede trusler og beslægtet social engineering

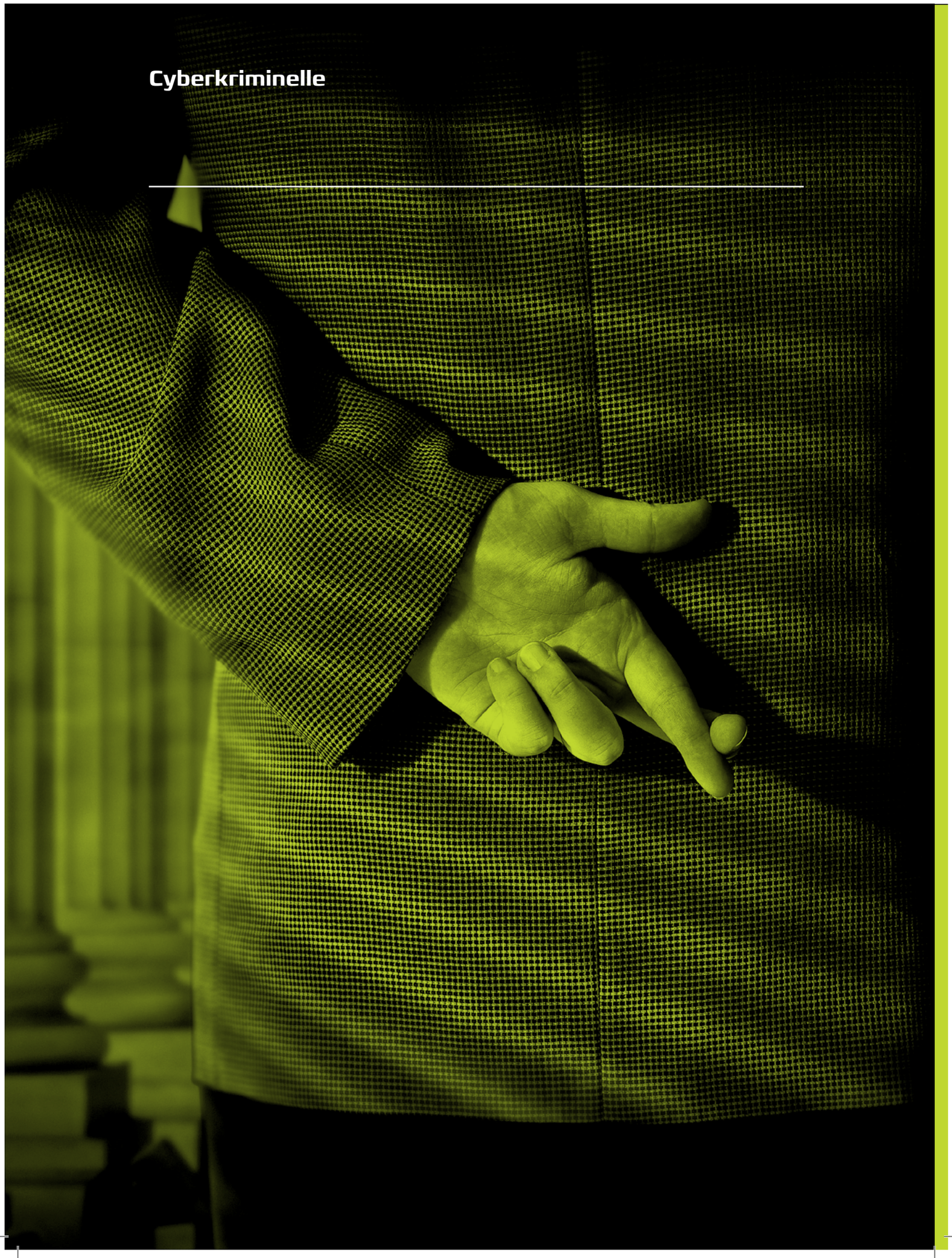
E-mailrelaterede trusler har i en årrække konsekvent ligget højt på listen over trusler. Truslerne udnytter svagheder i den menneskelige adfærd og har til formål at manipulere mennesker til at gennemføre handlinger, der i sidste ende gør dem til ofre for et angreb. E-mailrelaterede trusler handler generelt mindre om de tekniske sårbarheder i it-systemer, men mere om slutbrugerbevidsthed og udnyttelse af den iboende tillid, folk har til hinanden i forbindelse med e-mailkommunikation. Truslen består hovedsageligt af angrebsvektorerne: phishing, spearphishing, 'whaling', smishing, vishing, business e-mailcompromise (BEC).

Phishing sigter mod at stjæle vigtige oplysninger som kreditkortnumre og adgangskoder gennem e-mails, der involverer social manipulation og bedrag. Spearphishing er en mere sofistikeret version af phishing, der er rettet specifikt mod organisationer eller enkeltpersoner. Spearphishing kræver flere ressourcer at gennemføre og er derfor også mere avancerede enkeltangreb, mens almindelig phishing kan sammenlignes med at skyde med spredehagl. 'Whaling' er et spearphishing-angreb rettet mod brugere i høje stillinger (ledere, politikere osv.). Smishing, et udtryk afledt som en kombination af 'SMS' og 'phishing' forekommer, når oplysninger om ofre indsamles ved brug af SMS-beskeder.

En beslægtet type trussel er 'vishing', en kombination af phishing og stemme, der opstår, når information gives via telefon, hvor ondsindede aktører ved hjælp af social engineering-teknikker lokker følsomme oplysninger fra brugere.

Business e-mailcompromise (BEC), også kaldet 'direktørsvindel', er en raffineret metode rettet mod virksomheder og organisationer. Typisk vil cyberkriminelle prøve at lokke en mellemleder eller medarbejder til på vegne af topledelsen at foretage bankoverførsler til en angivelig legitim modtagers bankkonto. I virkeligheden tilhører disse bankkonti kriminelle bagmænd. Også forsøg på at få medarbejdere til at købe gavekort eller lignende på vegne af 'direktøren' eller 'bestyrelsesformanden' hører til i denne kategori.

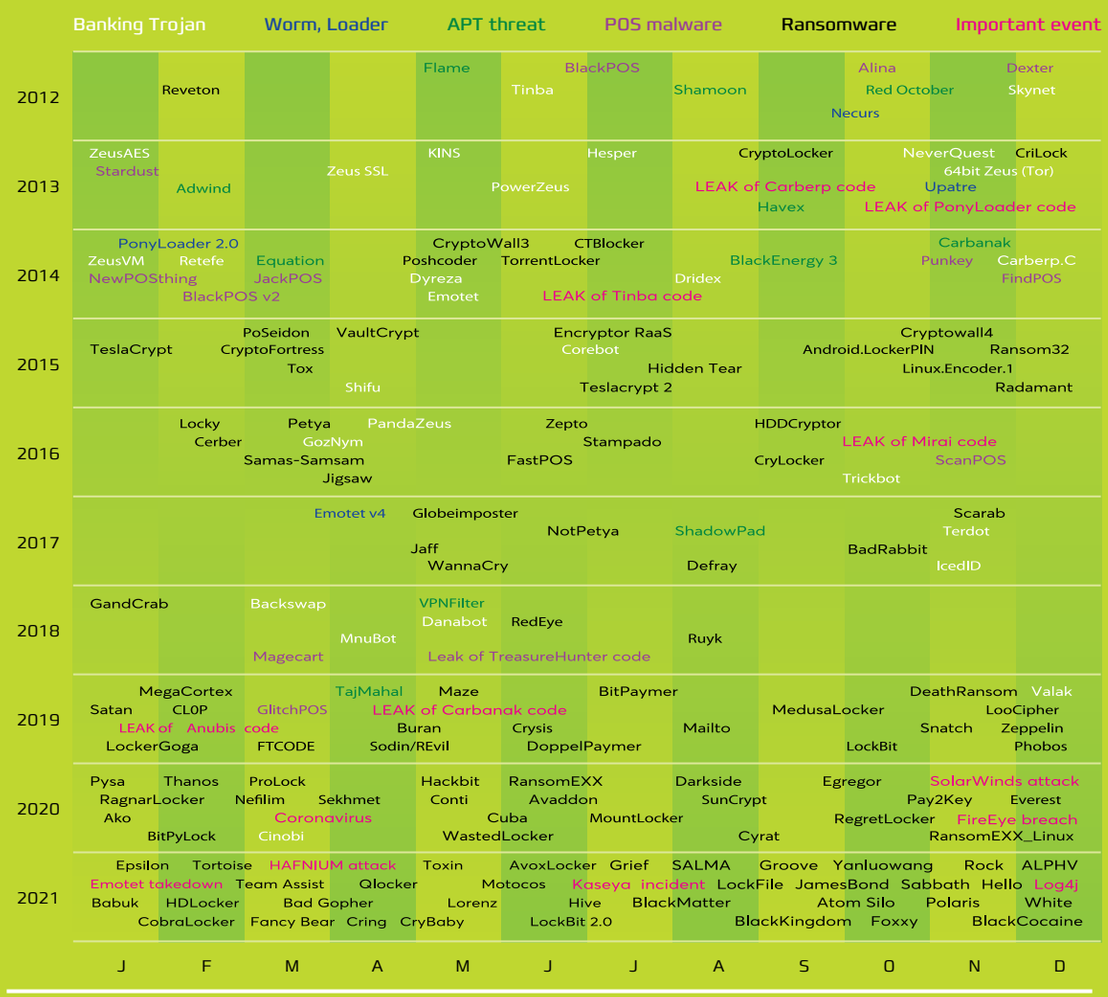
Cyberkriminelle



Cyberkriminelle

En konstant trussel i både freds- og krigstid.

Malware timeline 2012-2021 (Kilde CSIS)



Sikkerhedsfirmaet CSIS Security Group giver i sin H2 2021 Threat Matrix-rapport et indblik i trusselsbilledet og cyberkriminaliteten i andet halvår af 2021. Konklusionen er, at aktiviten inden for cyberkriminalitet har 'nået nye højder (..) både i forhold til kapacitet og den skadevirkning, der er forvoldt'. Det anføres, at der var ca fire gange så mange supply chain-attacks i 2021 i sammenligning med 2020. 2021 var også et rekordår for nye 0-dagssårbarheder, hvor der blev observeret dobbelt så mange 0-dagssårbarheder udnyttet 'in-the-wild' i 2021 i forhold til 2020.

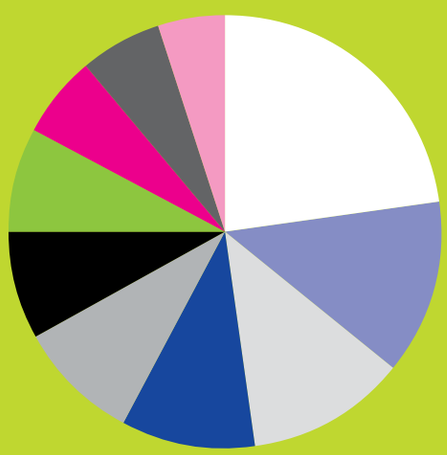
Dette kommer også til udtryk i udviklingen inden for større hændelser, som det fremgår af CSIS' optegnelse over internationale cybersikkerhedshændelser i de sidste ti år som det ses af skeamet ovenfor. Stigningen i malware er fortsat med stort kraft fra 2020 til 2021. Flere alvorlige og også i offentligheden kendte cybersikkerhedssager som fx Hafniumsårbarheden i Microsoft Exchangeserver, Kaseya-hændelsen, der påvirkede COOPs butikker i begyndelsen af juli og Log4j-sårbarheden i slutningen af december 2021, fremhæves som vigtige hændelser. Colonial Pipeline-hændelsen, hvor en olierørledning i USA blev udsat for ransomwareangreb, indgår ikke i opgørelsen. Årsagen til det er, at der var tale om et standardransomwareattack, hvor et kompromitteret kodeord blev anvendt for at opnå adgang til systemerne.

Cyberkriminelle

Top 10 phished brands

1	✶	Microsoft	23%
2	▲	Paypal	13%
3	▲	WhatsApp	12%
4	▼	Amazon	10%
5	▲	Facebook	9%
6	✶	Generic-Email Phish	8%
7	▼	Netflix	8%
8	✶	LabanQuepostale	6%
9	✶	Wellsfargo	6%
10	✶	Instagram	5%

Kilde CSIS

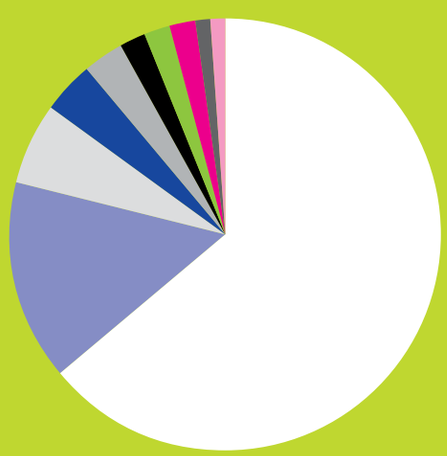


Changes in the last 6 months ✶ New ▬ Unchanged ▲ Moved up ▼ Moved down

Top 10 phishing hosts

1	▬	Hostinger	64%
2	▲	Cloudflare	15%
3	▬	Amazon	6%
4	▲	Lindex	4%
5	▲	Unified Layer	3%
6	▲	Microsoft	2%
7	▼	Digitalocean	2%
8	▬	Google	2%
9	▼	Namecheap	1%
10	✶	Cyrusone	1%

Kilde CSIS

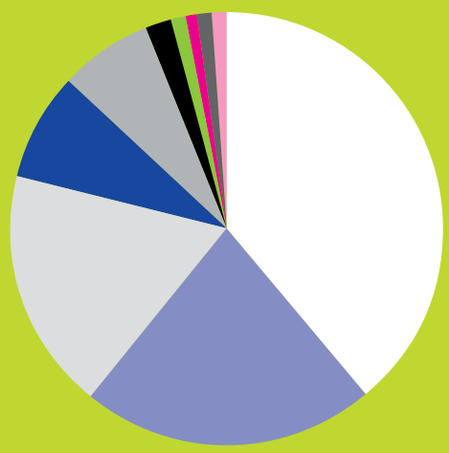


Phishing er den typiske angrebsvektor for de fleste forsøg på indtrængen. Phishing kan være både amatørens mulighed for at lave hurtig fortjeneste, hvad enten det er i forbindelse med falske indsamlinger eller simple datatyverier. Phishing eller spearphishing kan også være den professionelle cyberkriminelles strategiske indsatsområde mhp at sprede fx infostealers eller ransomware. Af figuren ses det, at Microsoft indtager førstepladsen som det oftest udnyttede brand med andre kendte varemærker på de efterfølgende pladser. Phishinghosts betegner de systemer hvorfra selve phishingangrebet udgår.

Cyberkriminelle

Infostealers H2 2021

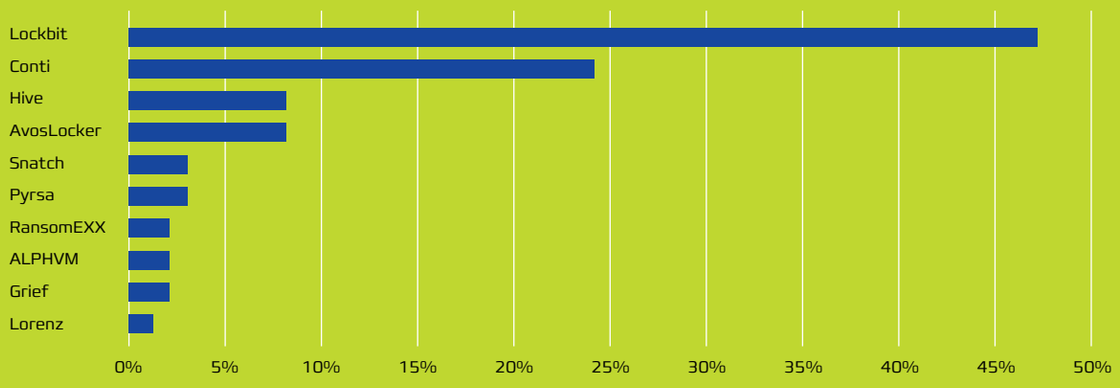
1	Variant:	Cryptobot	39%
2		Redline	22%
3		Raccoon	18%
4		Lokibot	8%
5		Oski	7%
6		Vidar	2%
7		Agenttesla	1%
8		Vertex	1%
9		Arkei	1%
10		KPOT	1%



Kilde CSIS

Infostealers er malware, der har til formål at få adgang til information hos ofrene. Informationen kan både være loginoplysninger til onlinetjenester eller e-mailkorrespondance, som kan anvendes i en social engineering-kontekst. Diagrammet viser fordelingen mellem forskellige infostealers på det internationale marked. Det fremgår, at Cryptbot var den dominerende variant i andet halvår af 2021, mens Redline er den primære kilde til identitetsdata, som sælges på kriminelle onlinefora.

Ransomware - Top 10 leak sites H2 2021



Ransomware-as-a-service vedbliver med at være en lukrativ forretning for ransomwaregrupperingerne. Både de grupper, der udbyder servicen, og dem, der anvender den til at afpresse ofre. Mange af grupperne har taget dobbeltafpresningen til sig ved at true ofrene med offentliggørelse af fortrolig data, hvis de ikke betaler løsesummen. De stjålne data offentliggøres via de 'leak sites', som grupperne står bag. Den mest produktive gruppe i andet halvår af 2021 er Lockbit. Conti-gruppen på andenpladsen er bl.a. kendt for i starten af 2022 offentligt at bekendtgøre sin støtte til Rusland i krigen mod Ukraine. REvil-gruppen, der stod bag angreb på Kaseya og slagterikoncernen JBS i USA, blev bekendtgjort nedtaget i sommeren 2021, men genopstod senere på året.

2. Trusselsvurdering 2022

2.2.5. Trusler mod data

Trusler mod data retter sig mod datakilder med det formål at opnå uautoriseret adgang og/eller afsløring. Truslen omtales hovedsageligt som databrud eller datalæk og henviser til frigivelse af følsomme, fortrolige eller beskyttede data til et upålideligt miljø.

Databrud kan forekomme som et resultat af et cyberangreb, et insiderjob, utilsigtet tab eller eksponering af data. Datatyveri bruges af ondsindede aktører til at kopiere eller overføre følsomme data, typisk med økonomiske motiver gennem videresalg til andre aktører, der kan bruge oplysninger og data om kendte personer, politikere m.v. til egne angreb, fx spearphishing eller whaling. I særlige tilfælde bruges opsnappede data til identitetstyveri, hvor de kriminelle typisk prøver at optage lån eller at købe forbrugsgoder i ofrets navn. Dermed kommer cyberkriminelles forskellige fagkompetencer i spil.

Trusler mod data rangerer konsekvent højt blandt de førende trusler i ETL.[12] Der udvikles hele tiden nye teknikker, som udnytter det øgede behov for at være online og brug af onlinetjenester. I betragtning af betydningen af data, især private og følsomme data, kombinerer angribere mere sofistikerede metoder for at nå sine mål, såsom ransomware- eller 'supply chain'-angreb.

2.2.6. Trusler mod tilgængelighed og integritet

Truslen mod tilgængelighed og integritet er målet for et væld af trusler og angreb, hvor blandt andet overbelastningsangreb - Denial of Service - og angreb på internet services skiller sig ud. Denial of Service retter sig mod system- og datatilgængelighed, og selvom det ikke er en ny trussel, er det fortsat en væsentlig trussel i cyberlandskabet. Angreb virker ved at brugere af et system eller en tjeneste ikke er i stand til at få adgang til relevant information, tjenester eller andre ressourcer. Dette kan opnås ved eksempelvis at overbelaste en enhed på netværksinfrastrukturen med forespørgsler.

Angreb på internet services retter sig primært mod dataintegritet og tilgængelighed og har ofte en stor angrebsflade, fx ondsindede URL'er (Uniform Resource Locators, dvs. webadresser) eller ondsindede scripts, der bruges til at dirigere brugeren eller offeret til et ønsket websted. Det kan også ske ved download af ondsindet indhold (vandhulsangreb, drive-by-angreb) og installering af ondsindet programkode fra et kompromitteret websted, som bruges til at stjæle information til brug for afpresning via ransomware.

2.2.7. Misinformation – desinformation

Stigningen i brugen af digitale teknologier og sociale medier har ændret den måde, hvorpå folk har adgang til informationer og nyheder. I modsætning til traditionelle medier (fx aviser og tv) giver sociale medier direkte adgang til informationer, der dog ikke er filtreret. Prisen, vi betaler for en så bekvem måde at få adgang til information på, er en stigende risiko for at få falske nyheder og manipuleret information.

I den sammenhæng indtager sociale medier rollen som foretrukken formidler af information og 'nyheder', typisk mere end de traditionelle medier. Oplysninger på sociale medier kan være enten falske eller reelle. Forstærkningseffekten af (sociale) medier kan være en trussel mod enkeltpersoner, virksomheder og endda stater, fordi en falsk nyhed eksempelvis kan opfattes som reel, mens et ubetydelig problem kan blive til en stor begivenhed i den offentlige mening.

Manipuleret information kan også benytte sig af såkaldt 'deepfake', hvor fx videoklip eller live videomøder kan manipuleres ved hjælp af kunstig intelligens, idet ansigter og stemmer fra andre kan sættes ind i videoer, således at fx politikere eller kendte personer tilsyneladende udbreder en anden parts budskab. Teknologien kan også anvendes til at tilføje falske mødedeltagere i online-møder. Teknologien bliver stadig bedre, og det kan være vanskeligt at gennemskue forfalskningen. Systematisk desinformation spiller en betydelig rolle i den aktuelle situation omkring Ukraine-krigen.

DKCERT har i februar 2022 beskrevet en metode fra CISA (Cybersecurity and Infrastructure Security Agency, USA) til at håndtere påvirkningskampagner (TRUST-modellen).[13]

[12] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (side 61ff)

[13] https://cert.dk/da/klumme/2022-02-24/Saadan-kan-du-modstaa-paavirkningskampagner

2. Trusselsvurdering 2022

2.2.8. Menneskelige fejl

Trusler betragtes almindeligvis som ondsindede aktiviteter udført af angribere, der har forskellige motiver til at angribe et bestemt mål.

Ikke-ondsindede trusler er for det meste baseret på menneskelige fejl og systemfejlkonfigurationer, men de kan også referere til fysiske katastrofer, der direkte eller indirekte rammer it-infrastrukturer. Ikke-ondsindede trusler klassificeres typisk i disse kategorier:

- Fejl og fejlkonfigurationer er forårsaget af uagtsomhed, manglende kompetencer eller simpelthen menneskelige fejl. Disse omfatter:
  - Fejlkonfigurationer
  - Fejlagtig systemstyring inklusive fejl i patching og opdatering
  - Fejlagtig systemadministration, for eksempel ved tildeling
  - Fejl ved styring af traditionelle systemer såsom netværkssikkerhed, adgangskontrol, identitetsstyring.
  - Udviklingsfejl, her under manglende inputvalidering
- Fejl på applikationsniveau (fejl introduceret ved brug af et program/system,)
- Uopmærksomhed ved brug af brugeridentifikation og adgangskoder
- Fysiske katastrofer kan klassificeres som:
  - Skader på eller svigt af fysisk infrastruktur, såsom utilsigtet skade på fiberkabler, tab af internetforbindelse, brand, ustabil strømforsyning
  - Naturkatastrofer, såsom oversvømmelser og jordskælv, der forårsager manglende tilgængelighed af it-infrastrukturen og relaterede tjenester/applikationer.

Denne kategori af trusler udgør i virkeligheden den største trussel mod påvirkning af tilgængelighed, integritet og fortrolighed.

ENISA foretog i 2020 en undersøgelse af trusler for teleområdet.[14] Denne undersøgelse viste, at over 9 ud af 10 af truslerne mod tilgængelighed, integritet og fortrolighed påføres af ikke-ondsindede trusler (naturkatastrofer, systemfejl og menneskelige fejl), og ondsindede angreb forekommer kun i to procent af tilfældene. Det kan antages, at en tilsvarende fordeling gør sig gældende for øvrige områder, således også uddannelses- og forskningssektoren.

Ud fra denne betragtning bør der sættes langt stærkere ind på at minimere menneskelige fejl og forebygge, at fysiske katastrofer får alvorlige konsekvenser for informationssikkerheden.

Truslen fra medarbejderes fejl betegnes typisk som 'insidertruslen'. Det kan efter DKCERTS opfattelse misforstås, eftersom en 'insider' kan ses som en person, der har uvederhæftige hensigter. Dette kan være tilfældet, men er det i langt de fleste tilfælde ikke.

DKCERT opererer derfor med en anden terminologi, som kendetegner forskellige medarbejdertypers tilgang til informationssikkerhed: Den ubevidste, den uagtsomme og den uvederhæftige medarbejder.

Den klassiske **ubevidste medarbejder** er den person, som på grund af fx uklare, manglende sikkerhedspolitikker eller manglende uddannelse ubevidst bryder organisationens sikkerhedspolitikker. Denne medarbejder kan eksempelvis sætte et ukendt og derfor usikkert USB-stik ind i sin arbejdscomputer eller blive narret til at oplyse adgangskoder eller andre følsomme oplysninger over telefon eller e-mail til personer, som hævder at tilhøre fx organisationens it-afdeling. Et andet meget udbredt eksempel er, at medarbejdere forlægger eller mister medier med følsomme eller fortrolige oplysninger på. Det kan også være afsendelse af åbne mails med følsomme oplysninger eller pengeoverførsel ifm. business email compromise.

En anden type medarbejderfejl er forårsaget af uagtsomhed; denne person kan kaldes **den uagtsomme medarbejder**. I 2020 blev der spurgt til ind til offentligt ansattes uagtsomhed i forbindelse med dataindsamlingen til rapporten Danskernes Informationssikkerhed.[15] Af analysen fremgik det det, at der var sket en stigning i andelen af offentligt ansatte, der bevidst undlader at efterleve organisationens retningslinjer for informationssikkerhed. En stor del af dem, der bevidst bryder reglerne, oplyser som årsag, at reglerne umuliggør udførelsen af deres arbejde.

[14] https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020

[15] https://cert.dk/sites/default/files/uploads/Danskernes%20informationssikkerhed%202020.pdf

2. Trusselsvurdering 2022

Dette gør dem ikke til uvederhæftige medarbejdere, men derimod uagtsomme. Kan man som medarbejder ikke udføre sit arbejde pga. regler og procedurer og bliver nødt til at omgå sikkerhedspolitikken, kan det medføre en sikkerhedsmæssig kompromittering, som kan få en alvorlig konsekvens for fx en uddannelsesinstitution.

Den **uvederhæftige medarbejder** – insideren – kan udføre handlinger, der kan have betydelig skade på en organisation. Mens ondsindede, eksterne hackere i mange tilfælde bliver stoppet af sikkerhedsmekanismer som firewalls, e-mailscanning og antivirus-filtre, vil insideren ofte have succes med sine handlinger. Det kan skyldes, at sikkerhedsmekanismerne ikke altid beskytter mod en insider, der vil være i stand til at udføre sine handlinger i kraft af misbrug af sin stilling og legitime it-adgange.

Den uvederhæftige medarbejder er svær at opdage, men hans eller hendes skadevirkende adfærd kan til en vis grad begrænses med funktionsadskillelse, bruger/rettighedsstyring og logs. Der er set eksempler på, at cyberkriminelle grupper systematisk har arbejdet med rekruttering af insidere mod betaling eller ved afpresning.

2.2.9. Supply chain-angreb

Denne kategori er kommet på ENISAs liste, ikke fordi den er udbredt, men mere fordi den har vist sig at være meget indgribende i virksomheders infrastruktur. Det senest kendte, større supply chain-angreb sås i slutningen af 2020 med eftervirkninger ind i 2021 i forbindelse med softwaren Orion fra SolarWinds, hvor det var lykkedes for hackere at placere bagdøre i leverandørens software. Disse bagdøre var blevet installeret hos kunder i forbindelse opdatering af deres software fra SolarWinds.

I løbet af 2021 stiftede vi også bekendtskab med Log4j. Log4j er en open source-logningssystem, som er distribueret af Apache-gruppen. Log4j bruges skønsmæssigt på en tredjedel af verdens web-servere. Her viste det sig, at der var en RCE-sårbarhed (Remote Code Execution i log4j installationer, som gjorde det muligt for en hacker eller angriber at afvikle kode på enheder, der bruger log4j logningsfunktionalitet. Dette har givet sårbarheden et navn: Log4Shell.

CFCS har udgivet publikationen 'SolarWinds: Statsstøttet globalt software supply chain-angreb', som i detaljer beskriver, hvordan en statsstøttet hackergruppe udførte det globale software supply chain-angreb via it-virksomheden SolarWinds.[16] Sagen illustrerer, hvordan hackere kan bruge en leverandør til at kompromittere mange ellers velbeskyttede ofre på én gang.

[16] https://www.cfcs.dk/da/cybertruslen/rapporter/solarwinds/

2. Trusselsvurdering 2022

2.3. HÆNDELSER FRA UNIVERSITETSVERDENEN

Der har gennem de sidste par år været konkrete hændelser, der har ramt universiteter i Europa, især kan fremhæves hændelser fra Danmark og Tyskland.

Aalborg Universitet (AAU)var i sommeren 2020 udsat for et hackerangreb, der betød, at ansattes personoplysninger blev kompromitteret.[17] Her blev 28 ansatte eller tidligere ansattes lønoplysninger, ligesom 15 studerende og ansattes kodeord kompromitteret.

Universitetets analyse viser, at omkring 30.000 brugere blev berørt af hændelsen, da angribere har haft adgang til universitetets netværk og brugerdatabase (Active Directory).[18] Af brugerdatabasen fremgår primært almindelige personoplysninger, som ligger offentligt tilgængelige på AAUs hjemmeside, desuden indeholdes passwords i krypteret form (password-hashes) og for nogle brugere mobilnummer til multifaktorautentifikation.

Personoplysninger så i sig selv ikke ud til at være motivet for angrebet. som måske var forberedelse til et ransomwareangreb. For at komme ind udnyttede angriberne en sårbar enhed, som ikke har været sikkerhedsmæssigt opdateret. Det gav dem adgang til det interne netværk, hvilket kan have betydning for integriteten af systemer, adgange til disse og andre fortrolige informationer. Efter angrebet blev der lukket for forbindelsen til internettet og dernæst sikret, at alle brugere skiftede password. Efterfølgende har AAU skærpet overvågning på alle systemer.

I april 2021 blev servere på Det Tekniske Universitet i Berlin (TU Berlin)[19] angrebet med ransomware af den russisk-baserede Conti-gruppe (se opslaget om Cyberkriminelle s. 13). Ved angrebet, der var målrettet universitetets Windows-operativsystem, blev hele systemer krypteret, især gik det ud over universitetets mailservere, der er den primære kommunikationskanal med de studerende. Angrebet blev bemærket, fordi forskellige krypterede filer pludselig befandt sig på forkerte steder i systemerne. I september 2021 led universitetet stadig under følgerne af angrebet.

[17] https://www.its.aau.dk/beredskab#478965
[18] https://www.its.aau.dk/beredskab
[19] https://www.morgenpost.de/berlin/article232177213/Hacker-greifen-Technische-Universitaet-an.html

2. Trusselsvurdering 2022

Angrebene fandt sted gennem upatchede Windows Remote Desktop Protocol (RDP), som bruges til at få adgang til interne computere udefra. Brugere, der anvendte VPN var ikke ramt. Hele universitetets AD blev kopieret og er siden observeret til salg på Dark Web.

I november 2021 blev et dansk universitet udsat for et hackerangreb, hvor der igen blev brugt upatchede services som angrebsvektor, denne gang på SharePoint. Motivet til angrebet er stadig uklart, men undersøgelser viser, at hackerne ikke har haft held med deres forehavende. Dette kan skyldes, at hackerne har været 'script kiddies', der har fået købt sig et tool på fx Dark Web, til udnyttelse af sårbarheden i SharePoint Angriberne har så heldigvis efterfølgende ikke vidst, hvad de skulle bruge den uautoriserede adgang til. Men angriberne kunne lige så godt have været statslige aktører fra andre lande, og så havde situationen set anderledes ud.

I maj 2020 blev en række supercomputere i forskningsinstitutter i hele Tyskland og Storbritannien angrebet af hackere. I Tyskland blev mindst seks systemer kompromitteret. Den 11. maj udsendte High Performance Computing Center (HLRS), et forskningsinstitut og et supercomputercenter baseret i Stuttgart, en notifikation om lukningen af 'Hawk' på grund af en sikkerhedshændelse.[20]

Hawk er flagskibet blandt supercomputere. Med en topydelse på cirka 26 Petaflops er Hawk et HPE Apollo 9000-system og er blandt de hurtigste supercomputere i verden. Det er således det hurtigste system til videnskabelig og industriel databehandling i Europa.[21]

Leibniz Supercomputing Centre fra Die Bayerische Akademie der Wissenschaften nær München bekendtgjorde også, at dets systemer var blevet ramt af hackere.[22]

Forschungszentrum Jülich og Karlsruhe Institute of Technology (KIT) rapporterede også de samme problemer, hvor sidstnævnte oplyste, at to højtydende computere bwUniCluster 2.0 og ForHLR II, var blevet ramt af en såkaldt alvorlig sikkerhedshændelse.

Stjålne eller hackede brugerkonti har været brugt til at opnå adgang til systemerne. De stjålne eller hackede konti er derefter blevet brugt til eskalering af privilegier, således at hackerne har haft root adgang til systemerne. Supercomputerne blev inficeret med cryptocurrency-mining malware. Cyberkriminelle leder altid efter nye måder at tjene penge på, og flere gange de senere år par år har ransomware været det foretrukne cyberangreb for dem, der gerne vil tjene hurtige penge. I de seneste år er set en stigning i cryptocurrency mining som en alternativ måde at tjene penge på.

I dette tilfælde bruges computernes processorkraft til at grave (mine) efter kryptovalutaer som fx Bitcoin og Monero,. Men i stedet for at bruge penge på specialiserede systemer til lovligt at udvinde kryptovaluta, anvender cyberkriminelle cryptojacking-malware for at gøre arbejdet for dem. Ideen er enkel: uvidende ofre får deres computer eller smartphone inficeret med malware, som bruger enhedens CPU-kraft til at udvinde kryptovaluta, der føres tilbage til angriberens cryptowallet.

[20] https://www.defenseworld.net/news/26987/Supercomputers_in_Research_Institutes_across_Germany__UK_Hacked#.YfelPJqZNaZ
[21] https://www.hlrs.de/news/detail-view/2020-02-19/
[22] https://web.archive.org/web/20200620135633/https://www.lrz.de/aktuell/ali00856.html

2. Trusselsvurdering 2022

2.4. GENERELLE TRENDS

ENISA har i den ovenfor citerede publikation 'ENISA Threat Landscape 2021' beskrevet en række trends inden for trusler mod it anvendelsen.

Listen nedenfor opsummerer de vigtigste tendenser, som er observeret i cybertrusselslandskabet fra april 2020 til juli 2021.

- Sofistikerede kompromitteringer i forsyningskæden (supply chain) er øget
- COVID-19 har skabt nye muligheder for cyberkriminelle
- Statslige organisationer har optrappet deres aktiviteter på både nationalt og internationalt plan
- Cyberkriminelle motiveres i stigende grad af økonomisk vinding til deres aktiviteter
- Cyberkriminalitetsangreb er i stigende grad rettet mod og påvirker kritisk infrastruktur fx i form af DDoS angreb
- De kriminelles forretningsmodeller fx Ransomware as a Service (RaaS) er steget i løbet af 2021
- Fald i rapporterede malwareangreb, men malwareangreb rettet mod containermiljøer er blevet meget mere udbredt
- Mængden af krypto-kompromitteringer nåede rekordhøjde i første kvartal af 2021 sammenlignet med de sidste par år. Den økonomiske gevinst forbundet med angrebene tilskyndede trusselsaktører til at udføre disse angreb
- COVID-19 er stadig det dominerende lokkemiddel i kampagner for e-mailangreb
- Business E-mail Compromise (BEC) er steget og er blevet mere målrettet
- Forretningsmodeller omkring Phishing-as-a-Service (PhaaS) som kriminel aktivitet – ikke at forveksle med fingerede phishingkampagner til awareness-formål - er ved at vinde udbredelse
- Traditionelle DDoS-angreb (Distributed Denial of Service) bevæger sig mod mobilnetværk og IoT (Internet of Things)
- Ransom Denial of Service (RDoS) er begyndt at vinde indpas som én af de cyberkriminelles forretningsmodeller
- Der er observeret flere menneskelige fejl og systemfejlkonfigurationer. I 2020 og 2021 observeredes en stigning i ikke-ondsindede hændelser.

3. Året i tal og ord

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

3.1 SCANNINGER, ADVARSLER, HÆNDELSER OG TEKNISKE ANALYSER

3.1.1 Sårbarhedsscanninger

DKCERT tilbyder sårbarhedsscanninger til institutioner tilknyttet forskningsnettet.

Scanningerne gennemføres på baggrund af konkrete bestillinger fra institutionerne. Enkelte institutioner får gennemført scanninger en-to gange årligt, mens andre får hyppigere scanninger, typisk hver måned. Af de 10 institutioner på forskningsnettet, der regelmæssigt benytter sig af tjenesten, får fire institutioner udført scanninger hver eller hver anden måned. Seks institutioner får gennemført scanninger en gang i kvartalet eller hvert halve år. Der er i alt 38 små og store institutioner på forskningsnettet.[23]

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

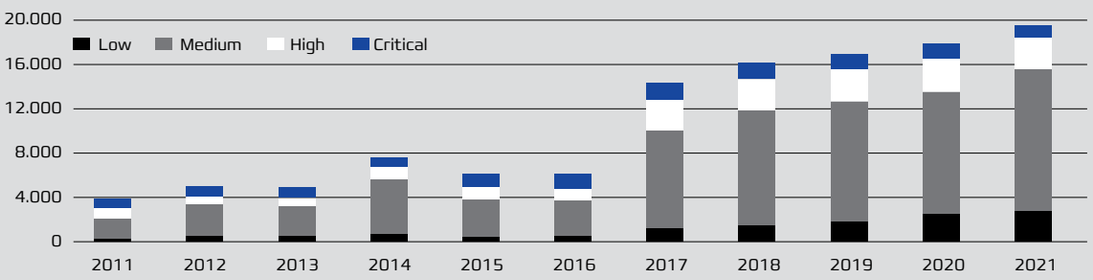
DKCERT mener:
I forhold til det nuværende trusselsbillede er det DKCERTs anbefaling, at institutioner på forskningsnettet får udført scanninger mindst en gang hver anden måned.

Scanningerne undersøger, om institutionernes it-systemer har kendte sårbarheder, som er publiceret i National Vulnerability Database (se Figur 1). DKCERT scanner IP-adresser på institutionerne og samler resultaterne i en rapport om de fundne sårbarheder i institutionerne med forslag til hvilke tiltag, som bør iværksættes for at højne sikkerheden for den enkelte institution. Rapporterne indeholder en prioritering af de fundne sårbarheder og anbefalinger til institutionens håndtering af disse ud fra sårbarhedernes kritikalitet.

Anbefalingerne til prioriteringen baseres på sårbarhedernes score i forhold til CVSS – common vulnerability scoring system. CVSS er den internationalt anerkendte metode til scoring af sårbarheder på en skala fra 1-10.

Figur 1: Publicerede sårbarheder i NVD fra 2011 - 2021

DKCERTs scanninger efter sårbarheder baserer sig på de CVE-numre, der bliver publiceret på National Vulnerability Database, udstiller indrapporterede sårbarheder. Det fremgår af grafen, at der har været en støt stigning henover årene. Stigningen kan skyldes, at der kommer flere og flere produkter på markedet, men også at der er kommet flere sikkerhedsresearchere til, der finder sårbarhederne.



3. Året i tal og ord

Årets eksterne scanninger
I 2021 har DKCERT gennemført 174 scanninger på forskningsnettet, heraf var 164 bestilte scanninger. I 2020 var antallet på 103 og i 2019 52.

Af de 174 scanninger var 83 ad hoc-scanninger, hvor institutionerne på baggrund af en konkret mistanke om en sårbarhed bestiller en scanning på en given server udelukkende med den pågældende sårbarhed i sigte. 81 scanninger var tilbagevendende scanninger, som foretages på abonnementsbasis, dvs. med aftalte mellemrum med institutionerne.

I særlige situationer gennemfører DKCERT desuden scanninger af hele forskningsnettet. I 2021 har DKCERT scannet forskningsnettet ekstraordinært 10 gange – de fleste gange målrettet en aktuel sårbarhed, i december en generel scanning.

DKCERT mener:
Den samlede stigning i antallet af bestilte scanninger fra 103 til 164 på institutionerne må betragtes som en øget opmærksomhed fra institutionerne på risikoen for, at sårbarheder udnyttes til konkrete angreb.

Det samlede antal scannede host-enheder/IP-adresser i 2021 var 115.069, hvilket er et fald fra godt 300.000 i 2020. Faldet skyldes formentlig, at institutionerne er blevet meget bedre til at specificere deres scope for scanningen.

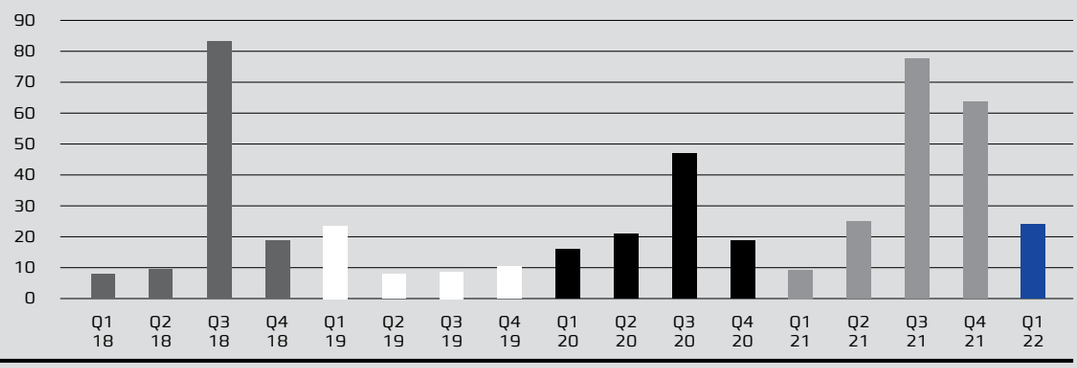
DKCERT mener:
Set i forhold til trusselsvurderingen er én uhåndteret sårbarhed en sårbarhed for meget. Efter DKCERTs opfattelse er næsten fem procent af hostenhederne med en høj eller kritisk sårbarhed en meget høj andel, som institutionerne opfordres til at forholde sig til.

Af det samlede antal scannede host-enheder/IP-adresser var 17.241 i 'live'. Det betyder, at der konstateredes aktivitet på dem. Samlet havde 817 af de levende host-enheder i 2021 en kritisk eller høj sårbarhed svarende til fire pct. I 2018 var 12 pct. af sårbarhederne fundet i de levende host-enheder 'kritiske', mens 27 pct. havde betegnelsen 'høj'. I 2021 var de tilsvarende tal hhv. to procent og 10 pct. Altså et mærkbart fald over en treårig periode.[24]

[24] Af tekniske årsager har sammenlignelige tal for 2019 og 2020 ikke kunnet beregnes.

Figur 2: DKCERTs sårbarhedsscanninger på forskningsnettet 2018-2022

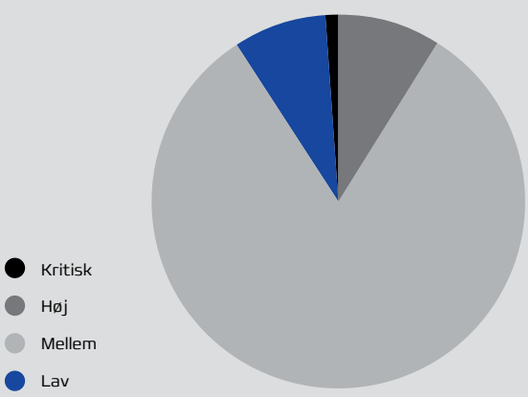
I 2021 udførte DKCERT 174 scanninger på forskningsnettet, hvoraf 164 var på baggrund af konkrete bestillinger fra institutionerne.



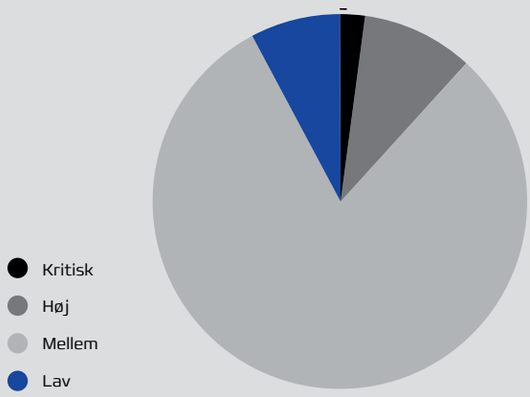
3. Året i tal og ord

Figur 3: Sårbarheder fordeling

Sårbarhedernes fordeling på baggrund af de lokale scannninger



Generel scannning december 2021



Diagrammet til venstre viser sårbarhedernes fordeling på kritikalitet ud af de i alt 22.549 fundne sårbarheder i de 81 scanninger i 2021, som DKCERT har gennemført på baggrund af faste aftaler om konkrete bestillinger. I december 2021 gennemførte DKCERT på egen foranledning en generel scanning af hele forskningsnettet, hvilket i sagens natur også omfattede institutioner, der ikke almindeligvis bestiller scanninger. Fordelingen på kritikalitet fremgår af diagrammet til højre. Bemærk, at andelen af kritiske sårbarheder i decemberscanningen er næsten dobbelt så stor (to pct) som i den mængde, der er fundet ifm. bestilte scanninger (1,2 pct).

Forskellen skyldes sandsynligvis, at de bestilte scanninger gennemføres for institutioner, der i forvejen har fokus på sårbarheder. Øvrige institutioner, der ikke bestiller scanninger, har ikke de samme fokus. Derfor fanger den generelle scanning også flere sårbarheder.

Sammenligningen mellem de to typer scanninger viser, at opmærksomhed på sårbarheder har betydning for robustheden.

De eksterne scanninger (se Figur 3) for 2021 viser, at godt to pct. af sårbarhederne er kritiske, små 10 pct. har vurderingen høj, 80 pct. er middel og otte pct. er lav. I alt er der fundet 22.549 sårbarheder.[25] Sårbarhedernes opdeling er baseret på OWASP TOP 10 Web Application Security Risks 2020.[26]

Hvis institutionen er længe om at opdatere software, tæller den samme sårbarhed med i flere scanninger.

Ud over de bestilte scanninger har DKCERT på eget initiativ gennemført scanninger af hele forskningsnettet 10 gange i alt. Dette skyldes primært fremkomsten af de meget kritiske sårbarheder, Proxylogon i marts, Printnightmare juli og Log4shell i december. Med dette har DKCERT scannet samlet 1,4 mio. IP'er.

Interne scanninger

DKCERT har i 2021 genoptaget servicen vedr. interne scanninger. En intern scanning gennemføres inden for institutionens firewall og scanner lokale netværk, mens eksterne scanninger udføres uden for firewall'en, hvorved man kun opdager offentligt tilgængelige sårbarheder. Den interne scanning giver en mere fintmasket undersøgelse af institutions systemer. Herved kan der evt. findes systemer med sårbarheder, der kan udnyttes, hvis en udefrakommende har fået adgang eller hvis en insider skulle være ondsindet. Intern scanning kan bestilles af institutionerne på linje med eksterne scanninger, dvs. ved kontakt til cert@cert.dk.

[25] Af trendrapporten 2021 fremgår det, at der er blevet fundet 1567 i 2021. Dette tal er fejlbehæftet.
[26] https://owasp.org/www-project-top-ten/

Sårbarheder 2021

ÅRETS ALVORLIGSTE SÅRBARHEDER

Undersøgelser viser, at gamle sårbarheder oftest bliver udnyttet. De ligger i systemer i årevis, uden at der bliver gjort noget ved dem, selv om der både er rettelser og opdateringer tilgængelige og udnyttelses-kode har været publiceret længe. Hvert år opdages nye sårbarheder, sandsynligvis langt flere end dem, der publiceres til National Vulnerability Database (se Figur 1), men nogle af dem er så spektakulære, at de får langt mere opmærksomhed fra både godsindede og det ondsindede miljø.

Her beskriver vi de fire mest kendte og alvorligste sårbarheder fra 2021.

1 **Log4Shell**

Log4Shell er en sårbarhed i Log4j - et bibliotek, som kan bruges af bl.a. Apache. Sårbarheden er meget kritisk, da den lader en person få totalt adgang over den server, der bruger log4j. Er sårbarheden først blevet udnyttet, kan adgang bruges til at lægge fx ransomware og kryptoudvindingssoftware på serveren eller fx tilføje serveren til et botnet.

Log4j er et open sourcebibliotek, der bliver kørt på mange forskelige applikationer lige fra hjemmesider til fx Minecraft. Sårbarheden fik en score på 10 ud af 10 mulige - fordi den er nem at udnytte, og fordi den er mange steder. Den store udbredelse af biblioteket gør den særligt kritisk og er af eksperter blevet spået til at kunne påvirke produkter i årevis.[27] Risikoen for udnyttelse af sårbarheden fik Århus Universitet til at lukke ned for en lang række systemer, indtil det blev afdækket, om systemerne anvendte Log4j.[28]

2 **ProxyLogon**

Proxylogon var en sårbarhed i Microsoft Exchange servers, hvor man kan opnå remote code execution ved at udnytte en fejl i Exchanges webbrowser-del, hvorefter man har adgang til hele systemet, ligesom man opnår også rettigheder som SYSTEM (Administrator). En af den store kritiske ting ved proxylogon var også, at Microsoft's patch, der skulle løse problemet, ikke fjernede alle de bagdøre, der allerede var blevet installeret på serveren igennem sårbarheden. Det betyder, at hackere ville have frit spil, hvis de havde nået at udnytte sårbarheden og fx installeret en bagdør.

3 **PrintNightmare**

PrintNightmare er en sårbarhed, der blev fundet i Windows printer spooler-service. Denne spooler-service er installeret på de fleste Windows-maskiner, herunder også Window's domain controllers. Hvis domain controlleren er påvirket af denne sårbarhed, ville hackere kunne udnytte den og overtage maskinen med SYSTEM-rettigheder.

4 **Sam The admin**

Sam The admin er en sårbarhed, der udnytter en sårbarhed i Window's active directory, hvor man kan opnå at blive AD administrator. Hvis denne sårbarhed bliver brugt sammen med en af de andre sårbarheder, kan man gå fra at overtage serveren til at overtage en virksomheds infrastruktur.

[27] https://www.computerworld.dk/art/259034/dyster-udsigt-log4j-vil-plage-industrielle-systemer-mange-aar-frem
[28] https://www.computerworld.dk/art/259022/aarhus-universitet-lukker-med-omgaaende-virkning-ned-for-lang-raekke-it-systemer-frygter-at-blive-hacket-via-log4j

3. Året i tal og ord

3.1.2 Advarsler fra tredjeparter

I 2021 modtog og udsendte DKCERT advarsler om 38 forskellige typer sårbarheder, som er identificeret på det danske forskningsnet. Denne service blev introduceret i slutningen af 2014 og hjælper det danske forskningsnet med at afdække, hvilke mulige angrebspunkter, som ondsindede aktører nemt kan finde. Advarslerne kommer fra samarbejdspartnere, først og fremmest Shadowserver-projektet, der dagligt scanner internettet for en række kendte og hyppigt udnyttede sårbarheder.

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

I gennemsnit er der i 2021 blevet udsendt 185 unikke advarsler pr. måned om sårbarheder på forskningsnettet. Det anslås, at omkring 60-70 pct. af disse dubletter, går igen i de scanningerne fra måned til måned.

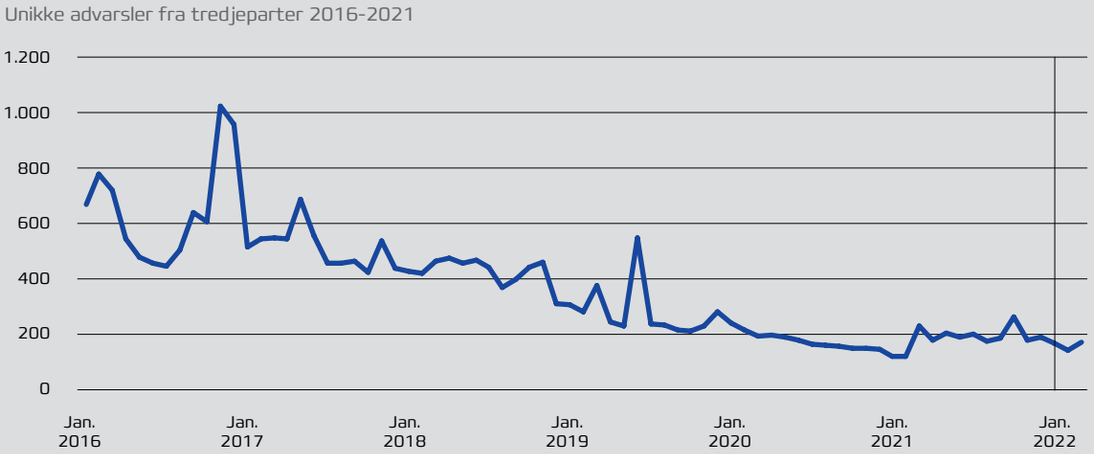
Siden 2016 har udsendelse af advarslerne været automatiseret. Grafen i Figur 4 viser, at antallet af unikke advarsler sendt til det danske forskningsnet generelt er faldende fra i gennemsnit 650 på måned i 2016 til 176 pr. måned i 2020. I 2021 har det være en mindre stigning. Faldet frem til 2020 skyldes efter DKCERTs opfattelse, at forskningsnettets institutioner generelt er blevet bedre til at tage hånd om sårbarhederne, og at krav i ISO27001 og andre tekniske minimumskrav har haft en vis grad af effekt.

3.1.3 Årets sikkerhedshændelser

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

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

Figur 4 Advarsler fra tredjeparter i 2016-Q1 2022



3. Året i tal og ord

DKCERT modtog i 2021 oplysninger om 88 hændelser, hvoraf DKCERT har undersøgt 67 af dem, mens de resterende 11 er blevet afhjulpet på anden vis. Hændelserne omhandler typisk inficerede systemer på forskningsnettet. DKCERT undersøger bl.a., om en mistanke om malware på et system kan bekræftes, sørger for notifikation af berørte parter, udfører rådgivning og understøtter kommunikation til eksterne ressourcer.

DKCERT ser hændelser eller potentielle hændelser i alle trin af angrebskæden, herunder forsøg på rekognoscering af zoner på forskningsnettet, forsøg på at få adgang til systemer og udnyttelse af kompromitterede systemer.

Ud over de nævnte hændelser har DKCERT behandlet sager om spam og phishing samt forsøg på målrettede angreb mod institutioner på forskningsnettet.

3.1.4 Dataanalyse

Data om netværkstrafik fra forskningsnettet kan give ny viden om angrebsmønstre og opdage angreb, der ellers ikke ville blive registreret. Ud fra den tanke kan DKCERT analysere trafikdata fra routerne på nettet. Dette anvendes til efterforskning af sikkerhedshændelser for institutionerne og i forbindelse med politisager. I 2020 gennemførte DKCERT analyser i forbindelse med sikkerhedshændelsen på Aalborg Universitet i august og i december 2020 og januar og marts 2021 i forbindelse med Sunburst-hændelsen på to universiteter i Danmark. Derudover har DKCERT i 2021 gennemført dataanalyse i forbindelse med offentliggørelse af sårbarheden i Log4j-biblioteket.

3.2 VIDENDELING

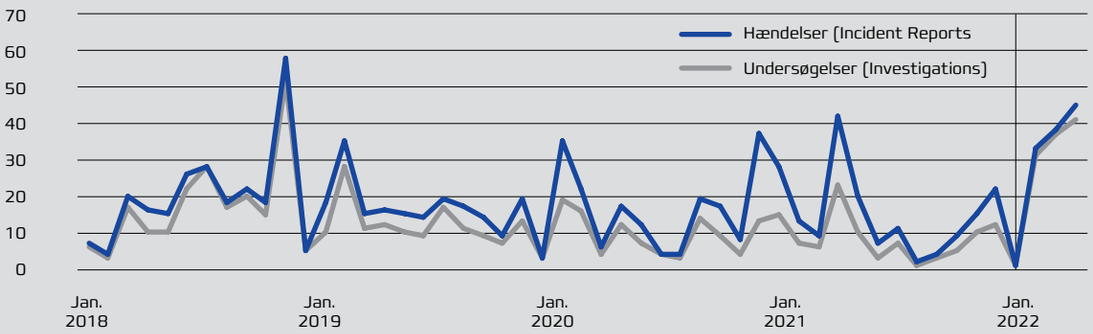
3.2.1 NYT VIDENDELINGVÆRKTØJ TAGET I BRUG

DKCERT har i 2021 stillet et nyt chatværktøj til rådighed for sikkerhedsteknikere ved universiteterne. Værktøjet – Mattermost – er en sikker kanal til udveksling af informationer dels i dagligdagen, dels i tilfælde af hændelser, hvor det er relevant at dele relevant viden, hurtigt og tilgængeligt, så universiteterne kan forberede en evt. aktivering af beredskabsplanen, hvis et vellykket angrebsmønster på et universitet kan forudses forsøgt brugt på et andet. Brug af Mattermost kræver tilknytning til en sikkerhedsfunktion på en forsknings- og uddannelsesinstitution og er sat op til at kræve multifaktorautentifikation ved hjælp af FIDO-nøgler.

DKCERT har i forbindelse med valg af chatværktøj gået efter den meste sikre løsning.

Figur 5 Hændelser og undersøgelser fra 2018- Q1 2022

Det fremgår af grafen, at DKCERT gennemfører flere undersøgelser af de rapporterede hændelser end tidligere. Det skyldes, at DKCERT i højere grad er begyndt at gennemføre undersøgelse på eget initiativ, ligesom DKCERT kan gennemføre selvstændige undersøgelser på foranledning af andre institutioner, som ikke indrapporterer via DKCERTs indrapporteringssystem.



MFA er ikke bare MFA

MFA er ikke bare MFA

Øgede trusler øger behovet for en reflekteret tilgang til multifaktorautentifikationsteknologien/metoden.

DKCERT's sikkerhedsreferencegruppe er begyndt at tage FIDO-nøgler i anvendelse. FIDO-nøgler er en to-faktorenhed, der autentificerer brugeren og giver adgang til den tjeneste, som brugeren logger på. Referencegruppen anvender FIDO-nøglerne til at få adgang til chatkanalen Mattemost, som sikkerhedsteknikere ved universiteterne kan bruge til hurtig vidensudveksling til formidling af nyt, som kun skal deles i en snæver kreds.

Kanalen skal have et sikkerhedsniveau, så der så vidt muligt ikke kan ske kompromittering af kommunikationen.

Hvad er en FIDO? – pt. den mindst usikre MFA
FIDO-nøgler indgår i en bestemt type multifaktorautentifikationsløsning, der kombinerer sikkerhed og beskyttelse af privacy. Selve nøglen er en mindre fysisk enhed på størrelse med et lille USB-stick, som man forbinde til computeren via USB eller NFC.

MFA består af kombinationen af mindst to forskellige faktorer: Noget 'man ved' (fx et kodeord), 'noget man har' (fx. en app på telefon eller en FIDO-nøgle) og 'noget man er' (fx fingeraftryk eller ansigt). Anvender man en FIDO-nøgle som 'det man har' i forbindelse med indlogning til en tjeneste via en browser, skal man forbinde nøglen med den hardwareenhed, fx PC eller telefon, man bruger. FIDO-nøglen skal så yderligere berøres, før indlogning kan finde sted. I fagsprog kaldes det 'user presence', hvilket bekræfter, at der er et menneske til stede.

Kryptografi i nøglen
En anden nok så væsentlig ting står også i modsætning til den såkaldte out-of band autentifikation, som det kendes fra fx NemID, MitID og diverse andre autentifikatorer. I out-of-band autentifikation autentificerer man sig via en anden kanal end den kanal, som den tjeneste, man skal logge ind i, anvender. Kanalen går altså uden om browseren fra serveren direkte til fx telefonen.

Det skaber det problem, at en bruger risikerer indlogning på en falsk tjeneste, fx borggerr.dk og ikke borger.dk. Det kan fx være et phishingsite, der anvender borger.dks profil til at lokke brugere til at afgive oplysninger. Eneste metode til at undgå det er, at brugeren skal tjekke, om URL'en er vederhæftig. Altså ved et manuelt gennemsyn af, om man logger ind på den rigtige tjeneste.

Ved FIDO-teknologien foregår autentifikationen fra serveren direkte til brugerens FIDO-nøgle. Det sker, fordi der ifm. registrering af brugerne etableres et nøglepar, hvor tjenestens adresse indeholdes i brugerens nøgle. Det betyder, at nøglen ikke vil lade brugeren logge ind et forkert sted. Nøglen er registreret til kun at logge ind på den nøjagtige adresse og dermed på det rigtige tjeneste.

Dette indebærer yderligere, at tjenesterne ikke kan se, hvilke andre tjenester som FIDO-nøglerne har været anvendt til. Det skyldes, at hver gang man registrerer en FIDO-nøgle på en ny tjeneste, etableres et nyt nøglepar. Dermed kan tjenesterne hver for sig ikke se, hvor FIDO-nøglen i øvrigt bliver anvendt. Og dermed er FIDO-nøglen født som en såkaldt privacyenhancing technology.

MFA er ikke bare MFA

Mange forskellige MFA-typer
I skemaet i figur 6 kan man se en række forskellige MFA-autentifikationsmetoder og deres modstandsdygtighed mod trusler.[30] Kodeord uden MFA (type 1) er som bekendt den mest usikre. Får andre adgang til kodeordet, uanset om det sker via man-in-the-middleangreb (MITM) eller kodeordet bliver gættet, er modstandsdygtigheden mod indlogning fra anden side lav. Sandsynligheden for at gætte eller cracke et kodeord afhænger af bl.a. længden af kodeordet.

Type 2 til 14 beskriver forskellige MFA-metoder. Det fremgår, at en opringning til en bruger ikke er særlig modstandsdygtig over for tyveri, ved MITM-angreb eller kompromittering af MFA-enheden. Det kan fx være sim-swapping af telefonen. Hvis man vil misbruge login ved hjælp af telefonopkald, handler det dybest set om at have adgangen til telefonen. Det samme gør sig gældende ved brug af sms til fremsendelse af to-faktorkoden.

Det fremgår også, at HOTP (type 6) og TOTP (type 7) via apps på telefonen kun er 'medium' modstandsdygtige over for tyveri, mens modstandsdygtigheden mod MITM-angreb er 'low'. Hvis MFA-enheden bliver kompromitteret er modstandsdygtigheden kun 'medium'.

OTP står for one-time-password og dækker over den egenskab, at der udstedes et enkeltstående kodeord via en telefon eller token. Er der tale om HOTP betyder det event-based one-time password. Her kræver adgangen, at brugeren reagerer positivt på den pågældende event: Er det dig, der forsøger at logge ind på tjeneste X? Google Smart Lock er eksempel på en HOTP. TOTP betyder time-based one-timepassword. Her gælder en given tilfældig, talbaseret sekscifret kode i fx 30 eller 60 sekunder, hvorefter der genereres en ny. Microsoft Authenticator er eksempel på et system, der tilbyder TOTP.

Figur 6 Authentication Factors and Threat Resistance

AuthN Type Number	Authentication Factor	Resistance to Threat				
		Theft (Phishing, etc.)	Theft via Dynamic MITM Phishing	Guessing /Offline Cracking	MFA Device Compromise	User Workstation Compromise
1	Password	Low	Low	Depends	n/a	Low
2	Phone call	Low	Low	High	Low	High
3	Phone call (VoIP)	Low	Low	Medium	Low	High
4	SMS	Low	Low	High	Low	High
5	SMS (VoIP)	Low	Low	Medium	Low	High
6	HOTP cell phone software	Medium	Low	High	Medium	High
7	TOTP cell phone software	Medium	Low	High	Medium	High
8	HOTP token	Medium	Low	High	High	High
9	TOTP token	Medium	Low	High	High	High
10	HOTP written (back up codes)	Low	Low	High	High	Low
11	DUO Push	High	Low	High	Medium	High
12	FIDO U2F token with password	High	High	High	High	High
13	PKI device certificate with device password	High	High	High	High	Medium
14	PKI token certificate with token password	High	High	High	High	High

[30] https://spaces.at.internet2.edu/display/MIPWG/MFA+Technologies%2C+Threats%2C+and+Usage

MFA er ikke bare MFA

MFA – ikke kun teknologi
Skemaet kan anvendes, når man som tjenesteudbyder skal overveje, hvilken type loginmetode man skal tilbyde sine brugere. Ligesom ved al anden sikkerhed handler valget af MFA-teknologi om at vælge den løsning, der passer bedst i forhold til brugervenlighed, sikkerhed og økonomi.

Gennemgår man skemaet, er det tydeligt at se, at heller ikke beskyttelse vha. MFA-løsninger er teknik, uanset hvor teknisk MFA end lyder. Der indgår teknologi i selve løsningen, men angrebsvejene og dermed også forsvarsværkerne kræver, at man tager brugermæssige overvejelser med.

Skemaet er udarbejdet af en arbejdsgruppe under den amerikanske forsknings- og uddannelsesføderation Incommon. Arbejdsgruppen afsluttede sit arbejde i 2017 med publiceringen af skemaet.

3. Året i tal og ord

3.2.2 Videndeling ved hændelser

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

Formålet med dette er, at andre institutioner kan forberede sig og evt hindre, at de rammes af samme type hændelser. I kriminalitetsmiljøet vil kendskab til succesfulde metoder til brud på informationssikkerheden i bestemte sektorer lynhurtigt brede sig, og cyberkriminelle vil forsøge at anvende samme metoder til angreb på andre institutioner.

En institution, som fx er udsat for cyberhændelser, vil derfor typisk 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 som udgangspunkt på CISO-niveau.

I 2021 har DKCERT indhentet viden og koordineret indsatsen ift. en hændelse på DTU og Log4j-sårbarheden, der fik Århus Universitet til at lukke ned for en række systemer for at undersøge om Log4j indgik i universitets it-miljø. Dette viste sig dog ikke at være tilfældet.

3.2.3 Faglig videndeling i netværk

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

Der deltager hver gang ca. 30 sikkerhedstekniker i møderne.

I 2021 er der gennemført fem online SikRef-møder. Møderne omhandlede bl.a. tilpasning og anvendelse af MISP (læs mere om MISP i afsnit 3.3.5), hvor man systematisk deler viden om bl.a. såkaldte "Indicators of Compromise" (trusler og hændelser, fx igangværende phishingkampagner), og udrulning af MFA på universiteterne. I 2022 forventes det, at halvdelen af netværksmøderne bliver fysiske halvdagsarrangementer på et af de otte universiteter. Resten blive onlinemøder,

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

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

CISO-forum har mødtes ca. en gang hver anden måned i 2021.

3. Året i tal og ord

3.2.4 DKCERTs deltagelse i Cybersikkerhedsrådet

Chefen for DKCERT Henrik Larsen er medlem af Cybersikkerhedsrådet, der er nedsat for at rådgive regeringen om, hvordan den digitale sikkerhed styrkes og sikre videndeling mellem myndigheder, erhvervsliv og forskningsverdenen. Rådet har i 2021 drøftet de overordnede linjer og givet input til regeringens cyber- og informationssikkerhedsstrategi. Ud over rådets faste møder har der været gennemført en række adhoc-møder om bl.a. coronapasset, kørekort- og sundhedskort-app'en samt sikkerhedsmæssige udfordringer ved overgangen fra NemID til MitID. Henrik Larsen er i forbindelse med lancering af den nye cyber- og informationssikkerhedsstrategi blevet genudpeget til rådets fornyede mandatperiode 2022-2023.

Uddannelses- og forskningsmiljøet er endvidere repræsenteret i rådet ved professor Jens Myrup Pedersen, Aalborg Universitet og lektor Christian Damsgaard Jensen, DTU.

3.2.5 Videndeling blandt ligesindede i Rådet for digital sikkerhed

DKCERT er medlem af Rådet for Digital Sikkerhed med Henrik Larsen som bestyrelsesmedlem.[31] Endvidere deltager medarbejderne ved DKCERT i visse af Rådets arbejdsgrupper i det omfang, der er faglig sammenhæng med opgaveløsningen. Deltagelse i arbejdsgrupperne er med til at nuancere problemstillingerne og øge DKCERTs medarbejderes netværk og viden. Rådet er en uafhængig medlemsorganisation, der 'arbejder for at fremme et trygt og frit digitalt samfund for alle'. Foreningen deltager i debatter og høringer om udspil fra regeringen og EU ud fra den målsætning om at understøtte et samfund med god balance mellem effektiv brug af moderne teknologi, beskyttelse mod digitale trusler og den enkeltes ret til privatliv.

3.2.6 International videndeling

CERT (CSIRT'erne)for de fem nordiske forskningsnet holder videomøder sammen med NORDUnet-CERT en gang om måneden. [32] På møderne diskuterer deltagerne aktuelle sikkerhedshændelser og erfaringer med værktøjer og metoder. I 2021 varetog DKCERT rollen som netværkets mødeleder, der på årsbasis går på skift mellem de nordiske lande.

Fra 30. november til 2. december 2021skulle NORDUnet tecnical workshop være gennemført i Danmark med et sikkerhedsspor og et sidemøde med de nordiske forskningsnet-CERT'er. Men workshoppen, som normalt afholdes hvert andet år, måtte aflyses pga. genopblussen af corona-pandemien.

I fjerde kvartal af 2021 er der påbegyndt et nordisk samarbejdsprojekt om sikkerhed, finansieret af NORDUnet-samarbejdet. Det handler bl.a. om samarbejde om MISP, sårbarhedsscanninger og DDoS-beskyttelse. Flere medarbejdere fra DKCERT og DeiC deltager i arbejdsgrupperne.

DKCERT er siden 2002 akkrediteret medlem af Trusted Introducer og dermed af TF-CSIRT, der er en organisation for CERT/CSIRT'er der er hjemmehørende og mødes i Europa, men som nu optager teams fra alle geografiske regioner.[33] Netværket, der nu har omkring 450 medlemsteams, faciliteres af de europæiske forskningsnets paraplyorganisation GÉANT.

DKCERT er også siden 1993 medlem af FIRST.org (Forum of Incident Response and Security Teams), som er en organisation for p.t. 622 CERT/CSIRT/PSIRT-teams for 99 lande.[34] DKCERT-medarbejdere deltager i et årligt regionalt seminar for Europa samt i årskonferencen og generalforsamlingen.

I 2021 blev årskonferencen og generalforsamlingen gennemført online.

Endvidere deltager Henrik Larsen i den globale Academic Security SIG, der mødes fysisk en gang årligt i forbindelse med FIRSTs årskonference og en til to gange via videokonference, i 2021 alene virtuelt.

[31] https://www.digitalsikkerhed.dk
[32] CERT® var fra 1997 til 2021 et registreret varemærke og stod oprindeligt for Computer Emergency Response Team. Det mere generiske CSIRT (Computer security incident response teams) er i dag mere almindelig anvendt. DKCERTs officielle navn er Danish Computer Security Incident Response Team)
[33] https://www.trusted-introducer.org/, https://tf-csirt.org/
[34] https://www.first.org/members/map

3. Året i tal og ord

Henrik Larsen deltager i GÉANT's SIG-ISM (Special Interest Group Information Security Management) . SIG-ISM beskæftiger sig med de nationale forsknings- og uddannelsesnetværks (NRENs) interne sikkerhed og har halvårlige møder, heraf et årligt fællesmøde WISE Community, som er et globalt netværk for sikkerhed i forsknings-it-infrastrukturer (bl.a. udsprunget af CERN). I 2021 var møderne virtuelle.

3.2.7 Nyhedsformidling

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

Artiklerne publiceres dagligt eller næsten dagligt og omhandler trusler, sårbarheder, hændelser og andre forhold, der har relevans for sikkerhedsdagsordenen i Danmark.

DKCERT modtager hver dag et globalt nyhedsklip med cybersikkerhedsnyheder fra en af vores samarbejdspartnere. Det gør, at mange af nyhederne baserer sig på internationale medier. Vi udvælger dem, der er relevante i en dansk kontekst og perspektiverer dem ind i danske forhold med udgangspunkt i universitets- og forskningssektoren.

Hensigten med den tilgang er at brede en forståelse af cyber- og informationssikkerhed ud som understøtter vores modtageres viden om betydningen handlinger og adfærd i forhold til informationssikkerheden – både i en professionel og en privat sammenhæng.

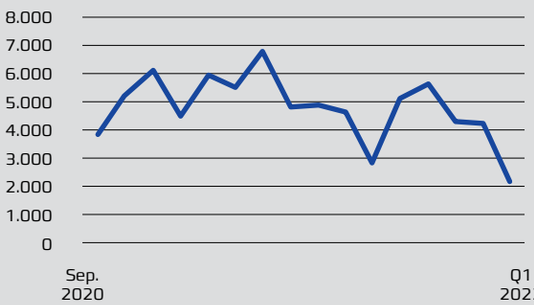
Hver mandag udsender DKCERT et nyhedsbrev. Hidtil er det sendt til fem forskellige målgrupper: Det sikkerhedsprofessionelle segment ved uddannelses- og forskningssektoren, øvrige ansatte ved forskningsnetinstitutionerne, DKCERTs interessenter generelt, borgere og små og mellemstore virksomheder. Endelig sendes nyhedsbrevet til pressen. I 2022 får DKCERT ny system til design og udsendelse af nyhedsbrevene. I forbindelse med omlægningen vil det samme nyhedsbrev blive udsendt til alle abonnenter. Udgangspunktet vil forsat være uddannelses- og forskningssektoren.

Derudover har Henrik Larsen frem til august 2021 skrevet en månedlig en klumme i Computerworld om aktuelle problemstillinger om cyber- og informationssikkerhed. Aftalen med Computerworld stoppede med udgangen af august. Klummerne, der nu kommer med mere ujævne mellemrum, bliver fremover mere sektorspecifikke og offentliggjort på DKCERTs hjemmeside samt i nyhedsbrevene.

Ved udgangen af 2021 abonnerede i alt 1.558 personer på et af DKCERTs nyhedsbreve. Tallet er steget en smule i forhold til 2020, hvor nyhedsbrevet havde 1.539 modtagere.

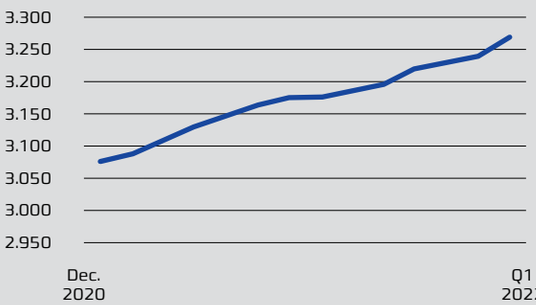
Figur 7: Unikke sidevisninger på cert.dk fra 1. januar 2021 til 31. marts 2022

Cert.dk havde i 2021 56.783 unikke pageviews. Antallet er faldet i forhold til 2020, hvor det var 81.288 og 78.976 i 2019.



Figur 8: DKCERT på Twitter i 2021 og frem til 31. marts 2022.

DKCERT havde ved udgangen af 2021 3257 følgere på Twitter. En stigning fra 3074 i 2020. I første kvartal er der sket en yderligere stigning, særligt i februar og marts, sandsynligvis som følge af krigen i Ukraine.



Klummer

KLUMMER I COMPUTERWORLD
Henrik Larsen har frem til august 2021 skrevet en klumme i Computerworld, hvor der sættes spot på en aktuel problemstilling i forhold til cyber- og informationssikkerhed.

> **#Hvadgørduselv?** (januar)
DKCERT afprøver en ny måde at formidle adfærdstal for at se, om det kan ændre adfærden.
Vil du være med?
https://cert.dk/da/klumme/2021-01-29/%23Hvadgoerduselv%3F

> **De offentligt ansatte i et dilemma** (februar)
Er offentligt ansatte selv i stand til at vurdere om regler og retningslinjer er nødvendige? Der er ikke nødvendigvis balance mellem sikkerhed, brugervenlighed og effektivitet (økonomi) i den offentlige sektor.
https://cert.dk/da/klumme/2021-03-01/De-offentligt-ansatte-i-et-dilemma

> **Alle kan lære af Exchange server-sårbarheden** (marts)
Årets første store hackerangreb var et lærebogseksempel på de mekanismer, der hersker i cyberkriminalitetsmiljøet og viser vigtigheden af, at man kender sin forretning. Her er de tre vigtigste pointer.
https://cert.dk/da/klumme/2021-26-03/Alle-kan-laere-af-Exchange-server-saarbarheden

> **Så tal dog om informationssikkerhed** (april)
Samtale fremmer forståelsen og viden. Går vejen til højere sikkerhed gennem samtalen og mere kommunikation? Ja – DKCERTs Trendrapport 2021 er på gaden.
https://cert.dk/da/klumme/2021-29-04/S%C3%A5-tal-dog-om-informationssikkerhed

> **Er dine forskningsinformationer i fare?** (maj)
PET og UFM har udgivet en publikation, der burde være pligtlæsning for alle, der arbejder med forskning.
https://cert.dk/da/klumme/2021-28-05/Er-dine-forskningsinformationer-i-fare%3F

> **Yes, brugervenligheden er tilbage!** (juni)
Danmark er på vej tilbage i balance, efter at Coronavirus i vinteren 2020 disruptede forholdet mellem brugervenlighed, sikkerhed og økonomi i det danske samfundssystem.
https://cert.dk/da/klumme/2021-25-06/Yes-brugervenligheden-er-tilbage%21

> **Lad os sammen aflive en myte: Sikkerhed er ikke gratis** (august)
Informationssikkerhedsområdet er præget af mange myter, fx at det er en teknisk disciplin. Den største myte er dog, at sikkerhed skulle være gratis. Får vi aflivet den myte, så er vi kommet rigtigt langt.
https://cert.dk/da/klumme/2021-30-07/Lad-os-sammen-aflive-en-myte-Sikkerhed-er-ikke-gratis

3. Året i tal og ord

3.3 TJENESTER

3.3.1 DPO-tjenesten

2021 har været et begivenhedsrigt år for DPO-tjenesten (DPO=Data Protection Officer, databeskyttelsesrådgiver) og persondatabeskyttelsen. Nedlukning af samtlige uddannelsesinstitutioner vanskeliggjorde naturligvis tjenestens arbejde, som ellers er præget af, at DPO-tjenestens tre medarbejdere har deres faste gang på institutionerne.

I midten af året stoppede den hidtidige leder af DPO-tjenesten Morten Eeg Ejrnæs Nielsen, og i september blev Lene Dehn ansat som ny konsulent. Lene kom fra stilling som CISO i Lægeforeningen. Teamet i DPO-tjenesten består derfor af Helle Meldgaard og Susanne Groth, der opererer med udgangspunkt i Århus, og Lene Dehn, der tager sig af de østdanske kunder.

Kunderne

Kundemæssigt var året ligeledes præget af store forandringer. Fra januar 2021 overtog DKCERT DPO-funktionen hos en række maritime skoler, og ved årets afslutning blev der indgået en aftale med SIMAC, Svendborg. DPO-tjenesten er derved i dag den primære enhed, der varetager DPO-funktionen for uddannelsesinstitutioner i den Maritime Klynge under Uddannelses- og Forskningsministeriet. Derudover kom Den frie Lærerskole med som ny kunde i januar 2021. Endelig er tjenesten blevet DPO for en række censorkorps i samarbejde med Censorsekretariatet på UC Syd, ligesom den fortsat betjener de tre kunstneriske skoler (Det Kongelige Akademi, Arkitektskolen i Aarhus og Designskolen i Kolding). Endvidere findes Studievalg Danmark, Professionshøjskolen Absalon, Dansk Dekommissionering og It-Universitetet på kundelisten.

Blandt de eksisterende kunder har der ligeledes været udskiftning. Roskilde Universitet besluttede at hjemtage DPO-funktionen ved en intern udnævnelse. Brugen af DPO-tjenesten har dog udviklet sig, da en del institutioner efterhånden føler sig mere rustet til selv at varetage en større del af de opgaver, der følger med databeskyttelsesforordningen. DPO-tjenesten er dog stadig tilknyttet institutionerne, men arbejdet har ændret karakter.

DPO-tjenesten tilbyder fx vikariater. Denne service har oplevet en opblomstring i 2021. Medarbejdere med et godt kendskab til databeskyttelsesforordningen er eftertragtede, så ofte er vikariaterne opstået i forbindelse med, at den eksisterende DPO er fratrådt eller på anden måde har været fraværende i stillingen i kortere eller længere perioder. I løbet af året har DPO-tjenesten været vikar på Syddansk Universitet, et vikariat der afsluttes i marts måned 2022, og i december indgik DKCERT en aftale om et DPO-vikariat på Københavns Universitet, indtil en ny DPO bliver ansat pr. 1. april 2022.

I DPO-tjenesten ser vi tre tendenser i forhold til kunderne. Institutioner i uddannelses- og forskningssektoren bliver mere og mere modne i forhold til at forstå GDPR-mæssige krav og implementering, dvs. compliance. De har svært ved at rekruttere DPO'er og sikkerhedskonsulenter med de rette kompetencer. Endelig oplever vi, at opgaven udvikler sig til også at omfatte rådgivning inden for anden lovgivning og informationssikkerhed.

3. Året i tal og ord

DPO Netværket
Siden 2018 har DKCERT's DPO-tjeneste drevet et DPO-netværk. Her mødes DPO'er ved de danske universiteter, professionshøjskoler og kunstneriske skoler fire gange årligt til erfaringsudveksling og videndeling om praksis og tolkning af GDPR. Derudover sker der på ad-hoc basis videndeling, der giver mulighed for perspektivering og afklaring af spørgsmål i den daglige drift af GDPR, som til en vis grad imødegår DPO'ers behov for et fagligt kollegaskab. DPO-netværket og ad hoc-videndelingen havde i 2021 fortsat stor opbakning og medvirkede dermed til at sikre fælles kurs på tværs af institutionerne.

3.3.2 TeleDCIS er flyttet til Teleindustrien

DKCERT har til og med 2021 været hjemsted for telesektorens decentrale cyber- og informationssikkerhedsenhed, TeleDCIS, som er af de seks enheder, der har været oprettet siden den forrige nationale cyber- og informationssikkerhedsstrategi dikterede det. Aftalen kom i stand, efter at de danske teleoperatører i 2019 etablerede en TeleDCIS-forening og outsourcede den operative opgave til DKCERT.

Aftalen med TeleDCIS-foreningen blev afsluttet med udgangen af 2021, hvorefter foreningen hjemtog opgaven. TeleDCIS har nu adresse hos Teleindustrien.

3.3.3 Awarenestjenesten Phish kan teste agtpågivenheden overfor phishingtrusler

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

I 2021 har DKCERT ikke haft efterspørgsel på phishingawareness-tjenesten, formentlig pga. travlhed i forbindelse med corona og manglende opmærksomhed på muligheden.

3.3.4 Beredskabsøvelser – håndtér en hændelse som i den virkelige universitetsverden

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

3. Året i tal og ord

CLAW er en workshop med en interaktiv krise-øvelse, som giver deltagerne mulighed for i et realistisk scenarium at afprøve de forskellige aktiviteter og fagligheder, der skal i spil i forbindelse med håndtering af kriser. Beredskabsøvelserne blev oprindeligt udviklet som analoge to-dags-workshops, men har i 2020 og 2021 været gennemført som virtuelle en-dags beredskabsøvelser. Hver deltager får tildelt en rolle som hhv. CISO, sikkerhedstekniker, netværkstekniker eller presserådgiver. I løbet af øvelsen bliver rollerne stillet en række spørgsmål og dilemmaer, som man under stort tidspres skal håndtere, som var det i den virkelige verden.

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

3.3.5 Universitetssektorens MISP – deler indsigt om events

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

MISP er en 'Malware Information Sharing Platform', hvor man systematisk deler viden om sikkerhedshændelser og angreb.[35] I dag bruger mere end 6000 organisationer verden over MISP.[36]

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

En MISP kan også automatisk samle data fra flere kilder. På denne måde behøver aktører ikke gennemgå adskillige varselsmails fra flere abonnementskilder for at skabe et overblik over sager, der skal reageres på. Ved gennemgang af disse informationer er det muligt for aktører at få en hurtigere forståelse af trusler og relevante sårbarheder i egne systemer.

MISP'en er modulerbar og kan – afhængig af konfigurationen – implementeres med henblik på deling af viden med andre sektorer, brancher eller organisationer, både nationalt og internationalt. I Danmark er der en fælles MISP for det, der hidtidigt har været betegnet som samfundskritiske infrastruktursektorer, tele, finans, søfart, sundhed, energi og transport.

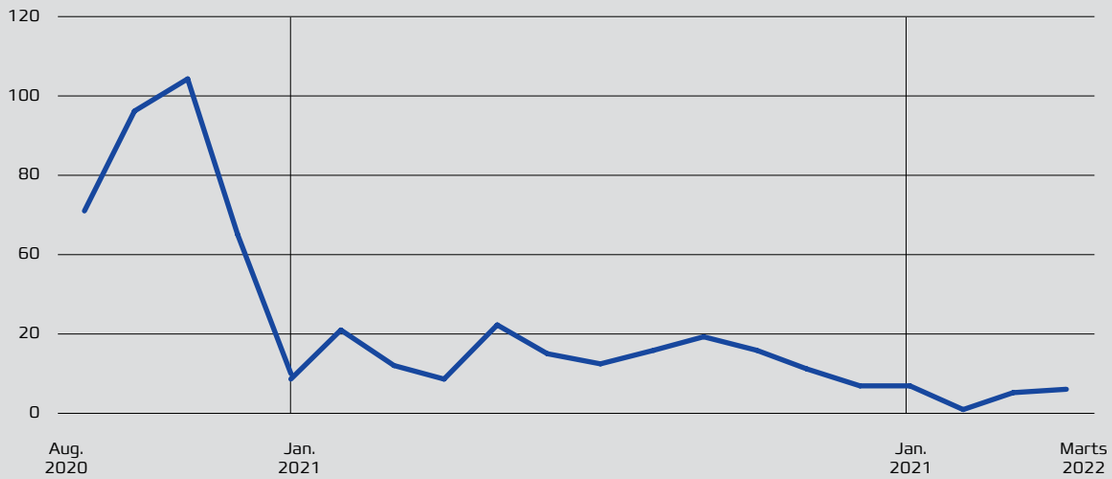
Universitetssektorens MISP er i første omgang sat op til at dele information mellem aktørerne internt i sektoren, men vil kunne dele oplysninger med eller importere fra en kommende nordisk MISP mellem de fem nordiske forskningsnet. Den vil også kunne tilkobles den omtalte sektorfælles MISP, idet man kan 'tagge' hændelserne til at blive delt inden for speficikke grupper i MISP'en.

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

3. Året i tal og ord

Figur 9: Hændelser i universiteternes MISP

Antal hændelser i universiteternes MISP siden pilotdriften i juli 2020. Samlet har der været registreret 187 nye events i 2021, svarende til 15,5 pr. måned.

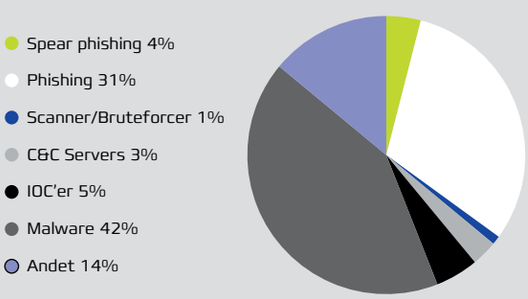


Figur 10: Hændelser fordelt på kritikalitet

Hændelser i universitetssektorens MISP fra 1. januar 2021 til 31. december 2021 fordelt på kritikalitet. Fordelingen af hændelser i MISP'en viser, at der er relativt mange high-risk hændelser. Det er op til det enkelte universitet at indrapportere hændelser og vurdere hændelsernes alvorlighedsgrad ud fra egen vurdering af hændelsens konsekvens. Det giver dermed en valid indikation af, hvor alvorlig hændelsen er.

Figur 11: Hændelser registreret i MISP

Fordelingen af hændelser, der er registreret i MISP i 2021. Fordelingen efter hændelsestype viser, at størsteparten af de indrapporterede hændelser vedrører malware (42 pct) og phishingangreb (31 pct), mens spear phishing-angreb er begrænset til fire procent.



4. Det eksterne perspektiv

Fem af DKCERTs samarbejdspartnere giver her indblik i fem forskellige uddannelser i cybersikkerhed.

Hvad er den bedste uddannelse i cybersikkerhed? Hvilken ville du vælge?

Der er mange uddannelser i cybersikkerhed, der hver henvender sig til hver deres målgruppe.

Vi har inviteret fem af DKCERTs samarbejdspartnere til at skrive et indlæg om den uddannelse, de udbyder eller har gennemført i cyber- og informationssikkerhed.

Bidragyderne er:

> Linda Mostrup Pedersen,
Founding Partner, happy42

> Henrik Kramselund Jereminsen,
adjunkt, Københavns Erhvervsakademi KEA

> Jens Myrup Pedersen,
professor, Aalborg Universitet

> Christian Damsgaard Jensen,
lektor, DTU

> Mikkel Nilsson,
Chef for produkt, Cyber, Tryg

4. Det eksterne perspektiv

4.1. CYBERSKILLS - EN INDSATS DER SKAL UNDERSTØTTE FÆLLESKAB OG FAGLIGHED

AF LINDA MOSTRUP PEDERSEN,
FOUNDING PARTNER, HAPPY42

Cyberangreb er blevet hverdagskost for danske virksomheder. I takt med en øget digitalisering stiger truslerne og samtidig også behovet for kvalificeret arbejdskraft, men vores talentpulje indenfor cybersikkerhed i Danmark er stadigvæk for svagt. Rekruttering af talenter starter for sent i fødekæden, og der er derfor et behov for at vække interessen for cybersikkerhed tidligt hos de unge, og dermed være med til at præge deres uddannelsesvalg.

Af den årsag blev CyberSkills sat i søen i oktober 2020. Projektet skal blandt andet udvikle communities, så unge med interesse for cybersikkerhed har mulighed for at dyrke og fastholde deres interesse – samtidig med, at de kan dygtiggøre sig yderligere og være en del af et fællesskab.

I Cyberskills udvikles undervisningsmaterialer, der både kan bruges i det formelle uddannelsessystem, og som samtidigt understøtter community-opbygning – dermed bidrager projektet til at øge interessen for cybersikkerhed, og samtidigt skabe de fællesskaber hvor interessen kan dyrkes.

De unge talenter har manglet et fællesskab
Vi ved, at fællesskaberne er særligt vigtige i ungdomsårene, når de unge skal vælge sig ind på en specifik faglighed. De unge er i en periode af deres liv, hvor de skal finde sig selv, men hvor spejling og feedback fra ligesindede er afgørende, særligt når vi ser på karrierevalg.

Det har derfor været tydeligt for os at mærke, hvordan de unge sætter stor pris på dét, som bliver gjort for dem i forhold til at samle unge med interesse for cybersikkerhed. En taknemlighed for, at nogen hjælper dem med at lave samlinger, mobilisere indsatser der går på tværs af byer og alder, så de får mulighed for at udvide deres netværk med andre med samme interesse - hvor de dygtige kan lære fra sig, og nybegyndere kan blive inspireret af rollemodeller.

Det fysiske samvær kan aldrig erstattes af online
CyberSkills blev igangsat under en corona-nedlukning og havde derfor svært ved at initiere fysiske aktiviteter fra start, og på trods af at online-events og online mødesteder fungerede som en substitut, kunne vi også se at de unge pludseligt så værdien af det fysiske samvær - og at det sædvanlige fællesskab bare kan noget særligt. De ytrede derfor selv konkrete ønsker om fysiske events, så snart det var muligt.

Så da verden åbnede op igen, har der været fuldt booket til alle vores arrangementer. I 2021 har der været afholdt mere end 50 CyberSkills arrangementer med mere end +2000 deltagere på tværs af landet.

Temaer har været alt ligefra logning, privacy, kryptografi, cyber threat intelligence til cyber awareness. Målet har været at give de unge hands-on øvelser, så de kan styrke deres kompetencer, samtidig med at de føler sig som en del af et fællesskab.

Efter lange snakke og interviews med de unge har det været tydeligt, at det handler om at være sociale omkring det faglige. At de synes, at det er fedt, at de kan tale om faglige ting med ligesindede, som deler samme passion, som de måske har svært ved at finde i deres normale klasse. Derfor ved vi, at CyberSkills kan gøre en forskel.

Målet er at få faglighed og fællesskab til at gå op i en højere enhed!
Med CyberSkills tror vi på, at vi kan få de unge cybertalenter til at blive endnu dygtigere og endnu mere passioneret, hvis vi kan få faglighed og fællesskab til at gå op i en højere enhed. Hvis vi med CyberSkills får opbygget det stærke sociale fællesskab, hvor de unge kan dyrke deres interesse for cybersikkerhed, så ved vi også, at de arbejder hårdere og mere vedholdende med det faglige.

I det fælleskab, både det fysiske og det virtuelle, kan de nemlig sparre med hinanden og på den måde møde de faglige udfordringer mere konstruktivt og med langt større faglig selvtillid, når de får opbakning fra fællesskabet.

4. Det eksterne perspektiv

CyberSkills handler også om udvikling af fagligt uddannelsesmateriale
Udover at etablere communities har Akademiet for Talentfulde Unge i regi af CyberSkills etableret et talentakademi indenfor cybersikkerhed. Alle pladser blev 'udsolgt' i første runde. Det viser, at de unge talenter har en interesse for feltet.

Derudover har universiteterne arbejdet på højtryk for at få udviklet uddannelsesmateriale inden for eksempelvis etisk hacking, privacy, trusselsvurderinger m.m., som er tilpasset faglige mål og niveauer på de forskellige uddannelsesniveauer.

Vi oplever en stor opbakning fra underviserne til at give feedback og involvere sig aktivt i udviklingsprocessen, da der virkelig er behov for aktuelt materiale, de kan anvende i undervisningen.

Cybermissionen - Et fagligt forløb i samarbejde med Styrelsen for It og Læring
Afslutningsvis har CyberSkills også igangsat et samarbejde med Styrelsen for It og Læring omkring Cybermissionen. Cybermissionen er et fagligt forløb, hvor elever på ungdomsuddannelser skal blive mere bevidste om vigtigheden af it-sikkerhed og udvikle en forståelse for, hvad det indebærer både fra et teknisk, menneskeligt og samfundsmæssigt perspektiv.

Styrelsen for It og Læring, står bag Cybermissionen sammen med CyberSkills med inddragelse af bla. TDC NET og Microsoft Development Center Copenhagen. Til Cybermissionen 2021 deltog mere end 7.000 elever fra ungdomsuddannelserne. Det var første gang at tilbuddet blev givet til ungdomsuddannelserne, og den enormt flotte tilslutning viser, at der er stor interesse blandt underviserne til at inddrage cybersikkerhed som en aktiv del af undervisningen.

CYBERSKILLS
CyberSkills realiseres af Akademiet for Talentfulde Unge, Aalborg Universitet, Danmarks Tekniske Universitet, Copenhagen Business School, It-Universitetet, Happy42, Forsvarets Efterretningstjeneste og Industriens Fond, der desuden støtter projektet med 17,4 mio. kroner.

4. Det eksterne perspektiv

4.2. DANMARKS FØRSTE KANDIDATUDDANNELSE I CYBERSIKKERHED UDDANNER SPECIALISTER

AF JENS MYRUP PEDERSEN,
PROFESSOR, AALBORG UNIVERSITET

Aalborg Universitet (AAU) i København har siden september 2020 uddannet landets kommende specialister i cybersikkerhed. De første cand.cyb. dimiterer til sommer 2022.

Kandidatuddannelsen i cybersikkerhed opfylder det stadigt stigende behov for ekspertise inden for cyber- og netværkssikkerhed, så både virksomheder og offentlige institutioner får mulighed for at få tilført kompetencer, der kan forhindre og håndtere de cyberangreb og -trusler, som de står overfor.

Stærk teknisk profil og faglighed
De uddannede kandidater i cybersikkerhed får en stærk teknisk profil og en god forståelse for den kontekst, den tekniske faglighed indgår i. De studerende får viden om væsentlige anvendelsesområder og erfaring med at omsætte den tekniske viden til udvikling af løsninger, fx inden for analyse, design og implementering af sikre systemer og software, analyse og håndtering af cybertrusler og forebyggelse af cyberangreb på forskellige typer af systemer.

De studerende får efterfølgende jobmuligheder inden for en lang række af private og offentlige virksomheder samt offentlige institutioner.

Der er stor interesse for emnet og for den nye uddannelse i cybersikkerhed. Uddannelsen tiltrækker studerende med forskellige baggrunde fra både ind og udland – både tekniske profiler, men også de studerende med en blødere it-profil. Det skaber nogle gode læringssituationer, især i projektarbejdet, hvor de studerende også lærer meget af hinanden i samarbejdet og får anvendt de forskellige vinkler, de kommer med.

Cybersikkerhed er en relativt ungt fag, som først inden for de senere år blevet modnet. Mange fagligheder har været med til at bringe det til, hvor det er i dag – og erkendelsen er, at der er brug for mange discipliner for at løse de mange forskellige opgaver, som en cybersikkerhedskompetence skal løse. På de aktuelle hold er der bachelorer fra fx computer engineering, ITCOM, software engineering og datalogi, men også fra fx elektronik, medialogi og informationsteknologi.

> Diversiteten blandt de studerende styrker vores tværfaglighed og samarbejde på uddannelse, da vi kan bringe forskellige styrker i spil – og hjælpe hinanden.
> **Jacob Vejlin Jensen,**
> studerende, Cyber Security, AAU

Uddannelsen skaber desuden et fællesskab blandt studerende og undervisere, da alle deler en stor passion for cybersikkerhed.

Tæt samarbejde med erhvervslivet
Kandidatuddannelsen i Cyber Security er bygget op om gruppe- og projektarbejde, som det er kendetegnet ved AAUs uddannelser. Det betyder, at de studerende lærer at samarbejde og får mulighed for at lave projektarbejde i samarbejde med erhvervslivet. De studerende kommer således tæt på praksis og komplekse problemstillinger fra virkeligheden, og de får erfaringer med, hvordan virksomheder og organisationer udvikler og forandrer sig. Samarbejdet med erhvervslivet er en vigtig brobygger mellem uddannelser og virksomheder.

> Kurserne er praktiske, og vi arbejder med problemer fra den virkelige verden. Det er meget motiverende – og vi er altid opdateret på nyeste viden inden for cybersikkerhed.
> **Zohra Amini,**
> studerende, Cyber Security, AAU

Studenterinnovation skaber værdi for samfundet
Projektarbejdet på uddannelsen passer godt sammen med AAU's undervisningsmodel, problembaseret læring, hvor virkelige problemer er omdrejningspunktet for de studerendes læringsproces. Samtidig med, at de studerende lærer en masse, resulterer projekterne i konkrete produkter og løsninger, som kan gøre en forskel for mange mennesker og for samfundet.

En gruppe studerende fra uddannelsen i Cyber Security har fx udviklet et system, der skal beskytte danskere på internettet. Systemet kan identificere enheder, som ikke er korrekt installeret og

4. Det eksterne perspektiv

derfor bruges til ondsindede formål af hackere. Det er et stigende problem med sårbare enheder – brugerne er ikke klar over, hvordan enhederne installeres korrekt og sikkert. Og da enhederne er koblet på internettet, så kan potentielle hackere i nogle tilfælde finde frem til ejerne. Derfor har de studerende udviklet et system, der kan identificere disse usikre og sårbare enheder og dernæst sende ejerne en advarsel.

Det motiverer de studerende at arbejde på et projekt, som gør en forskel og har potentiale til at blive en public service. Når de arbejder med virkelige problemer, så opstår også en dybere mening med deres arbejde. Det er også motiverende for underviserne at se teori blive brugt i praksis til løsning af konkrete udfordringer.

Første kandidater til sommer
De første studerende på uddannelsen er her i foråret 2022 i gang med at skrive deres speciale, og efter dimitering kan mange af dem fortsætte som fuldtidsansatte i de studenterjob, de allerede har. I specialeopgaverne er der fokus på både praksisnære projekter og egentlige forskningsprojekter, som der er basis for at arbejde videre med.

Den viden, der blevet genereret her, skaber ikke kun basis for at øge kompetenceudbudet på et område, der er præget af mangel på arbejdskraft, men også øge det samlede vidensgrundlag i cybersikkerhedsmiljøet i Danmark.

> Uddannelsens fokus på virkelige problemer og den tætte kontakt til den virkelige verden, skaber en forståelse for, hvordan og hvorfor cybersikkerhed er relevant. I mine projekter har vi bl.a. arbejdet med cybersikkerhed ift. droner og smart-homes. Vi lærer mange forskellige teknologier, og det er motiverende, at vi er med til at gøre verden mere sikker.
> **Kim Christensen,**
> studerende, Cyber Security, AAU

CYBER SECURITY-UDDANNELSEN

Varighed:
2 år

Sprog:
Engelsk

Hvor:
Aalborg Universitet, København

De studerende får viden om: Cybertrusler og forebyggelse, IoT netværkssikkerhed, detektion og håndtering af cyberangreb på forskellige typer af systemer

Jobmuligheder:
De studerende kan få job i større private virksomheder og offentlige institutioner, som arbejder med udvikling af produkter og services inden for cybersikkerhed. Det kan fx være konsulentvirksomheder, politi, myndigheder og forsvar samt offentlig administration.

Læs mere om kandidatuddannelsen i cybersikkerhed her https://www.aau.dk/uddannelser/kandidat/cyber-security/

Læs mere om bacheloruddannelsen i cyber- og computerteknologi her https://www.aau.dk/uddannelser/bachelor/cyber-computerteknologi/

4. Det eksterne perspektiv

4.3 DIPLOM I IT-SIKKERHED, EFTERUDDANNELSE MED KOMPETENCER

HENRIK KRAMSELUND JEREMINSEN,
ADJUNKT PÅ KØBENHAVNS ERHVERVSAKADEMI KEA OG REGELMÆSSIG FOREDRAGSHOLDER HOS PROSA

Manglen på it-folk er tydelig, og manglen på it-sikkerhedsressourcer er skræmmende. Vi står over for et væld af trusler, og situationen forværres næsten dag for dag. Det er fakta for danske netværk, danske virksomheder og organisationer.

Vores værn er en hård kerne af it-sikkerhedsfolk, som dagligt gør deres bedste. Vi er dog for få, alt for få. Hvis man kunne klone sig selv, ville jeg straks overveje det.

Da der er mange etiske aspekter i kloning af mennesker, har jeg valgt det næstbedste, uddannelse af andre. Gennem mere end 20 år har jeg været til undervisning, foredrag, workshops og konferencer om it-sikkerhed. Jeg har også selv været med til at stable mange tilsvarende arrangementer på benene.

Da jeg så blev spurgt af KEA, om jeg kunne være interesseret i at undervise på en relativt nystartet diplomuddannelse i it-sikkerhed sprang jeg hurtigt til. Opgaven var at undervise i Netværk og kommunikationssikkerhed i februar 2019. Et kursus med formelle ECTS-point og en studieordning bagved. Fra 2021 er jeg ansat i adjunktforløb på KEA. Min opgave er sammen med et væld af dygtige kollegaer at uddanne på et fuldtidsstudium og en efteruddannelse. Jeg har mest fokus på diplom i it-sikkerhed, som er en erhvervsrettet it-sikkerhedsuddannelse som udbydes af KEA, UCL, UCN og Erhvervsakademi Aarhus. Under næsten samme studieordning kan man gennemføre kurserne som fuldtidsuddannelse, dvs som professionsbachelor i it-sikkerhed.

Den primære forskel mellem de to er at efteruddannelsen udbydes via KEA Kompetence, undervisningen er aften og det foregår i Hellerup, frem for på Nørrebro.

Hvorfor uddanne sig

Hvis vi skal ændre og forbedre sikkerheden, skal vi have viden, og det gør vi ved at uddanne og videreuddanne it-folk generelt. Tiden, hvor man kunne klare sig med MS-DOS, Telnet og FTP, er slut. Vi er nødt til at afsætte tid til at arbejde mere effektivt.

En uddannelse giver typisk et overblik over emnerne, anbefalinger i form af både processer og konkrete værktøjer. Specielt arbejder vi med en strategi, som indebærer, at man skal ikke kun vide, man skal kunne. Uddannelsen er således lagt an på løsning af konkrete problemstillinger, så man kan udføre sikkerhedsarbejde efterfølgende.

De studerende er typisk en blandet gruppe af erfarne mennesker inden for mange områder, som gerne vil mere med sikkerhed. Det kan være de ønsker at skifte fra administratorrollen til en mere styrende sikkerhedsrolle.

Vi har set, at de studerende efterfølgende er vokset undervejs i forløbet og til eksamen optræder de selvsikkert med begreber, overblik og handlekraft. Flere af de studerende har fået mere styr på opgaverne hjemme i organisationen eller har fået flere og mere interessante opgaver.

En ekstra bonus på efteruddannelsen er også, at man som underviser udbygger sit professionelle netværk med andre ligesindede.

4. Det eksterne perspektiv

Adgangskrav, fokus og niveauer
En del af forskellene mellem uddannelserne i it-sikkerhed i Danmark er adgangskrav, fokus og niveauer. Nogle uddannelser stiller færre formelle krav, og andre kræver næsten en kandidatuddannelse for at komme gennem nåleøjet. Vores uddannelse adskiller sig ved, at man ud over optagelse gennem formelle uddannelser kan blive vurderet med den baggage, man har med fra tidligere. Det kan betyder, at man kan starte på uddannelsen, men ofte kan enkelte fag springes over.

Det ser jeg som en stor fordel, idet vi har mange dygtige it-folk ude i organisationerne. De kæmper dagligt med udfordringerne, som regel med et lille budget, få hænder, men med følelsen af et stort ansvar. Mange har ikke en formel uddannelse eller it-uddannelse overhovedet. En del har ikke været til eksamen i 15-20 år. De har til gengæld et væld af leverandørkurser og certificeringer. Jeg har selv taget CISSP og Juniper certificeringer samt andre tilbage i tiden. De har ofte et andet og mere snævert fokus. Vores fokus er bredt.

Når vi underviser i sikkerhed er der store sammenfald i emnerne på tværs af uddannelserne. Eksempelvis er emner som firewalls, Virtual Private Network (VPN) og Transport Layer Security (TLS) gennemgående nødvendige for at kunne begå sig inden for sikkerhed. Det er derfor ingen overraskelse at disse emner også er at finde i vores studieordning.

Vi bygger broer
Vi bygger dog en bro mellem tekniske discipliner med netværkspakker, kryptering og op til governance, således at man kan begå sig på flere niveauer - uden at man dog behøver at være ekspert i det hele. Det er et fundament til at bygge videre på, i den retning som den studerende efterfølgende finder mest interessant. Så hvis man vil være ekspert i teknikken, har man med kurserne på diplomniveau fået viden, færdigheder og kompetencer. Samlet udgør det en begrebsverden, som gør én i stand til at gå direkte til faktiske problemstillinger og arbejde intenst med eksempelvis netværkssikkerhed.

De færdiguddannede studerende kan også begå sig i mange forskellige roller i organisationen - og der er brug for både tekniske og ikke-tekniske kompetencer nu og i fremtiden.

Jeg vil mene, at vi med den uddannelse opnår nogle mere helstøbte profiler, som bedre kan vurdere de mange tiltag. Det betyder, at de bliver mere effektive som ansatte, sikkerhedstiltagene bliver mere effektive og fanger mere. Selve organisationen får også en mere omkostningseffektiv løsning af opgaverne, ved at de passende tiltag prioriteres og udgifter til smarte superløsninger som man tror kan alt, måske kan undgås.

Den rigtige uddannelse af medarbejdere er en god forretning.

FAKTA OM DIPLOMUDDANNELSEN

Diplomuddannelsen i it-sikkerhed hører under åben uddannelse og er tilrettelagt som en deltidsuddannelse over op til tre år. Forløbet svarer til et års fuldtidsstudium og har et omfang af 60 ECTS. Uddannelsen skal afsluttes senest seks år efter den er påbegyndt. Obligatoriske moduler er Netværks- og kommunikationssikkerhed (10 ECTS), Softwaresikkerhed (10 ECTS) og it-governance (5 ECTS).

Valgfag er typisk 5 ECTS og kan kombineres med fag uden for uddannelsen, fx Data science for it-sikkerhed, Hændelses- og trusselshåndtering, Introduktion til it-sikkerhed, Netværkspenetrationstest, SIEM og loganalyse og Systemsikkerhed (10 ECTS).

Adgangskravene er baseret på relevant erhvervserfaring og adgangsgivende uddannelse som eksempelvis erhvervsakademiuddannelse som datamatiker eller it-teknolog. Hvis man ikke opfylder kravene, kan man muligvis optages på baggrund af en Realkompetencevudering (RKV).

Målgruppen er medarbejdere i softwarevirksomheder, hvor en stor del af jobbet indeholder it-sikkerhed. Målgruppen omfatter også it-sikkerhedsmedarbejdere i finanssektoren, i det offentlige og medarbejdere dedikeret til it-sikkerhed i større it-virksomheder eller virksomheder med it-afdeling.

4. Det eksterne perspektiv

4.4 MASTER OF CYBER SECURITY PÅ DTU

Masteruddannelsen henvender sig til erfarne sikkerhedsfolk, der har behov for videreuddannelse.
Mange virksomheder og offentlige organisationer har svært ved at finde kvalificerede medarbejdere med kompetencer inden for cybersikkerhed.

En kortlægning af behovet udgivet af Erhvervsstyrelsen i december 2019 viser en omfattende mangel på kvalificerede medarbejdere inden for alle områder af cybersikkerhed.[37] I den seneste rapport fra ESG og ISSA svarer 95 pct. af de adspurgte, at personalemanglen ikke er blevet mindre de seneste fem år; 44% mener endda, at den er blevet værre.[38]

Selv om erhvervsakademier og universiteter har øget udbuddet af kurser og uddannelser inden for cybersikkerhed de seneste år, er antallet stadigvæk utilstrækkeligt til at dække behovet. Det afhjælper heller ikke manglen på erfarne cybersikkerhedsmedarbejdere. Der er altså behov for et generelt løft på tværs af branchen gennem videre-/efteruddannelse.

Når virksomheder opkvalificerer deres egne folk inden for cybersikkerhed, får de medarbejdere, der kender arbejdspladsens kultur, forretningsgange og forretningsområder.

Det er på den baggrund, at DTU har oprettet deltidsmasteruddannelsen Master of Cyber Security.[39] Uddannelsen videreuddanner erfarne it-medarbejdere til at gå foran og lede arbejdet med cybersikkerhed i en organisation. Det første hold med 10 deltagere fra offentlige og private virksomheder er begyndt på masteruddannelsen i sommeren 2021.

Målgruppe
Masteruddannelsen kan følges af enhver med en it-baggrund, som ønsker en solid faglig fundering inden for cybersikkerhed. Men uddannelsen retter sig særligt mod styrkelse af den faglige profil blandt medarbejdere, der allerede varetager eller ønsker at kvalificere sig til it-sikkerhedsledelsesopgaver i organisationer. Derfor fokuserer masteren på at give de studerende en forståelse for de ledelses- og forretningsmæssige aspekter af cybersikkerhed, såvel som de teoretiske og teknologiske aspekter.

Målgruppen omfatter eksisterende it-sikkerhedsledere (CIO, CSO, CISO, CTO, CDO/DPO), som ønsker en bredere teoretisk og teknologisk indsigt for at kunne indgå i en ligeværdig faglig dialog med specialiserede medarbejdere, eksterne konsulenter og leverandører.[40] De kan fx have en generel it-baggrund, enkelte certificeringskurser inden for it-sikkerhed og personlig interesse og erfaring fra arbejde med it-sikkerhed i organisationen og som følge deraf er blevet forfremmet til en lederstilling.

Med til målgruppen hører også den større gruppe af medarbejdere, der har ansvar for udvikling og/eller drift af centrale produkter, systemer og infrastruktur, hvor cybersikkerhed udgør et væsentligt element. Dette inkluderer produkt- og projektledere, it-arkitekter, netværksarkitekter og -administratorer.

[37] Højbjerre, Brauer og Schultz: Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark, Erhvervsstyrelsen, december 2019.
[38] Jon Oltsik og Bill Lundell: The Life and Times of Cybersecurity Professionals 2021 - Volume V, ESG Research Report, Enterprise Security Group, July 2021.
[39] En deltidsmasteruddannelse retter sig mod studerende med en bacheloruddannelse eller lign, som har mindst 2 års erfaring inden for området og ønsker at videreuddanne sig samtidigt med, at de er i arbejde. Uddannelsen svarer typisk til et års fuldtidsstudium, som læses i løbet af 2-4 år.
[40] En CIO (Chief Information Officer) er ansvarlig for, at systemers infrastruktur understøtter organisationens strategi. En CSO (Chief Security Officer) er ansvarlig for alle aspekter af organisationens fysiske og tekniske sikkerhed (herunder identifikation af aktiver), mens en CISO (Chief Information Security Officer) er ansvarlig for at undgå eller afbøde trusler mod organisationens data og it-systemer. En CTO (Chief Technology Officer) svarer på mange måder til en CIO, men ansvaret retter sig mere mod de anvendte teknologier. En CDO (Chief Data Officer) eller DPO (Data Protection Officer) er ansvarlig for organisationens indsamling og håndtering af data, herunder beskyttelse af persondata i henhold til Persondataforordningen (GDPR).

4. Det eksterne perspektiv

Overblik og indhold af Master of Cyber Security
Uddannelsen foregår på engelsk og består af fire semestre, der hvert har et overordnet tema: I første semester er temaet it-sikkerhedsledelse og governance. I andet semester gennemgås de teknologier og systemer, der udgør it-sikkerhedsinfrastrukturen. I tredje semester er der fokus på udvikling og drift af sikre applikationer og systemer. I fjerde og sidste semester skrives masteropgaven. Den overordnede struktur er vist i figuren.

Semester	Kususprogram, Master of Cyber Security		
1		**It-sikkerhedsledelse og governance**	
	Security Principles	It-Security Governance	Risk Management
2		**It-sikkerhedsinfrastruktur**	
	Identity & Access Management	Enterprise Security Architectures	Consultancy Project
3		**Sikre applikationer og systemer**	
	Application Security	Data Protection & Privacy	Trends in Cybersecurity
4		**Master Project**	

1. semester: It-sikkerhedsledelse og governance
Det første semester giver en bred introduktion til de fundamentale begreber og principper inden for cybersikkerhed, samt et solidt grundlag for god It-sikkerhedsledelse og en risikobaseret tilgang til It-sikkerhedsarbejdet, der tager højde for organisationens risikoprofil. De studerende får også en indføring i god praksis omkring It-sikkerhedsarbejde, herunder hvordan politikker og kontroller afhænger af aktuelle trussels- og risikovurderinger.

2. semester: It-sikkerhedsinfrastruktur
Det andet semester fokuserer på sikkerhed i de systemer og den infrastruktur organisationer benytter til at opnå deres strategiske mål. Dette introducerer fundamentale principper omkring opbygning og drift af It-systemer og -infrastrukturer og de værktøjer og teknologier, der er nødvendige for at opnå den tilstrækkelige sikkerhed. Der vil være et særligt fokus på identitets- og adgangskontrolsystemer, da disse spiller en central rolle i at regulere adgang til data og systemer.

3. semester: Sikre applikationer og systemer
Det tredje semester fokuserer på fundamentale principper for udvikling, anskaffelse og drift af sikre It-systemer, herunder applikationer og tjenester, samt beskyttelse af persondata i henhold til Persondataforordningen. Dette giver indsigt til at lede udvikling og/eller anskaffelse af It-systemer, hvor der stilles krav til cybersikkerhed. Studerende vil desuden forstå den rolle, som systemets brugere spiller i det overordnede sikkerhedsbillede, herunder behovet for beskyttelse af deres persondata, samt hvordan de grundlæggende sikkerhedsprincipper, der blev introduceret i det første semester, realiseres i praksis.

4. semester: Masterprojekt
Det fjerde og sidste semester er afsat til den afsluttende opgave, der skal demonstrere en samlet forståelse af flere af de emner, der er blevet gennemgået på studiet. Opgaven omhandler typisk en problemstilling i den studerendes egen organisation.

Optagelse og adgangskrav
Der starter nye hold på Master of Cyber Security en gang om året i slutningen af august med ansøgningsfrist i juni. Kandidater til uddannelsen skal skrive en motiveret ansøgning, der dels dokumenterer deres uddannelse og erhvervserfaring, dels reflekterer over, hvordan uddannelsen kan hjælpe dem i deres nuværende stilling eller hjælpe dem videre i en karriere inden for cybersikkerhed. Adgangskravene følger retningslinjerne for deltidsmasteruddannelser, dvs. der kræves en relevant bacheloruddannelse eller uddannelse på tilsvarende niveau, samt minimum to års relevant erhvervserfaring efter gennemført adgangsgivende uddannelse.

4. Det eksterne perspektiv

OMFANG OG PRAKTISKE FORHOLD

- Master of Cyber Security er en deltidsmasteruddannelse på 60 ECTS point, hvilket svarer til et års fuldtidsstudium. Heraf optjenes 40 ECTS gennem kurser, 5 ECTS gennem et midtvejsprojektkursus (konsulentprojekt) udført i en af deltagernes organisationer) og 15 ECTS gennem det afsluttende masterprojekt.
- Uddannelsen tilrettelægges som deltidsundervisning inden for en tidsramme på normalt to år, idet størstedelen af deltagerne følger uddannelsen sideløbende med, at de er i job.
- Hvert kursus består typisk af 2 x 2 dage on site undervisning (fredag og lørdag i udvalgte uger), med hjemmearbejde før og mellem de to undervisningsperioder, således at den studerende arbejder aktivt med kursusmaterialet mellem møderne og via de intense moduler får et godt netværk gennem de andre studerende.
- Undervisning sker fysisk på DTU Campus i Lyngby.
- Uddannelsen koster 190.000 kr.
- Der findes flere informationer på uddannelsens hjemmeside: https://www.compute.dtu.dk/english/education/master-of-cyber-security
- Kursusbeskrivelser for de enkelte kurser findes i DTU's kursuskatalog: https://kurser.dtu.dk/
- Flere af kurserne kan tages som enkeltfag.
- Uddannelsen foregår på engelsk.

4. Det eksterne perspektiv

4.5 IT-SIKKERHEDSAMBASSADØRUDDANNELSEN PÅ FORSIKRINGSAKADEMIET

AF MIKKEL NILSSON,
CHEF FOR PRODUKT, CYBER, TRYG

Hos Tryg Forsikring er it-sikkerhed højt på agendaen – ikke blot i dagligdagen blandt medarbejderne men også over for vores leverandører, samarbejdspartnere og kunder. Det er helt indgroet i kulturen i Tryg og afgørende for en virksomhed som vores.

Vi fik et wakeup call i 2015, da Tryg blev ramt af ransomware. Dette angreb betød en skærpelse af sikkerheden i alle aspekter lige fra fysisk adgangskontrol, 2-faktor godkendelse når man arbejder hjemme, og løbende awarenesstræning blandt medarbejderne, for blot at nævne et udpluk.

Netop awarenesstræningen har stor effekt, da man ikke rent teknisk kan sikre sig mod alle angreb - så medarbejderne bliver inddraget som en del af 'Last line of Defence'. Vi bliver jævnligt trænet og udsat for eksempelvis phishing-kampagner for at undersøge, hvor mange der kan snydes til at trykke på links og måske endda indtaste brugernavne og passwords.

Forankring af viden i forretningen
It-sikkerhed er forankret i Group IT, og for at gøre det til en naturlig del i alle processer, projekter og compliance opgaver i hele virksomheden, sendte Tryg en række medarbejdere på uddannelsen Business Cybersecurity Ambassador – det der i dag hedder It-sikkerhedsambassadøruddannelsen.

Baggrunden skal findes i, at man også ønsker at forankre viden om it-sikkerhed i forretningen i Tryg, så det kan sprede sig i afdelingerne og indtænkes i de mange projekter, vi driver.

I foråret 2021 blev der oprettet en afdeling i Tryg, som skal fokusere på cyberforretningen på tværs af de nordiske lande. Vi kan se, at det er et område i vækst, da cyberangrebene er blevet flere og mere sofistikerede. Afdelingen har til opgave at koordinere aktiviteterne og sikre, at vi har løsninger, der kan understøtte kundernes behov.

FAKTA OM UDDANNELSEN

Hvor:
Foregår på Forsikringsakademiet – Rungstedgaard.

Underviser:
Kursusforløbet er udviklet i samarbejde med it-sikkerhedsvirksomheden Dubex.

Målgruppe:
Uddannelsen er målrettet medarbejdere, der:
> har interesse i og lyst til at være it-sikkerhedsambassadør i din afdeling eller team
> arbejder som produktudvikler- systemudvikler, hvor it-sikkerhed indgår som et naturligt parameter
> arbejder i projekter med fokus på digitale løsninger
> har en rolle som kulturbærer i din afdeling/team
> har kundekontakt og skal have bedre forudsætninger for at forstå erhvervskundernes it-sikkerhedssituation
> erfaring med it-sikkerhedsarbejde er ikke en forudsætning.

Opbygning
Uddannelsen er bygget op omkring 2 + 2 dage med en opgave mellem modul 1 og 2, samt en afsluttende multiple choicetest.
> Dag 1: It Governance
> Dag 2: Cyber Risk Management
> Dag 3: It Security Compliance
> Dag 4: GDPR Compliance & Information Security

Sprog:
Undervisningsmaterialet er engelsksproget, inklusive opgaven mellem første og anden del af kurset. Den afsluttende test er ligeledes engelsk.

Opgavebesvarelsen kan efter eget valgt skrives på enten engelsk eller dansk.

Selve undervisningen foregår på dansk. Underviser taler dansk og vil være behjælpelig med evt. sproglige usikkerheder i løbet af kurset.

Pris:
Pris 25.300,- ekskl. moms. (aktionær-fordelspris).

Pris for øvrige 28.300,- ekskl. moms.

Prisen omfatter undervisning, materialer, indkvartering på Rungstedgaard, middag og fremtrædende gæsteforelæsere om aftenen.

4. Det eksterne perspektiv

Uddannelsen øger indsigt i teknik, risici og lovgivning
I min rolle har jeg ansvar for rapportering, leverandøraftaler samt den strategiske udvikling af vores produkter og processer, så kundeoplevelsen optimeres.

It-sikkerhedsambassadøruddannelsen var derfor interessant for mig for at øge min indsigt i teknik, risici og lovgivning på området. Min afdeling koncentrerer sig om blikket udad mod kunderne og markedet, så det er her min interesse ligger.

Min baggrund er kommerciel, så jeg har en ikke-teknisk tilgang. Dette stemmer meget godt overens med vores mindre erhvervskunder, som vi er nødt til at kommunikere med på en meget let forståelig måde for at skabe en forståelse for nødvendigheden af it-sikkerhed.

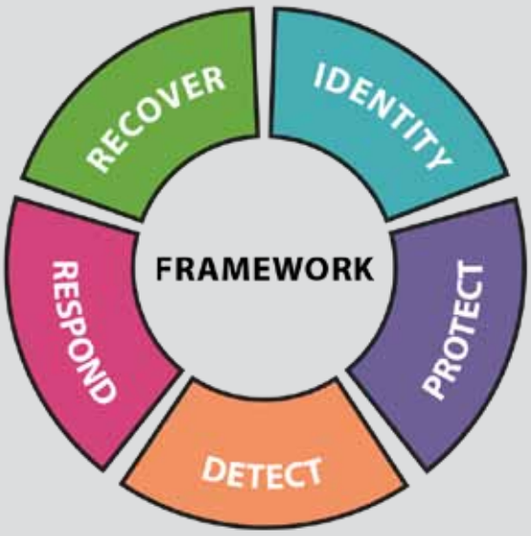
Som nyuddannet ambassadør består min rolle ikke kun i at bringe forståelsen for it-sikkerhed ind i vores dialog med kunderne. Den er lige så vigtig i forhold til vores egen sikkerhed i min afdeling i Tryg. Tryg er ligesom andre små og store virksomheder udsat for forsøg på cyberangreb, og når vi udbreder sikkerhedsforståelsen hos kunderne, skal vi også gøre det hos os selv. Det gør jeg konkret på forskellige måder i samarbejde med mine kollegaer:

- Jævnlig deling af viden fra webinarer, møder og artikler
- Generel opmærksomhed på, hvem der bør have adgang til hvilke Sharepoint sites
- Ingen fremmede folk ind gennem sluserne ved indgangen til bygningen
- Deltagelse i forskellige fora i Tryg, både i Danmark og med vores nordiske kollegaer
- Låsning af skærmen hver gang, man forlader sin plads
- Ekstra opmærksomhed på mistænkelige mails og links gennem phishingtræning, hvor et forkert klik betyder ekstra træning, mens en korrekt anmeldelse bliver kvitteret med et 'Godt gået!'.

Vi er os bevidste om, at vi trods ambassadøruddannelsen stadig kan blive ramt af cyberangreb, men vi arbejder trusselsforståelsen ind i vores kultur. Dermed tror vi på, at vi er mere agtpågivende og forberedte, hvis en cyberhændelse skulle ske.

NIST modellens fem faser
Et af de meget konkrete værktøjer, der blev undervist i på It-sikkerhedsambassadøruddannelsen er NIST rammeværktøjet, som på overskuelig vis illustrerer de nødvendige it-sikkerhedsmæssige tiltag, man bør foretage sig før, under og efter et potentielt cyberangreb.

NIST-modellen



NIST-modellen er blevet en naturlig ramme i Tryg, når vi forretningsudvikler og italesætter vores produktudbud og strategi, selv om forsikringselementet i princippet først træder i kraft i forbindelse med de to sidste faser, Respond og Recover.

I de første faser af modellen (Identify, Protect, Detect) ligger der en stor del forebyggelse og basal it-sikkerhed, som sagtens kan løftes hos især de små og mellemstore virksomheder – og hos os selv.

Et fælles sprog mellem tekniske og kommercielle medarbejdere
Cyberkriminalitet er en af de største trusler for dansk erhvervsliv. En trussel, som kun bliver større i takt med, at de danske virksomheder bliver stadigt mere digitale. De små og mellemstore virksomheder skal dog især hjælpes med at erkende incitamentet i at investere i ekstra it-

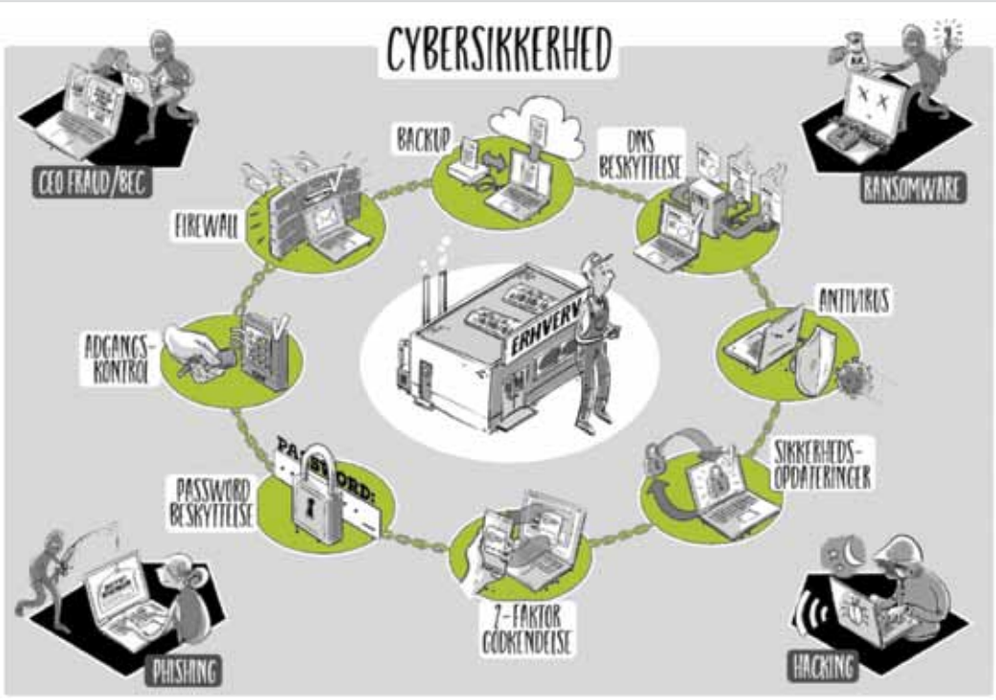
4. Det eksterne perspektiv

sikkerhed, men de bremses af en række barrierer:

- De interesserer sig ikke for området.
- De føler sig ikke udsat.
- De kan ikke overskue det.
- De har manglende økonomiske ressourcer.
- De har er usikre på gevinsten ved at investere i it-sikkerhed.

Vi arbejder løbende på at gøre de tekniske begreber mere forståelige, for vi ønsker at hjælpe med at løfte vores kunders basale it-sikkerhed, og derfor er vi nødt til selv at forstå sammenhængene.

Uddannelsen på Forsikringsakademiet har både skærpet min interesse og kendskab til et område, der normalt er forbeholdt it-ansatte, men ved at øge indsigten hos de mere kommercielle medarbejdere som mig selv, er der skabt en kobling og basis for et mere fælles sprog – både i relation til kunderne og i forhold til sikkerheden i Tryg.



Sikkerhedsbegreber illustreret i Tryg

5. Trends og anbefalinger

Med udgangspunkt i det aktuelle trusselsbillede giver DKCERT her et bud på cybertrends i 2022 og anbefalinger til hhv. ledelsen og de it-ansvarlige på uddannelses- og forskningsinstitutioner.

5.1 TRENDS 2022

Ukraine
Krigen i Ukraine øger trusselsniveauet. I endnu højere grad end tidligere vil der blive udkæmpet cyberkampe, hvor styrkerne i modsætning til de traditionelle slag er løst organiseret og autonome, hvorved også truslen fra destruktive cyberangreb uvægerligt vil blive højere. Det kan ramme de traditionelle, kritisk infrastruktursektorer i Danmark og samfundsvigtige funktioner.

> https://cert.dk/da/news/2022-02-23/CISA-advarer-om-hybrid-trussel-mod-amerikansk-kritisk-infrastruktur
> https://cert.dk/da/news/2022-03-01/Ny-malware-brugt-mod-Ukraine
> https://cert.dk/da/news/2022-03-01/Check-point-Cyberangreb-stiger-i-antal
> https://cert.dk/da/news/2022-02-24/CFCS-opfordrer-myndigheder-og-samfundsvigtige-virksomheder-til-at-styrke-cyberberedskabet

Mere politisk opmærksomhed på cybersikkerhed i kraft af introduktionen af 'samfundsvigtige funktioner'
Den nye cyber- og informationssikkerhedsstrategis bredere syn på samfundets afhængighed af it peger på samfundsvigtige funktioner fremfor alene 'kritisk infrastruktur'. Disse samfundsvigtige funktioner består af 'systemer, tjenester, processer, netværk og aktiviteter samt serviceydelser, der er nødvendige for at opretholde eller genoprette samfundsvigtige funktioner'. De vil i langt højere grad end tidligere skulle øge deres robusthed mod cybertrusler, og det stiller krav til de ansvarlige ministerområder om at oprette DCIS'er og selvstændige cybersikkerhedsstrategier.

Dette omfatter også uddannelses- og forskningssektoren, som fremover i højere grad end tidligere skal efterleve ISO27001 og de basale, tekniske minimumskrav, som også den øvrige statslige sektor er underlagt. Det må også forventes, at efterlevelsen bliver underlagt kontrol.

> https://cert.dk/da/klumme/2022-01-24/Ny-cybersikkerhedsstrategi-lanceret
> https://fm.dk/nyheder/nyhedsarkiv/2021/december/ny-national-strategi-skal-styrke-danmarks-digitale-sikkerhed/

Opmærksomhed på sikkerheden ved open source-software
I slutningen af 2021 opdagede verden den systemiske risiko ved at mange virksomheders it-systemer er afhængig af open source. Open source har på mange områder været trendsættende, hvor uafhængige it-folk sammen udvikler kode, der stilles frit og kvit til rådet for videreudvikling. Men hvem har ansvaret, når det brænder på, som vi så det ved Log4j-sårbarheden i december 2021?

Dette bragte præsident Joe Biden på banen ved et topmøde med techgiganterne i januar 2022 – og det vil givetvis være en samtale, der også bliver ført i andre lande og organisationer fremover.

> https://cert.dk/da/news/2022-01-18/Det-Hvide-Hus-inviterer-til-nyt-tech-topmoede

5. Trends og anbefalinger

Ransomwareplagen fortsætter
Ransomwareaktører har haft gode vilkår i 2021. Alvorlige sårbarheder som Proxylogon, Printnightmare og Log4shell i en lang række produkter har gjort det nemt for cyberkriminelle grupperinger og statsstøttede aktører at vælge deres ofre. Samtidig har ransomware været på dagsordenen på højeste sted, da den amerikanske præsident Joe Biden drøftede det med den russiske præsident Vladimir Putin i forsommeren 2021. Selv om visse grupper er lukket, enkeltpersoner anholdt, så vil sårbarheder altid kunne tiltrække aktører, der forsøger at udnytte dem.

> https://cert.dk/da/news/2021-12-02/FBI-beslaglaegger-2%2C3-millioner-dollars-fra-ransomware-aktoer
> https://cert.dk/da/news/2021-11-08/Det-Vilde-Vesten-i-cyberspace
> https://cert.dk/da/news/2021-10-20/Nye-metoder-fra-ransomwaregrupper
> https://cert.dk/da/news/2021-08-25/Praesidenten-inviterer-paa-kaffe

Mere fokus på sårbarhedernes betydning for sikkerheden
Med CISAs iværksættelse af det såkaldte Known Exploitable Vulnerabilities Catalogue kommer der mere fokus på krav om håndtering af sårbarheder. KEV-kataloget er CISAs publicering af kendte, udnyttede sårbarheder og krav om de føderale myndigheders håndtering af dem inden for en vis tidsfrist. Det har givet de lokale systemadministratorer en rettesnor at gå efter og de lokale ledelser et værktøj at benchmarke sig op i mod.

> https://cert.dk/da/news/2021-11-08/CISA-Ret-disse-saarbarheder
> https://cert.dk/da/news/2021-12-13/CISA-udvider-sin-saarbarhedsliste
> https://cert.dk/da/news/2022-01-17/15-nye-saarbarheder-til-CISAs-katalog

Cyberaktivismen stiger - cyberangreb som politisk våben
Der er en tendens til at cyberaktivismen stiger. CFCS skriver ganske vist i sin trusselsvurdering 2021, at truslen fra cyberaktivisme er LAV. De mange protester, der har præget 2020, har ikke ført til en stigning i antallet af cyberaktivistiske angreb på verdensplan. Men ved indgangen til 2022 er cyberangreb i forbindelse med spændingerne omkring Ukraine set anvendt som et politisk våben, ligesom det også er set i forbindelse med andre konflikter på verdensplan.

> https://arstechnica.com/information-technology/2022/01/hactivists-say-they-hacked-belarus-rail-system-to-stop-russian-military-buildup/

Supply chain-angreb
I slutningen af 2020 blev der offentliggjort oplysninger om kompromittering af softwareproduktet SolarWinds Orion. Kompromitteringen blev anvendt til installation af en bagdør ind i SolarWinds Orion. Dermed så verden det hidtil mest alvorlige software supply chain-angreb, som netop er kendetegnet ved at aktører gemmer malware i opdateringer, som leverandører utilsigtet distribuerer til sine kunder. Supply chain-angreb kan også påvirke andre elementer i forsyningskæden og er et effektivt våben, idet en leverandør intetanende bliver anvendt til ondsindet aktivitet. Tilliden til leverandøren misbruges. Log4j-sårbarheden kan på samme måde anvendes til installation af bagdøre og dermed vil et supply chain-angreb kunne sættes i værk. Supply chain-angreb er meget attraktive for cyberkriminelle at kunne iværksætte og derfor også en voksende trusselstrend, som politiske ledere har sat på dagsordenen og fået tech-samfundet involveret i.

> https://cert.dk/da/news/2021-08-25/Praesidenten-inviterer-paa-kaffe
> https://cert.dk/da/news/2021-08-26/Gigant-er-forpligter-sig-til-gigantinvesteringer

5. Trends og anbefalinger

PERSONDATATRENDS

Dataoverførsel til tredjelande

Den 4. juni 2021 vedtog Europa-Kommissionen et sæt nye Standard Contractual Clauses (SCC), der kan benyttes som overførselsgrundlag ved overførsel af personoplysninger til lande uden for EU/EØS. De nye SCC'er kunne bruges fra den 27. juni 2021, men de 'gamle' blev først ophævet fra den 27. september. Aftaler indgået på baggrund af de tidligere SCC skal dog være fornyet senest den 27. december 2022. Det forventes, at problematikken omkring overførsel af data til tredjelande stadig vil fylde meget i det kommende år.

> https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_da

Revidering af fortegnelse

Persondataforordningen trådte i kraft 25. maj 2018. Mange organisationer er nu gået i gang eller vil i gang med at revidere deres fortegnelser over behandlingsaktiviteter, efterhånden som de er blevet mere vant til at arbejde med Persondataforordningen. Revisionerne kan også ske som følge af nye vejledninger fra Datatilsynet.

> https://www.datatilsynet.dk/Media/E/5/Fortegnelse%20(3).pdf

Standardisering af GDPR gennem mere detaljerede vejledninger fra nationale myndigheder og EDPB

Praksis på området er i stigende grad ved at blive ensrettet og specificeret for de dataansvarlige. Et vigtigt værktøj er vejledninger, som både det danske Datatilsyn og det Europæiske EDPB (European Data Protection Board) udsender. Fx er spørgsmål om tilsyn og databehandlere hyppigt forekommende. Begge emner har Datatilsynet udsendt nye vejledning til sidst i 2021, og i januar udsendte EDPB en ny guideline for, hvordan brud skal behandles. Baggrunden for den nye guideline er et ønske om at standardisere de forskellige nationale myndigheders arbejde og give klare vejledning til de dataansvarlige om, hvornår man skal indberette et brud.

> https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf

> https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

Aktive lovgivere

Lovgiverne i EU og i Danmark er meget aktive inden for det digitale område, og den udvikling vil givetvis fortsætte. I det kommende år ventes bl.a. The Digital Services Act en modernisering af e-handel, den nye cyber- og informationssikkerhedsdirektiv NIS2 og lovændringer om telelogning.

> https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020PC0825&from=en

> https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

> https://www.ft.dk/samling/20211/lovforslag/l93/index.htm

5. Trends og anbefalinger

5.2 ANBEFALINGER TIL LEDELSEN PÅ UDDANNELSES- OG FORSKNINGSINSTITUTIONER

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 og arbejde med disse anbefalinger:

1. Sørg for at er sat ressourcer af til igangsætning af eksterne sårbarhedsscanninger og håndtering af fundene fra disse.
2. Tag stilling til risikoen for, at ansatte, studerende mv. bliver rekrutteret til at være insidere og overvej tiltag mod dette.
3. Vurder betydningen af, at ministerområdet skal tage stilling til og kortlægge digitalt understøttede samfundsvigtige funktioner, jf. National cyber- og informationssikkerhedsstrategi 2022-24.
4. Gennemfør et eller flere møder med organisationens forretningsområder, hvor betydningen af medarbejderes adfærd i en krisesituation adresseres. Gør det så nært som muligt, så medarbejderne bliver bevidste om alvoren.
5. Inkluder informationssikkerhed i den langsigtede strategiske planlægning og udarbejd i tilknytning til det en strategi for kommunikations- og læringsindsatsen i forhold til cyber- og informationssikkerhed.
6. Gør det tydeligt, at ledelsen er aktivt og løbende involveret i arbejdet med informationssikkerhed.
7. Sørg for løbende at adressere behovet for at efterleve retningslinjer for informationssikkerhed i organisationen og monitorer efterlevelsen. Det er ikke nok, at medarbejderne undervises.
8. Overvej evt. disciplinære forholdsregler og mulige konsekvenser ved overtrædelse af sikkerhedspolitikken og -retningslinjerne.
9. Understøt en kultur, hvor risiko og sikkerhed er tænkt ind fra starten i udviklingen af produkter og tjenester.
10. Sørg for, at der er ressourcer til, at der kan føres tilsyn med overholdelse af databeskyttelsesforordningen.
11. Etabler et beredskab, udarbejd en beredskabsplan for kritiske hændelser og gennemfør øvelser med jævne mellemrum.
12. Prioriter og synliggør risikostyring gennem løbende risikovurderinger af forretningskritiske systemer – også ved hændelser, der rammer lignende institutioner.
13. Arbejd sammen med andre institutioner om informationssikkerhed, del viden og erfaringer.
14. Afsæt tid, penge og personale til håndtering af informationssikkerhed.
15. Understøt en kultur, hvor dialog om informationssikkerhed er en del af sikkerhedsarbejdet.

5. Trends og anbefalinger

5.3 ANBEFALINGER TIL IT-ANSVARLIGE PÅ UDDANNELSES- OG FORSKNINGSINSTITUTIONER

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

1. Beton vigtigheden af at gennemføre regelmæssige sårbarhedsscanninger over for ledelsen.
2. Insister på at få kommunikationshjælp til at gennemføre awarenessrettede tiltag og indarbejde det i planlægning af året.
3. Mind ledelsen om også at italesætte informationssikkerhedssituationen uden for sikkerhedsudvalget og ledelsesgangene.
4. Opfordr ledelsen til at være aktiv i informationssikkerhedsarbejdet.
5. Ajourfør og vedligehold informationssikkerhedspolitikken med faste mellemrum og få ledelsen til at godkende og håndhæve den.
6. Ved implementering af nye systemer skal du overveje brugen af persondata og beskyttelse af disse. Vær opmærksom på princippet om dataminimering jf. GDPR.
7. Hav fokus på sikkerheden ved udvikling af applikationer og tjenester samt tilretninger af eksisterende systemer, eksempelvis med udgangspunkt i principperne om security og privacy by design.
8. Tænk sikkerhed ind i relationen til leverandører og samarbejdspartnere og følg op med kontrol.
9. Hold brugernes enheder opdateret. Overvej, hvordan det kan sikres, at brugernes egne enheder er opdaterede og sikre, når de anvender dem til arbejds- eller studieformål.
10. Effektiviser og vedligehold patch management – eventuelt ud fra principperne i ITIL.
11. Hav fokus på sikkerheden i institutionens webapplikationer.
12. Begræns brugernes privilegier, fx ved at fjerne lokal administrator i Windows.
13. Etabler whitelisting af tilladte applikationer.
14. Klassificer data for at identificere kritiske data.
15. Begræns adgangen til kritiske data og beskyt dem eventuelt med kryptering.
16. Tag sikkerhedskopi af alle data, der skal beskyttes. Kontroller, at sikkerhedskopier kan indlæses. Husk at slette kopierne i henhold til din backup-politik.
17. Indfør tiltag mod misbrug via gæstenetværk.
18. Anvend single sign-on suppleret med to-faktor-autentifikation.
19. Tilbyd en passwordmanager til brugerne.
20. Undervis brugerne i sikkerhedsrisici og forholdsregler.

6. Referenceliste




Academic Security SIG
Academic Security SIG er et netværk inden for den akademiske verden organiseret under FIRST.org. Academic Security SIG sigter mod at understøtte en platform specifikt til samarbejde med akademiske sikkerhedsteams mhp. deling af erfaringer om aktuelle sikkerhedsproblemer. Det er primært etableret for at skabe forudsætningerne for samarbejde om forbedring af sikkerheden i akademiske miljøer, herunder forsknings- og uddannelsesnetværk, universitets-CSIRT'er og videnskab- og forskningsinfrastrukturer. SIG står for Special Interest Group. Under FIRST.org er der en lang række SIG'er.

CERT
CERT® var fra 1997 til 2021 et registreret varemærke og stod oprindeligt for Computer Emergency Response Team. Det mere generiske CSIRT (Computer security incident response teams) er i dag mere almindelig anvendt. DKCERTs officielle navn er Danish Computer Security Incident Response Team) CERT® var fra 1997 til 2021 et registreret varemærke og stod oprindeligt for Computer Emergency Response Team. Det mere generiske CSIRT (Computer security incident response teams) er i dag mere almindelig anvendt.

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. Centerets organisatoriske placering er p.t. under evaluering.

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 cyber og fysisk infrastruktur og 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.

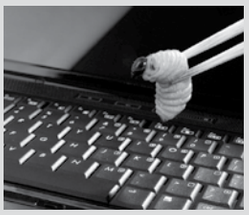
CSIRT
CSIRT står for Computer Security Incident Response Team.

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

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.

6. Referenceliste






FIRST.org
FIRST står for Forum for Incident Response Security Team og er en organisation, der organiserer en lang række CERT-teams fra det meste af verden. Pr. 1 maj 2022 er der 622 CERT/CSIRT/PSIRT-teams fra 99 lande.

FIRSTs sekretariat er hjemmehørende i USA. DKCERT blev som et af de første teams uden for USA medlem af FIRST i 1993.

Forskningsnettet
Forskningsnettet er et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner DeiC forskningsinstitutionerne med en række tjenester til e-infrastruktur og eScience, herunder DKCERT.

GÉANT
Det europæiske samarbejde om e-infrastruktur og tjenester til forskning og uddannelse. 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. Forskningsnettet er det 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.

SIG-ISM (GÉANT)
SIG-ISM er GÉANTs 'special interest group' for CISO'er for 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 4-6 gange årligt.

TF-CSIRT
TF-CSIRT (Task Force Computer Security Incident Response Teams) er et forum under de europæiske forskningsnetværks paraplyorganisation GÉANT. Medlemmerne er organisationer, der håndterer sikkerhedshændelser. Under TF-CSIRT kan organisationer mødes med andre organisationer af samme type og diskutere emner af fælles interesse. TF-CSIRT arrangerer også kurser og fremmer brugen af fælles standarder og procedurer for håndtering af sikkerhedshændelser.

Trusted introducer
Trusted Introducer (TI) blev etableret som en tjeneste i Europa i 2000. Formålet er at hjælpe teams, der håndterer 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, 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.

WISE Community
WISE er et globalt fællesskab, hvor sikkerhedseksperter deler information og skaber samarbejde mellem forskellige e-infrastrukturer inden for forskningsområdet som fx CERT. WISE leverer en ramme af standarder, retningslinjer og praksis for at fremme beskyttelsen af kritisk infrastruktur.

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

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

Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed