DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed

DKCERT Trendrapport 2021

Redaktion: Henrik Larsen og Eskil Sørensen, DKCERT.

Tak til vores bidragydere:

Trude Talberg-Furulund, seniorrådgiver, NorSIS/ Norsk senter for informasjonssikring

Torben B. Sørensen, security communication specialist, Nets A/S

Eva Elisabeth Roland, specialkonsulent, Erhvervsstyrelsen

Anders Due, kommunikationskonsulent, Datatilsynet

Jan Kaastrup, chief technology officer, CSIS Security

Simon Nexø Jensen, DKCERT

Johnson Akpotor Scott, DKCERT

Morten Eeg Ejrnæs Nielsen, DKCERT

Carina Lis Lamb, DKCERT

Jack Glen Hjortholm, DKCERT

Dennis Alan Larting, DKCERT.

Design og layout: Kiberg & Gormsen

DeiC-journalnummer: DeiC-JS 2021-02

DKCERT - en del af DeiC

DTU, Asmussens Allé, Bygn. 305

2800 Kgs. Lyngby

Copyright © DeiC 2021

Om DKCERT

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

Det er DKCERTs mission at skabe øget fokus på informationssikkerhed i uddannelses- og forskningssektoren ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DKCERT i stand til at offentliggøre og udsende 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.

KCERT er en del af DeiC, Danish e-Infrastructure Cooperation. DeiC er det nationale samarbejde med og mellem universiteterne om den digitale forskningsinfrastruktur (computing, datalagring og netværk). DeiC koordinerer samarbejdet og deltager på universiteternes vegne i nordiske og europæiske e-infrastrukturorganisationer og projekter. 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 2021.

I år fejrer DKCERT sit 30 års-jubilæum. 1. juli 1991 blev vi etableret efter inspiration fra Carnegie Mellon-universitetet, der var det første til at etablere en CERT-funktion. Det gør DKCERT til det ældste danske team, der er autoriseret af Carnegie Mellon til at bruge betegnelsen CERT.

I 1993 blev vi medlem af FIRST, the Forum of Incident Response and Security Teams, grundlagt 1990, som det første europæiske CERT/CSIRT-team. I dag er der 574 teams i 97 lande. Et vigtigt fællesskab, som udover DKCERT har fire andre danske medlemmer. Og i 2000 var vi med til at etablere Trusted Introducer, som også er en certificerings- og samarbejdsorganisation, hvis medlemmer mødes i TF-CSIRT-sammenhæng[1]. Siden 2002 har vi været akkrediteret medlem af Trusted Introducer, der nu har mere end 400 teams, de fleste fra europæiske lande. Dertil kommer medlemskab af en række fora, foreninger og netværk i Danmark, der alle arbejder med informationssikkerhed.

Medlemskabet af disse organisationer er med til at understøtte DKCERTs arbejde med at opbygge og videreudvikle viden om beskyttelse og overvågning af det danske forskningsnet – og som vi giver videre i de andre fora, vi er medlem af både på nationalt og internationalt plan. En videndeling og koordinering, som yderligere har været intensiveret mellem offentlige og private aktører i de sidste 10 år, og som har været afgørende for dels at højne sikkerhedsniveauet og dels at løfte denne dagsorden blandt aktører, politikere, presse, virksomheder og myndigheder.

Kommunikation og samtale om informationssikkerhed er nøgleordene her, fordi det spiller en afgørende rolle for vidensformidling, awarness og den brede uddannelsesindsats, der er behov for. På den baggrund har vi valgt kommunikation som tema for årets trendrapport. Vi har fået eksterne bidrag fra Erhvervsstyrelsen, NORSIS, Datatilsynet og Nets A/S om, hvordan de arbejder med kommunikation om informationssikkerhed. Vi ved, at kommunikation er afgørende for højnelse af informationssikkerheden, men hvilke erfaringer er gode at lære af? Er det et specielt formuleret budskab, er det gode råd, er det nationale kampagner eller mikroindsatsen?

Det er mit håb, at vi med dette kan igangsætte mere videndeling om kommunikationen om informationssikkerhed.

[1] Task Force CSIRT (www.tf-csirt.org) er et samarbejds- og koordinationsforum for CSIRTs (Computer Security Incident Response Teams) i Europa og naboregioner, parallelt med Trusted Introducer. Begge fora koordineres af GÉANT, det europæiske samarbejde for e-infrastrukturer og -tjenester for forskning og uddannelse.

1. Velkomst

TRENDRAPPORTENS OPBYGNING

Vi har i år bygget rapporten 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 3, efter at vi i kapitel 2 giver et vue over det aktuelle cybersituationsbillede.

I kapitel 4 gennemgår vi de mange opgaver, som DKCERT har løftet i løbet af 2020 og de tjenster, vi stiller til rådighed for sektoren, samtidig med at vi introducerer to nye i 2021: Universitetssektorens 'Malware Information Sharing Platform (MISP)' til deling af viden om aktuelle forhold, hændelser og trusler, der bliver formidlet direkte til systemadministratorernes håndtering og facilitering af beredskabsøvelser baseret på GÉANTs øvelseskoncept.

I kapitel 5 fortæller vores eksterne bidragydere om deres måde at kommunikere om cyber- og informationssikkerhed til deres respektive målgrupper.

I kapitel 6 gennemgår vi trends, vi ser inden for 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. Cybersituationsbilledet 2020/21

Et år i Coronaens tegn, der fortsætter.

Center for Cybersikkerhed har i fem år udgivet en vurdering af cybertruslen mod Danmark. I alle årene har truslen fra cyberkriminalitet og cyberspionage været vurderet som MEGET HØJ. I den seneste trusselsvurdering, der udkom i juni 2020[2], gentages vurderingen, og en opdatering ses i Forsvarets Efterretningstjenestes efterretningsmæssige risikovurdering fra december 2020[3]. Her fremgår det, at udnyttelsen af COVID-19 udgør et nyt element i det samlede trusselsbillede, men '..truslerne har derudover ikke ændret sig markant. COVID-19 har primært påvirket trusselsbilledet, i forhold til hvilke angrebsmetoder hackerne vælger.'

Her nævnes særligt, at nye arbejdsformer med hjemmearbejde og hjemmeskole giver angribere lettere adgang til myndigheder og virksomheders systemer og kan gøre det sværere at opdage, at systemerne har været udsat for kompromittering. Dette understøttes også af PwC's cybercrime survey[5], hvoraf det fremgår, at der i 2020 har været rekordmange phishing-angreb, og mere end hvert tredje phishing-angreb har været relateret til COVID-19.

Med erfaringerne fra en verden i pandemiens greb in mente, tegner der sig et billede af en sikkerhedssituation, hvor ikke alene værdien af informationer fx i relation til bekæmpelse af COVID-19 er steget, men også andre typer informationer, som virksomheder eller myndigheder er afhængige af.

Når det sker, tiltrækker det kriminelle, der vil kapitalisere på informationerne. Disse informationer omsættes på The Dark Web, hvor kriminelle med forskellige specialer køber og sælger data, samt tilbyder tjenester med en pris afhængig af kompleksiteten i det udførte arbejde. IT Governance Blog har data på, at der i 2020 er sket en stigning på 50 pct. i mængden af personoplysninger, som har været inkluderet i sikkerhedsbrud[6].

Det sorte marked for salg af informationer er med pandemien blevet en kæmpe forretning for de dygtigste kriminelle og kan have en tiltrækkende effekt for de mindre dygtige, der gerne vil have en del i markedet.

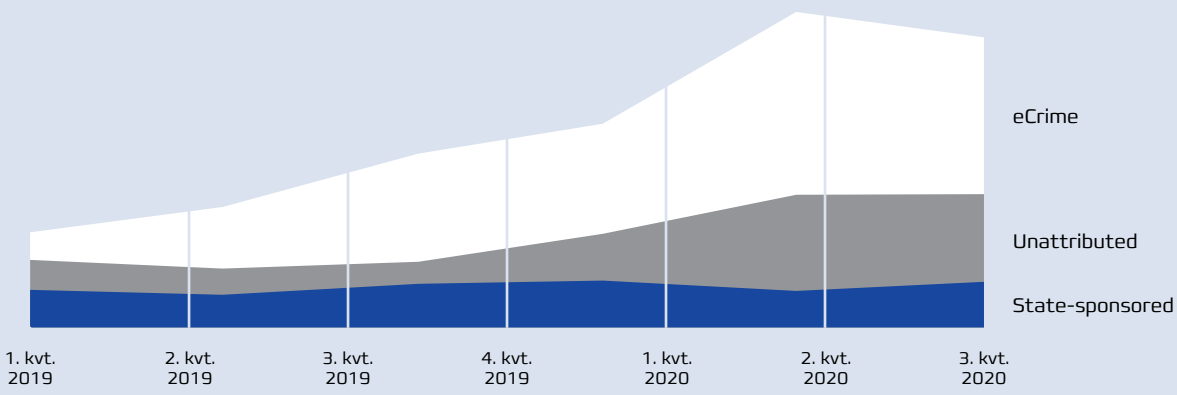
I mediebilledet får de største og mest kendte trusselsaktører og de mest spektakulære hack mest opmærksomhed, ligesom angribernes metoder og strategier ikke kun bliver kendt for offentligheden, men også udbredt og kopieret i kriminelle kredse.

DKCERT forventer, at denne udvikling vil fortsætte i de kommende år.

2 https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/-cybertruslen-mod-danmark-2020-.pdf
3 https://fe-ddis.dk/globalassets/fe/dokumenter/2020/risikovurderinger/-risikovurdering-2020-.pdf
4 https://govcyberhub.com/2020/11/13/2020-threat-hunting-report-insights-from-the-crowdstrike-overwatch-team/
5 https://govcyberhub.com/2020/11/13/2020-threat-hunting-report-insights-from-the-crowdstrike-overwatch-team/
6 https://www.techradar.com/news/improving-cybersecurity-in-education-systems

Figur 1: Udvikling i trusselstyper

CrowdStrike[4]



3. Trusselsvurdering 2021

Cybertruslen mod den danske uddannelses- og forskningssektor 2021

3.1 INDLEDNING

Denne trusselsvurdering beskriver de generelle cybertrusler, der er rettet imod den danske uddannelses- og forskningssektor. Den tager primært udgangspunkt i nationale, men også nordiske og internationale eksempler på cyberangreb mod uddannelsessektoren, som sammenholdes med danske forhold samt viden om trusselsaktørernes kapacitet og intention.

Uddannelses- og forskningssektoren har en samfundsvigtig rolle i Danmark, men er ikke defineret som samfundskritisk i den Nationale Strategi for Cyber og Informationssikkerhed 2018-2021[7]. Cyberangreb mod den danske uddannelsessektor kan have stor betydning for sektorens institutioner og påvirke andre funktioner i samfundet som helhed. Det er derfor vigtigt, at disse trusler imødegås og risici afhjælpes, så organisationerne, infrastrukturen og ydelserne i videst muligt omfang og hele tiden sikres fortrolighed, integritet og tilgængelighed.

Uddannelses- og forskningssektoren består af mange forskellige delelementer med forskellige særpræg og sårbarheder. Denne trusselsvurdering analyserer trusler mod uddannelsessektoren som helhed. Uddannelsessektoren inkluderer i denne vurdering derfor alt fra universiteter og professionshøjskoler til mindre uddannelsesinstitutioner, forskningscentre, HPC-centre og enkeltforskere. Ifølge CrowdStrike[8] er academia den sjette mest udsatte sektor for cyberangreb, og antallet af succesfulde angreb i sektoren steg med mere end 60 pct. fra 2019 til 2020.

TechRadar[10] påpeger også, at uddannelses- og forskningssektoren er et stadigt mere populært mål for cyberkriminalitet grundet en øget økonomisk gevinst, eftersom sektoren ligger inde med stadig mere eftertragtede og værdifulde data.

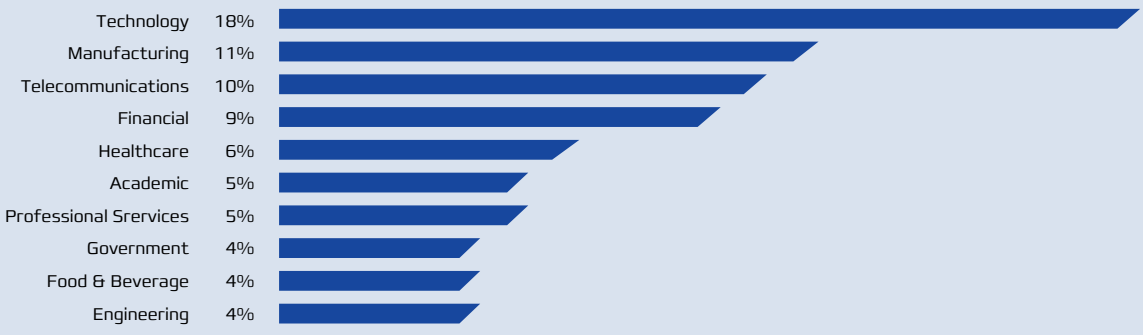
Samtidig med dette er sektoren også blandt de mest sårbare pga. sektorens åbne natur med både studerende, samt videnskabelig og administrativt personale. Der er få andre sektorer, som får så mange nye mennesker inden for hvert år, og dette stiller store krav til både sikkerheden og til oplysning.

COVID-19 epidemien har forstærket dette forhold, idet COVID-19-relaterede data har været i fokus blandt de ondsindede aktører, som man fx så i angrebet på European Medicines Agency (EMA), der godkender vacciner. Her var angrebets formål at få adgang til oplysninger om vaccinepatenter[11], og sandsynligvis også at anvende angrebet til at sprede misinformation[12].

7 https://digst.dk/strategier/cyber-og-informationssikkerhed/
8 https://govcyberhub.com/2020/11/13/2020-threat-hunting-report-insights-from-the-crowdstrike-overwatch-team/
9 https://govcyberhub.com/2020/11/13/2020-threat-hunting-report-insights-from-the-crowdstrike-overwatch-team/
10 https://www.techradar.com/news/improving-cybersecurity-in-education-systems
11 https://www.msn.com/en-gb/news/world/pfizer-biontech-vaccine-documents-hacked-in-cyber-attack-on-european-medicines-agency/ar-BB1bN5ww
12 https://www.politico.eu/article/hackers-of-eu-medicines-agency-sought-to-sow-distrust-in-vaccines/

Figur 2: Fordelingen af succesfulde angreb på sektorer

Crowdstrike[9]



3. Trusselsvurdering 2021

3.2 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 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 uddannelsessektoren er **lav**.

> Insidertruslen mod uddannelses- og forskningssektoren er **meget høj.** Der er manglede opmærksomhed vedrørende truslen og konsekvenserne heraf, hvilket øger sandsynligheden for menneskelige fejl, uanset om disse er bevidste eller ubevidste.

Disse konklusioner bygger på indsamlede oplysninger fra både egne kilder og eksterne kilder, samt fra oplysninger fra institutioner og samarbejdspartnere. Vurderingen er en samlet vurdering baseret på baggrund af disse oplysninger ud fra CFCS's definition af trusselsniveauer.

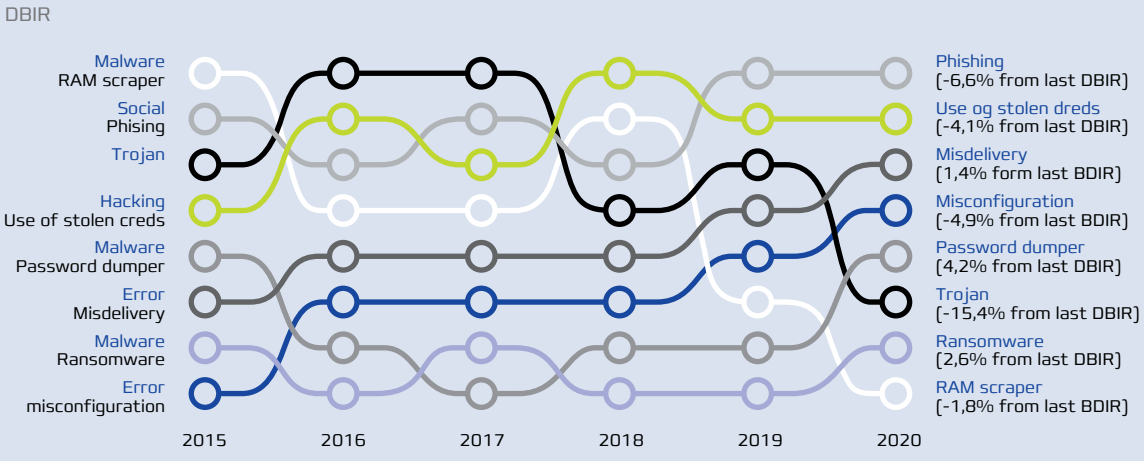
3.3 HVAD ER CYBERTRUSLER?

Cybertrusler defineres som trusler fra cyberangreb, hvor en aktør bevidst forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester, eller ubevidst forårsager problemer med disse. Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udfører dem. DKCERT beskriver og vurderer her aktiviteter, der har til formål at udføre cyberspionage, cyberkriminalitet og cyberaktivisme.

Trusselsniveauerne er baseret på en analyse af indberettede hændelser, scanninger af netværk og it-udstyr, samt kendskab til sårbarheder og andre kilder, herunder Center for Cybersikkerheds trusselsvurderinger og kendte udenlandske eksempler på cyberangreb mod uddannelse og forskning. Truslerne ændrer sig løbende, og det samme gør typerne af angreb, metoderne og hvilke sikkerhedsbrud organisationer rammes af.

Hackere kan være statsstøttede APT'er (Advanced Persistent Threats), som ofte har et meget smalt og veldefineret fokus, og som i udgangspunktet ikke ønsker at gøre opmærksom på deres tilstedeværelse. De fleste hackere, både APT'er og andre typer, er dog kriminelle, som med en finansiel agenda ønsker at skabe så meget opmærksomhed som mulig, så ofrene bliver presset til at betale løsesum for at få frigivet egne data.

Figur 3: Ændringer i hyppighed af sikkerhedsbrud



3. Trusselsvurdering 2021

3.4 CYBERSPIONAGE

Danske myndigheder og virksomheder er konstant udsat for forsøg på cyberspionage, der primært udføres af statslige aktører. DKCERT vurderer, at cyberspionage også udgør en **MEGET HØJ** trussel mod den danske uddannelses- og forskningssektor. Yderligere vurderer DKCERT, med udgangspunkt i CFCS' trusselsvurderinger, at det er meget sandsynligt, at fremmede stater har hensigt og kapacitet til at udføre cyberspionage mod sektoren. Det er sandsynligt, at fremmede stater særligt har interesse i de dele af sektoren, der producerer eller har adgang til forskningsdata eller intellektuel ejendom.

Under COVID-19 situationen har forskningsinstitutioner været et populært mål, hvis de udførte arbejde, som på nogen måde har kunnet relatere sig til COVID-19. Yderligere er der klare tegn på, at flere statsstøttede APT'er bliver mere interesseret i at stjæle eller kopiere den intellektuelle ejendom, som forskningsinstitutionerne bidrager med.

DKCERT modtager flere rapporter, der vedrører cyberspionage, og selvom det både kan være kriminelle med en økonomisk gevinst for øje, er det stadig oftere statsstøttede grupper, som står bag. Således udsendte en række cybersikkerhedsmyndigheder i flere lande, herunder Australien, USA og Storbritannien, en Joint Cybersecurity Advisory om, hvordan kinesisk-støttede grupper stod bag spionage mod flere sektorer, herunder forskningssektoren[13].

Tyveri af IP tegner sig på globalt plan for mere end 25 pct. af de $600 mia., som er de beregnede årlige omkostninger og tab relateret til cyberkriminalitet, og dette tal forventes at stige år efter år. Statsstøttede aktører forventes fortsat at være drivkraften inden for cyberspionage, og organisationer, der er i målgruppen, bør forvente at blive udsat for vedvarende og velfinansierede angreb, der involverer en række teknikker såsom social engineering, phishing, zero-day udnyttelse, DDoS-angreb og avancerede teknikker[14].

ENISA beskriver en lang række eksempler på organisationer, som har været påvirket af cyberspionage i det forgange år, herunder Visma i Norge, Airbus og flere tyske selskaber som fx BASF, Siemens og Henkel[15]. Ifølge Verizons DBIR har 14 pct. af deres registrerede hændelser i Europa relateret sig til cyberspionage[16].

Silent Librarian

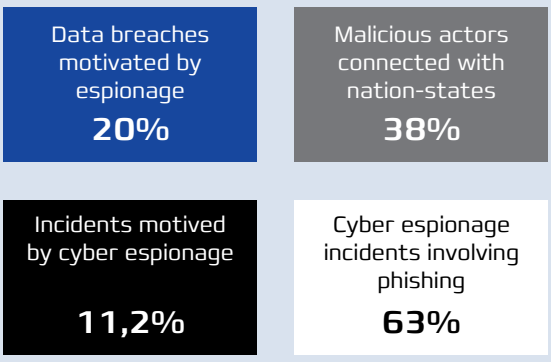
En gruppering, der har opereret i flere år, er Silent Librarian (også kaldet Cobalt Dickens), hvoraf flere dele menes at være direkte støttet af den iranske regering.

Der er bred enighed om, at gruppens formål er at stjæle værdier fra universiteter og forskningsinstitutioner i hele verden. Denne gruppe har således specialiseret sig i at indhente værdifuld information, som forskere og studerende har brugt ressourcer og tid på at udvikle, og opnå adgang til dyre forskningsdatabaser som universiteter i velstående lande abonnerer på. Om informationerne anvendes til kopiering af forskningsresultater, eller om de sælges videre, er ikke så afgørende.

Silent Librarians metoder er efter sigende ikke nyskabende, men effektive. Gruppen sender en mail til en modtager med besked om at logge ind på en bibliotekskonto via det medsendte link, deraf bibliotekar-navnet. Denne fører til en falsk loginside, som ved login kan tappe modtageren for login-oplysninger. Disse anvendes til indsamling af informationer, som modtageren arbejder med. Det kan være fortrolige forskningsdata, eller det kan være andre typer informationer.

Dele af grupperingen er meget fokuseret i deres mål, mens andre dele virker mindre kompetente og skyder med spredehagl til udvalgte modtager-

Figur 4: ENISAs opgørelse over cyberspionage



3. Trusselsvurdering 2021

grupper i forventning om, at der er værdifuld information. Grupperingen er konstant til stede, men angriber meget i bølger, så efter en række angreb, vil den oftest forsvinde i en periode, før den starter op igen.

På globalt plan ses der jævnligt angreb fra Silent Librarian, men i Norden er det ikke i helt samme omfang. Dog begyndte grupperingen i september 2020 på en ny kampagne, stadig målrettet uddannelses- og forskningsinstitutioner i den vestlige verden, og universiteter i Tyskland, Danmark, Norge, Sverige og Holland har alle set angreb fra gruppen[17].

Shadow Academy

Shadow Academy er en ny gruppering, der menes at komme fra Tyrkiet eller være støttet af den tyrkiske regering. Gruppen har ligesom Silent Librarian universiteter og forskningsinstitutioner som målgruppe, og metoderne er i høj grad kopieret fra Silent Librarians playbook. Denne gruppe hørte man første gang om i 2020, hvor den blev knyttet sammen med kompromitteringen af universiteter i Australien, Afghanistan, UK og USA[18].

Alle disse angreb brugte lignende taktikker, teknikker og procedurer som Silent Librarian og har også målrettede indsatser med henblik på at kompromittere universitetsstuderende og –ansatte. Det sker typisk ved at efterligne universitetsressourcer ved hjælp af falske skygge-domæner for at høste akkreditiver.

Metoderne er dog en smule anderledes end Silent Librarians, idet de går mere målrettet, fx med spear phishing, efter navngivne forskere. Det er en metode, der er mere omkostningstung end de klassiske phishing-angreb, eftersom det kræver et større forberedelsesarbejde at finde frem til forskere og ansatte ved uddannelsesinstitutioner, der har den ønskede viden. Når målene er identificeret, kræver det ydermere en særlig indsats for at lokke informationer eller login-informationer ud af personerne. Til gengæld kræver det næppe så meget efterbearbejdning, når først de ønskede informationer er indhentet.

Louisiana State University er det første bekræftede offer for denne nye gruppering i gruppens første kampagne, der løb fra juli 2020 til oktober 2020. Denne ramte også 12-13 andre, mindre kendte universiteter I USA[19].

13 https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
14 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage
15 https://www.securityforum.org/research/threat-horizon-2021-the-digital-illusion-shatters/
16 https://enterprise.verizon.com/resources/reports/dbir/
17 https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
18 https://www.riskiq.com/blog/external-threat-management/shadow-academy/
19 https://www.riskiq.com/blog/external-threat-management/shadow-academy/

3. Trusselsvurdering 2021

3.5 CYBERKRIMINALITET

Cyberkriminelle angriber alle dele af det danske samfund for at tjene penge på bl.a. afpresning og datatyveri. Dette er ikke anderledes for uddannelsessektoren, og derfor vurderer DKCERT at truslen fra cyberkriminalitet mod den danske uddannelses- og forskningssektor er **MEGET HØJ**. Dele af sektoren er præget af ældre og sårbare systemer, hvor der tidligere ikke været samme fokus på cybersikkerhed. Dette kan have ført til, at cyberkriminelle har rettet deres fokus mod disse systemer. Derudover bliver sektoren ramt af mere brede angreb, som ikke er rettet mod bestemte sektorer.

Cyberkriminelle har et meget klart økonomisk fokus, deres mål er at sætte organisationer i en situation, hvor de er nødt til at betale for at komme tilbage til normal drift eller se deres indtjening falde betydeligt grundet nedsat drift. Derfor tvinger de organisationer til at vægte løsesummens størrelse imod de økonomiske tab ved forstyrrelse af driften. Yderligere er flere kriminelle aktører begyndt at anvende den tilegnede data på flere måder, fx ved exfiltrering af et sæt data og krypteringaf et andet. Dette for at kunne true med offentliggørelse af data for at lægge et yderligere pres på organisationerne til at betale den ønskede løsesum.

Cyberkriminelle er rigtigt gode til at udnytte forskellige situationer til at fremme deres mål. Eksempelvis bruger de gerne store begivenheder eller kriser til det, og ved epidemier udgiver de sig fx for at være sundhedsorganisationer. Alle efterspørger informationer om epidemien og er derfor ikke så mistænksomme, som de normalt ville være, når de modtager mails.

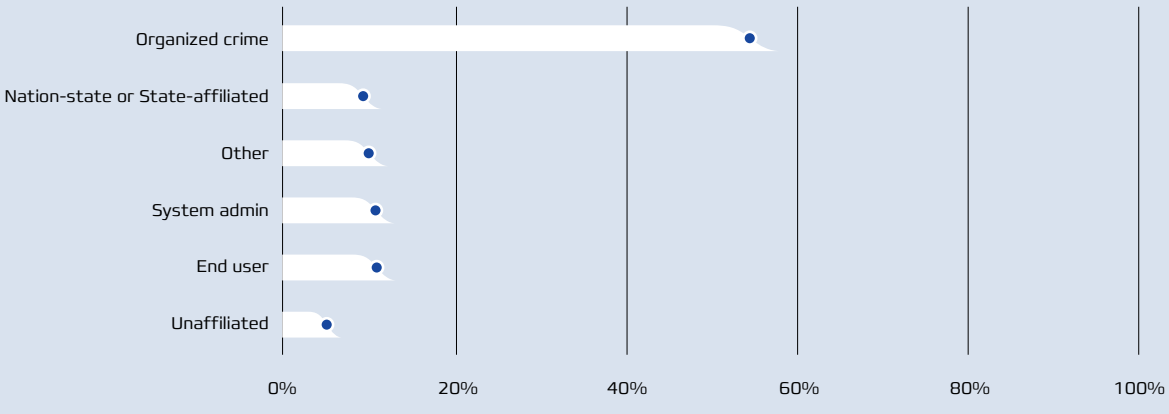
Hen over valentinweekenden den 13.-14. februar 2021, blev både Universiteit van Amsterdam og Hogeschool van Amsterdam (Amsterdam University of Applied Sciences) ramt af et cyberangreb, der forsøgte at installere ransomware. Begge universiteter havde imidlertid lært lektien fra angrebet mod Maastricht University i slutningen af 2019, så var der dels oprettet overvågning i form af en SOC (Security Operations Centre), hvilket gjorde universiteterne i stand til at opdage angrebet tidligt, og dels implementeret multifaktor-login, hvilket gjorde angrebet sværere for de kriminelle. Det betød, at angrebet kun har resulteret i mindre forstyrrelser af driften.

De kriminelle var dog samtidig også hurtige til at reagere på, at universiteterne åbent informerede om, at de var under angreb. De udsendte derefter phishingmails med falske instruktioner, om at brugerne skulle ændre password, sammen med et link til en falsk login-side[21].

[20] https://enterprise.verizon.com/resources/reports/dbir/

[21] https://www.uva.nl/en/shared-content/studentensites/uva-studentensite/en/announcements/2021/03/uva%E2%80%AFand-auas-repel-cyber-attack.html

Figur 5: DBIRs opgørelse over de trusler, der oftest er skyld i et sikkerhedsbrud[20]



3. Trusselsvurdering 2021

Selv om der er tale om et nyere interesseområde for kriminelle, så er mange af de angrebsmetoder, som anvendes, ikke forskellige fra dem, der har været benyttet gennem rigtigt mange år. De to store angrebsteknikker er at udnytte mennesker til at få adgang (fx ved hjælp af phishing mv) eller opsnuse ikke-patchede sårbarheder i organisationens udadvendte services (fx en forældet krypteringsversion i HTTPS).

3.5.1 Malware, der udvinder kryptovaluta, stiger i omfang

Kriminelle tager i hemmelighed andres computere i brug med henblik på at udvinde kryptovalutaer ved 'mining'. Angrebene på andre computere gennemføres ofte, uden at computerejerne selv er opmærksomme på det, ved installation af små programmer til beregning af kryptovaluta. Angreb, der har til formål at installere kryptominers stiger og falder sammen med kurser på kryptovaluta. Det er svært at vurdere omfanget af truslen i den kommende tid, men det er dog en konstant trussel.

Hvis organisationer har udstyr, som kan være brugbart for kriminelle at udnytte til mining, så bør disse løbende holde øje med priserne på krypto-valuta. Eksempelvis er prisen på bitcoins kraftigt stigende i slutningen af 2020 og de første måneder af 2021. Det indebærer, at denne type angreb er blevet mere økonomiske rentable for de kriminelle.

HPC-anlæg kan være særligt eftertragtede for de kriminelle at få adgang til, men også institutionernes og især forskernes it-udstyr kan være følsomme over for malware, der udvinder kryptovaluta. Da forskeres it-udstyr typisk er designet og testet til at fungere under nogle bestemte vilkår, øges risikoen for, at malwaren har utilsigtede konsekvenser. I maj 2020 var der angreb på en europæisk HPC-gruppering med det formål at udnytte kapaciteten til udvinding af kryptovaluta, og fem HPC-anlæg i Tyskland blev lukket ned efter at være blevet inficeret med malware til kryptomining[22].

3.5.2 Ransomware kan forstyrre driften og ødelægge forskning

Ransomware er en form for skadelig software, der krypterer data og dermed spærrer for adgangen til offerets computer eller data. For at få genoprettet adgangen skal offeret betale en løsesum til bagmændene for at få dekrypteret deres data. Uddannelses- og forskningssektoren i både Danmark og i udlandet har ligesom en lang række andre sektorer været ramt af ransomware. Dette kan være problematisk for sektoren, dels fordi forskeres arbejde kan være tidskritisk, og dels fordi mange års data pludselig ikke længere er tilgængeligt. Eller hvor fortroligheden brydes ved at de opnåede data publiceres. hvis løsesummen ikke betales.

Aalborg Universitet blev i sommeren 2020 ramt af et formodet forsøg på ransomwareangreb, som forstyrrede driften på universitet, på trods af, at de ondsindede aktører faktisk ikke nåede til at inficere systemerne med ransomware. Medarbejdere ved AAU reagerede hurtigt, da de blev opmærksomme på, at universitetet var blevet kompromitteret af hackere, hvorfor de den 4. august lukkede ned for adgangen til alle it-systemer[23].

Denne hurtige nedlukning fangede sandsynligvis de ondsindede aktører i deres rekognosceringsfase, hvor de med en eller flere kompromitterede brugere havde til hensigt at kortlægge it-landskabet hos AAU. Med dette kunne de sikre, at deres ransomware ville have maksimal effekt og meget vel ville kunne have låst data i de fleste af universitetets systemer. Det kan ikke udelukkes, at tyveri af forskningsdata kunne have været et sideordnet formål med angrebet.

Der var tale om en række af tilsyneladende enkeltstående begivenheder, der alligevel viste sig at være sammenhængende. Dette fik universitetet til at konkludere, at der var tale om et sofistikeret og målrettet angreb, hvorfor adgangen til systemerne blev lukket ned.

Selv uden at have inficeret AAU med ransomware formåede hackerne altså at forstyrre driften på universitetet i en periode. Var angrebet ikke opdaget kunne det meget vel have haft betydelige konsekvenser.

Tal fra Verizons DBIR[24] viser også tydeligt, at ransomware stadig er langt mest udbredte malware i uddannelsessektoren.

[22] https://www.bbc.com/news/technology-52709660
[23] https://www.version2.dk/artikel/aalborg-universitet-hacket-de-kan-have-skaffet-sig-adgang-forskning-alle-andre-oplysninger
[24] https://enterprise.verizon.com/resources/reports/dbir/

3. Trusselsvurdering 2021

Den bedste måde at forsvare sig mod ransomwareangreb er brugerrettighedsstyring for at forhindre, at den ondsindede kode kan eksekveres på maskiner. Derudover er netværkssegmentering, backup og offline backup vigtige afhjælpende tiltag, der kan mindske problemets omfang. DKCERT kan på baggrund af sårbarhedsscanninger konstatere, at selvom de danske uddannelses- og forskningsinstitutioner er gode til at tage backup, så halter det hos flere institutioner med at implementere netværkssegmentering og tilstrækkelig patch-management. Dette gør ransomware til en større trussel, end det behøver være.

3.5.3 Business E-mail Compromise (BEC) er fortsat en udfordring

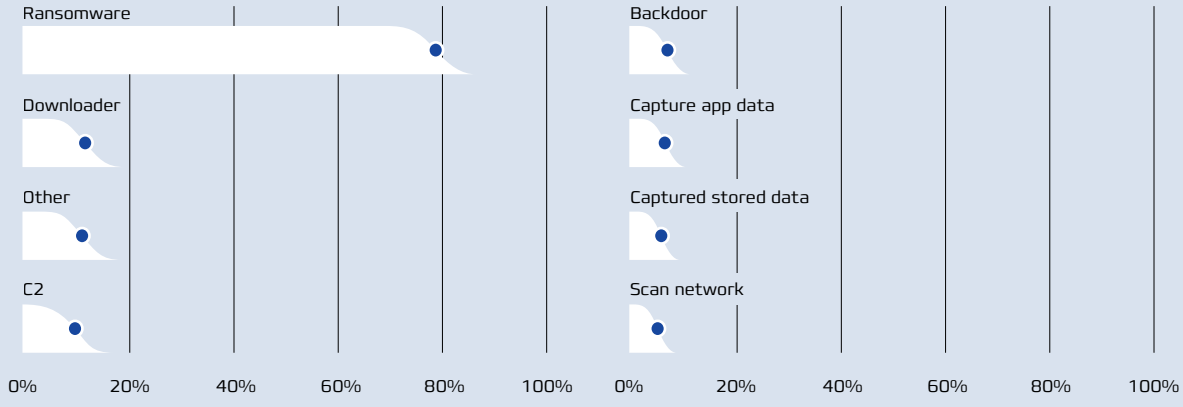
Flertallet af organisationer i uddannelses- og forskningssektoren i Danmark har været udsat for forsøg på Business E-mail Compromise (BEC), hvor kriminelle har forsøgt at snyde ved at udgive sig for at være en ledende medarbejder.

De såkaldte BEC-scams har til formål at franarre virksomheder, myndigheder og institutioner penge gennem falske anmodninger om pengeoverførelser. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også ofte for CEO-fraud eller direktørsvindel. De bedrageriske e-mails sendes ofte fra fremmede mailkonti, men i nogle tilfælde kan bedrageriforsøget anvende ledende medarbejderes kompromitterede mailkonti (også kaldet whale-phishing). Hvis en ondsindet aktør er lykkedes med at kompromittere medarbejderes konti, øger dette risikoen for et succesfuldt bedrageriforsøg. DKCERT har en forventning om, at uddannelses- og forskningssektoren, ligesom resten af Danmark, oplever mange forsøg på BEC-scams, og at en del af disse bliver mere og mere avancerede. DKCERT har intet overblik over problemets omfang, da denne type hændelser typisk ikke bliver indberettet til DKCERT af universiteterne.

Mens der i sådanne bedrageriforsøg ikke er tale om en kompromittering af it-systemer, afspejler de truslen fra bedrageriske e-mails og misbrug af organisations- og personoplysninger. Sker sådanne angreb i fremtiden fra kompromitterede e-mailkonti i organisationer, vil det være vanskeligere for den enkelte organisation at erkende angrebet i tide.

[25] https://enterprise.verizon.com/resources/reports/dbir/

Figur 6: DBIRs opgørelse over de mest udbredte malware i uddannelses- og forskningssektoren[25]



3. Trusselsvurdering 2021

3.6 CYBERAKTIVISME

Cyberaktivisme har til formål at formidle et holdningsmæssigt, ideologisk eller politisk budskab gennem cyberangreb. Cyberaktivisme er typisk fokuseret på enkeltsager og personer, organisationer eller virksomheder, som aktivisterne opfatter som modstandere af deres sag.

Da DKCERT ikke har adgang til efterretningskilder, kan DKCERT ikke lave en selvstændig vurdering på trusselsniveauet for cyberaktivisme. Vi henviser derfor til CFCS, der vurderer den generelle truslen fra cyberaktivisme mod Danmark til at være **LAV**. Trusselsniveauet kan dog stige uden eller med kort varsel, hvis enkeltsager fanger aktivisternes opmærksomhed. Tilsvarende kan truslen variere, afhængig af hvilke emner uddannelses- og forskningsinstitutioner arbejder med og hvilke emner, som er på dagsordenen på bl.a. sociale medier. Dette kan fremme opmærksomheden mod emner, som institutionerne er involveret i.

Inden for uddannelses- og forskningssektoren er der dog adskillige konkrete eksempler på, at både videnskabeligt og administrativt personale har modtaget trusler, enten grundet i institutionens eller i den individuelles involvering i arbejdet med fx vira eller vacciner. Sådanne trusler kan meget vel få et cyber-aspekt altså i form af cyberaktivisme.

Overbelastningsangreb

Den mest udbredte form for cyberaktivisme er overbelastningsangreb, oftest i form af DDoS-angreb, som efterhånden kan købes af de fleste på det sorte cybermarked for ganske få penge. DDoS var en af de første angrebsmetoder, som blev udbudt til alle og hver med en smule penge og en interesse i at genere andre. Flere computerspil har oplevet mindre DDoS-angreb initieret af spillere, som havde set sig sure på spillet, ligesom vi har set angreb mellem spillere, i vores sektor mest på kollegier.

Overbelastningsangreb kan dog også udføres af seriøse aktører med store konsekvenser til følge, eksempelvis hvis hospitalssystemer angribes, hvorved behandlingskrævende personer ikke kan bestille tid eller modtage behandling.

3.7 DESTRUKTIVE CYBERANGREB

En række lande har cyberkapaciteter, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur, fx i energi- og forsyningssektorerne. Baseret på den offentligt tilgængelige viden om destruktive cyberangreb, samt viden om hændelser inden for sektoren vurderer DKCERT, at truslen er **LAV**. Der er kapacitet til stede, men der har ikke været konkrete hændelser rettet mod den danske uddannelses- og forskningssektor. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

3.8 INSIDERTRUSLEN

En insider er en person med legitim adgang, som bevidst eller ubevidst påvirker organisationens virke gennem at sprede, skade eller ændre de informationer og processer, der udgør dens fundament. Et generelt problem for organisationer i forhold til insidere er, at både de bevidste og ubevidste allerede er inden for i organisationen, og derfor er deres evne til bevidst eller ubevidst at forårsage skade på organisationen større end de fleste udefrakommendes ville være.

DKCERT vurderer at insidertruslen mod uddannelses- og forskningssektoren er **MEGET HØJ**.

Sådan kan denne trusselsvurdering bruges

Trusselsvurderingen beskriver de generelle cybertrusler mod den danske forsknings- og uddannelsessektor og anbefales anvendt i institutionernes risikovurderingsarbejde.

Denne trusselsvurdering er udarbejdet for at give input til institutionernes risikovurderingsarbejde Vurderingen skal ses som en støtte, så de enkelte institutioner ikke skal udarbejde en trusselsvurdering selv.

Trusselsvurderingen peger på at sektoren er udsat for generelle trusler, som udgør en del af et samlet risikobillede for institutionerne.

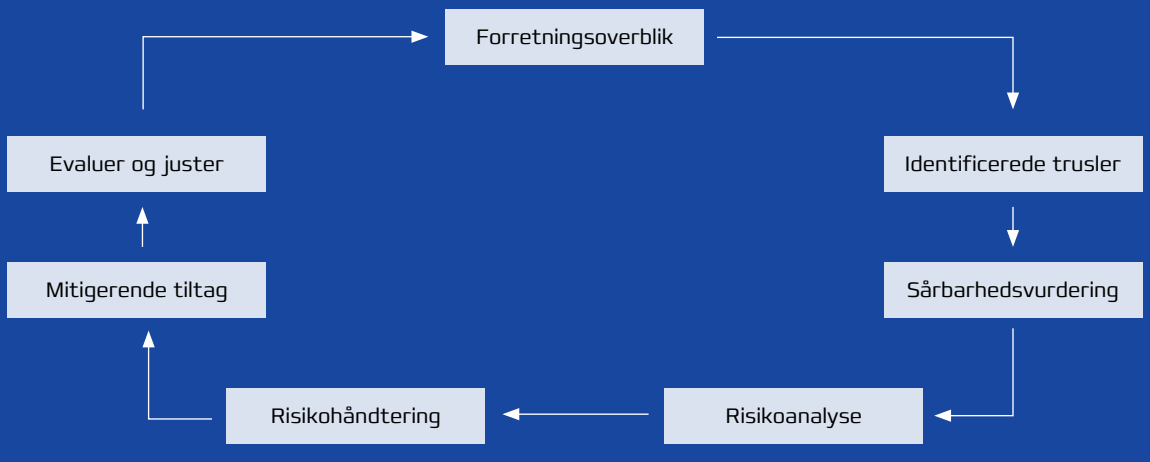
For at anvende trusselsvurderingen bedst, bør institutioner i første omgang opdatere overblikket over deres forretningsområde, altså det domæne, som institutionen arbejder inden for. Domænet består bl.a. af ansatte, interessenter, samarbejdspartnere, processer, lokationer, som typisk er understøttet af it i form af hardware og software. Alt sammen er det elementer, som hænger sammen både digitalt og analogt, og som typisk har en række konkrete sårbarheder, som kun den enkelte institution eller proces- og forretningsejer har mulighed for at kende til bunds.

Den enkelte institution bør ud fra kendskabet til egen forretning identificere de konkrete sårbarheder i organisationen, som trusselsaktører kan udnytte. Overblik over eget forretningsområde og de sårbarheder, de er knyttet til dem, afgør således, om truslerne nævnt i denne trusselsvurdering er relevante.

Når truslen om cyberspionage er meget høj, bør en institution, der fx arbejder med vaccineforskning, ud fra kendskabet til egne processer, mennesker, it-understøttelse, transmission og opbevaring af data på servere, enheder, papirarkiver osv. identificere mulige sårbarheder. En sårbarhed kan fx være tildeling af brugerrettigheder og styring af brugerrettigheder. Hvis konsekvenserne ved at ondsindede aktører får fat på brugernavne og adgangskoder fra ansatte med administratorrettigheder vurderes at være kritiske for forretningen, bør institutionen eliminere eller minimere risikoen for, at der kan ske kompromittering af informationerne.

Efter sårbarhedsvurderingen kommer den egentlige risikovurdering, hvor organisationen tager stilling til de enkelte identificerede risici og beslutter hvordan de skal håndteres.

Figur 7: Proces i forbindelse med institutionens risikovurdering



3. Trusselsvurdering 2021

Den ubevidste insider
Alle organisationer er sårbare overfor cyberangreb og relaterede hændelser, der bevidst eller ubevidst er forårsaget af medarbejdere, som uden deres vidende kan medvirke til brud på informationssikkerheden. Ligesom det gælder for sårbarheder i fx software, kan en ubevidst insider medvirke til, at organisationen bliver kompromitteret. Derfor bør alle organisationer forholde sig til truslen fra ubevidste insidere.

Den klassiske ubevidste insider er den medarbejder, som på grund af fx uklare eller manglende sikkerhedspolitikker eller manglende uddannelse ubevidst bryder organisationens sikkerhedspolitikker. Den ubevidste insider 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.

En anden type ubevidst insider er den uagtsomme insider. Af rapporten Danskernes Informationssikkerhed 2020[27] fremgår det, at der er sket en stigning i andelen af offentligt ansatte, der bevidst undlader at efterleve organisationens retningslinjer for informationssikkerhed. En stor del af de offentligt ansatte, der bevidst bryder reglerne, oplyser som årsag til bruddet, at reglerne umuliggør udførelsen af deres arbejde.

Dette gør ikke, at de er bevidste insidere, men derimod 'uagtsomme insidere', da en omgåelse af reglerne får risikoen for kompromittering af data til at stige.

I sådanne tilfælde er der således tale om en dårlig balance mellem sikkerhed og den praktiske udførelse af arbejdsopgaverne, der øger risikoen for, at handlinger fra uagtsomme insidere kan medføre en sikkerhedsmæssig kompromittering, som kan få en alvorlig konsekvens for fx en uddannelsesinstitution.

En længere gennemgang af resultaterne fra Danskernes Informationssikkerhed 2020 findes i afsnit 4.5.

Oplæring og opmærksomhedstræning og sikring af, at procedurer bliver overholdt og regler efterlevet er i høj grad det, der kan mindske truslen fra den ubevidste insider.

[26] https://itsecuritycentral.teramind.co/
[27] https://cert.dk/sites/default/files/uploads/Danskernes%20informationssikkerhed%202020.pdf

Figur 8: IT Security Central[26] Typer af insidere

Den ubevidste insider
Insidere, der normalt er uvidende om organisationens sikkerhedspolitik eller ikke forstår de potentielle sikkerhedsrisici, som organisationen er udsat for, og derfor ikke skænker sikkerhed en tanke. Disse medarbejdere er mest sårbare over for social engineering.

Den uagtsomme insider
Insidere, som har kendskab til eller er uddannet i organisationens sikkerhedspolitikker, men som alligevel vælger at omgå dem for at være mere effektiv, eller hvis politikkerne ses som besværlige.

Den bevidste insider
Insidere, der stjæler data med vilje eller ødelægger virksomhedsnetværk – såsom en ansat, der sletter virksomhedsdata på sin sidste arbejdsdag.

3. Trusselsvurdering 2021

Den bevidste insider

En bevidst insider kan være særlig skadelig for en organisation. Modsat udefrakommende hackere, som i mange tilfælde bliver stoppet af sikkerhedsmekanismer som firewalls, e-mailscanning og antivirus-filtre, vil en bevidst insider ofte have succes med sine handlinger. Det skyldes, at sikkerhedsmekanismerne ikke beskytter mod en insider, som ikke nødvendigvis anvender malware, men er i stand til at udføre sine handlinger alene ved at misbruge sin stilling og legitime it-adgange. En undersøgelse fra Carnegie Mellon University i USA[28] viser, at op til 80 pct. af de bevidste insiderhandlinger er ansporet af arbejdsrelaterede hændelser som eksempelvis afskedigelse, forflyttelse eller en disciplinærsag, der har skabt en konfliktsituation mellem medarbejderen og arbejdsgiveren. Som konsekvens af konflikten vælger medarbejderen at skade organisationen for at få en form for oprejsning.

I forbindelse med brug af underleverandører og outsourcing har en organisation ofte ringe kendskab til eller indflydelse på interne forhold hos leverandøren. Organisationer bør derfor være opmærksomme på, at konflikter mellem underleverandøren og dennes medarbejdere kan opstå uden organisationens vidende, hvorved truslen fra bevidste insidere i forsyningskæden kan øges uden eller med kort varsel.

Sagen om Britta Nielsen, som havde svindlet for mere end 117 millioner kroner fra Socialstyrelsen, er til dato stadig det bedst kendte nyere eksempel på en bevidst insider. Britta Nielsen har tilsyneladende ikke haft til hensigt at skade Socialstyrelsen, men alene berige sig selv. Hendes handlinger har dog alligevel voldt stor skade på Socialstyrelsen image og også skadet dele af befolkningens tiltro til det offentliges forvaltning af 'deres' skattepenge.

En organisation har således kun mulighed for at adressere truslen fra den bevidste insider ved at etablere kontroller, der kan forhindre misbruget eller minimere konsekvenserne ved det. Den bevidste insider vil imidlertid ofte i kraft af sit kendskab til procedurer og kontrollerne kunne omgå dette.

[28] https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21232

3. Trusselsvurdering 2021

3.9 TENDENSER INDEN FOR CYBEROMRÅDET

Cyberområdet er ligesom mange andre områder i konstant udvikling, og selvom der fra tid til anden dukker helt nye aktører eller malwaretyper op, er det meste dog mere udviklinger af tidligere metoder og malwarekoder.

Der har dog i de seneste år været en klar stigning inden for en række områder, og to af disse har DKCERT valgt at fremhæve, da vi vurderer, at disse har størst betydning for cybersikkerheden for uddannelses- og forskningssektoren. Der er tale om Social Engineering og Supply-Chain angreb, som begge uddybes i dette afsnit.

Yderligere bør det nævnes, at Googles Threat Analysis Group har identificeret en kampagne, der begyndte i slutningen af 2020. Kampagnen er rettet mod sikkerhedsresearchere, der arbejder med opdagelse af sårbarheder og -udvikling hos forskellige virksomheder og organisationer. Aktørerne bag denne kampagne, som tilskrives en regeringsstøttet enhed med base i Nordkorea, har brugt en række midler til at opnå kontakt med researcherne.

For at opbygge troværdighed og oprette forbindelse til sikkerhedsforskere etablerede aktørerne en forskningsblog og flere Twitter-profiler for at interagere med potentielle mål. De har brugt disse Twitter-profiler til at sende links til deres blog, sende videoer af deres påståede bedrifter og til at forstærke og retweete indlæg fra andre konti, som de kontrollerer[29].

Social Engineering

Der er de seneste år sket en kraftig stigning i andelen af sikkerhedshændelser, hvor social engineering er brugt som indgangsvinkel med det formål at få fat på medarbejderes loginoplysninger. Dette understreger vigtigheden af aktiviteter, der skaber opmærksomhed blandt ansatte om denne trussel.

Social engineering er en slags hacking af mennesker og ikke systemer. Det er beskrevet som den psykologiske manipulation af mennesker til at udføre handlinger eller videregive fortrolige oplysninger. Et slags tillidstrick med henblik på informationsindsamling, svig eller systemadgang, der adskiller sig fra traditionel svindel ved, at det ofte er et af mange trin i et mere komplekst angreb.

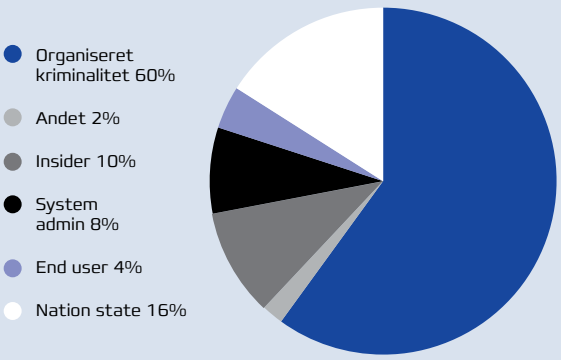
Jo flere oplysninger, kriminelle eller statsstøttede aktører kan indsamle via sociale medier om en person, jo nemmere er det for dem at gøre brug af social engineering over for personen. Derfor er social engineering et vigtigt opmærksomhedspunkt, når man træner den generelle opmærksomhed om cybertrusler.

Med udgangspunkt i de offentligt tilgængelige oplysninger manipulerer hackerne sig til at få flere oplysninger ud af deres ofre, enten ved at lade som om, at de kommer fra troværdige organisationer, eller ved at foregive at de ønsker at hjælpe. Da de allerede er i besiddelse af nogle oplysninger, virker de troværdige, og lokker ofte informationer ud af ofrene ved at bede dem om at bekræfte visse oplysninger.

Ifølge ENISA[30] gør 84 pct. af alle cyberangreb brug af social engineering, og det er tydeligt, at de ondsindede aktører har fået øjnene op for, hvor god en kilde til oplysninger social engineering er. Ligeledes ser Europol social engineering som den vigtigste faktor til at facilitere andre cyberangreb.

[29] https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/
[30] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport
[31] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport

Figur 9: Brugen af social engineering fordelt på aktører (ENISA[31])



3. Trusselsvurdering 2021

Leverandørvinklen
Cozy bear eller APT29 er en gruppe, som den amerikanske regering har identificeret som værende gruppen bag SolarWinds-hacket, der blev kendt i slutningen af 2020. APT29 formodes at være knyttet til en eller flere russiske efterretningstjenester. Angrebet betegnes som et af de mest vellykkede nogensinde, eftersom en såkaldte trojaniseret version af overvågningssoftwaren Orion blev sendt ud som en opdatering allerede i marts 2020.

Dette angreb er et eksempel på et veleksekveret supply chain attack. SolarWinds Orion-softwaren bliver brugt af mange tusind store og små virksomheder i hele verden og ved at få sin egen ondsindede kode ind i Orion, er det lykkedes for ATP29 at få adgang til rigtigt mange af disse virksomheders netværk og vigtige oplysninger.

ATP29 fik lagt en bagdør ind i en digitalt signeret SolarWinds komponent i Orion-strukturen. Ved hjælp af denne bagdør har der kunnet installeres malware, der i første omgang har ligget i dvale i op til to uger, hvorefter den har hentet og udført kommandoer.

Grundet Orions store popularitet og udbredelse er det via dette angreb lykkedes ATP29 at få adgang til fx flere amerikanske ministerier og kildekoden i flere af Microsofts source code repositories. I Danmark har mindst 30 danske virksomheder og myndigheder – heriblandt mindst to universiteter – haft den kompromitterede version af Orion installeret, og ifølge Dansk Energi er to store danske energiselskaber blevet ramt af det alvorlige SolarWinds-hackerangreb, hvor det er lykkedes for hackerne at installere såkaldte bagdøre i de to store energiselskabers it-systemer. Umiddelbart er der dog intet der tyder på, at hackerne har udnyttet disse bagdøre[32].

Et angreb som SolarWinds-hacket viser med al tydelighed, hvor vigtigt det er, at have den interne sikkerhed i orden, da ondsindede aktører kan komme ind i organisationer på mange forskellige måde. Det er ikke bare phishing, brute force og credential stuffing, der er et problem, men selv troværdige partnere kan være vejen ind for de kriminelle. Derfor anbefaler DKCERT, at kommunikationskanaler til leverandører beskrives, og at der stilles krav til leverandørerne om anvendelse af kanalerne, at der etableres kontroller mhp. at sikre, at kravene bliver overholdt.

De seneste oplysninger vedrørende SolarWinds indikerer, at en kinesisk gruppe muligvis har brugt en anden sårbarhed i SolarWinds' software til at tilgå oplysninger hos organisationer, som bruger denne[33].

3.10 ANBEFALINGER

Mange af de sikkerhedshændelser, der forekommer i uddannelsessektoren, er et resultat af dårlig sikkerhedshygiejne samt dårligt kendskab til sikkerheden og forståelse for nødvendigheden af sikkerheden blandt medarbejderne. Hvis menneskelige fejl kan reduceres, kan man komme langt. Der bør dog også etableres en baseline for sikkerhed på alt udstyr, der er tilgængeligt fra internettet, og øge sikkerheden på dette, eksempelvis med multifaktorautorisation.

Et andet baselineområde er etablering af god patch management-kultur i organisationer, som er en grundlæggende forudsætning for al sikkerhedsarbejde.

Antallet af medarbejdere med adgang til forretningskritiske it-systemer og data bør begrænses. Særligt bør antallet af medarbejdere med administratorrettigheder begrænses til et minimum, hvilket også bidrager til at beskytte mod udefrakommende hackere. I forbindelse med ansættelsesophør eller overgang til ny funktion er det vigtigt, at overflødige it-adgange hurtigt spærres, og at eventuelle fælles administrator- eller rootadgangskoder, som medarbejderen har kendskab til, ændres. Jobrotation og opdeling af opgaver og ansvar er to af de mest udbredte måder at undgå snyd, begge dele er meget brugt i økonomiafdelingerne i offentlige og private virksomheder, men mangler i høj grad at blive implementeret i it-afdelingerne i de samme organisationer.

Endelig anbefales det, at opretholdelse af god it-hygiejne bliver en del af sikkerhedskulturen i organisationen, og at der leves op til de tekniske minimumskrav til sikkerheden hos statslige myndigheder[34].

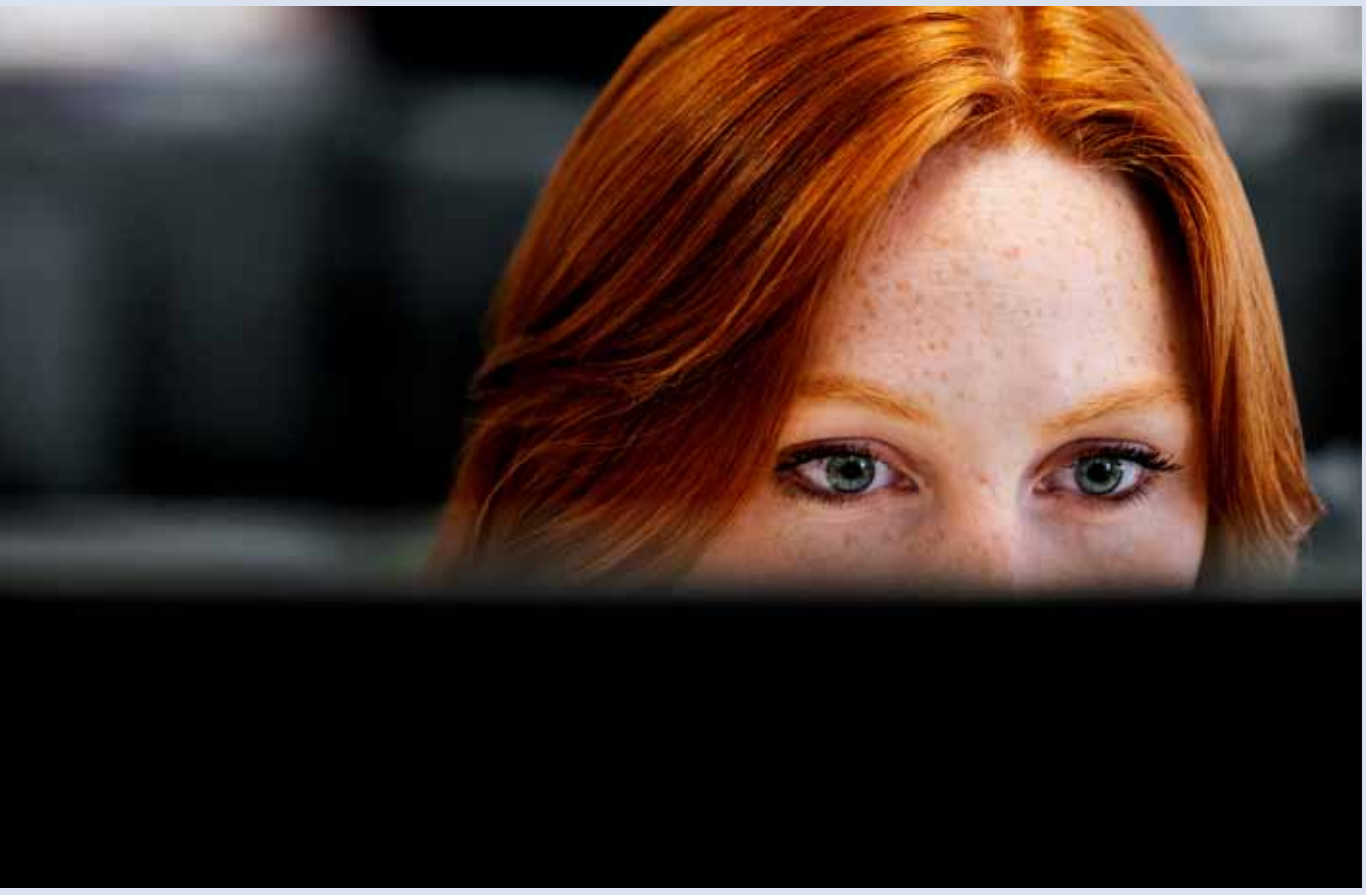
[32] https://jyllands-posten.dk/indland/ECE12722218/danske-energiselskaber-ramt-af-cyberangreb/
[33] https://www.bloomberg.com/news/articles/2021-02-02/suspected-chinese-hackers-also-exploited-solarwinds-reuters
[34] https://sikkerdigital.dk/media/10946/tekniske-minimumskrav.pdf

3. Trusselsvurdering 2021

3.11 TRUSSELSNIVEAUER

DKCERT anvender for sammenligningens skyld samme trusselsniveauer, som Forsvarets Efterretningstjeneste bruger:

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er generelle trusler. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er erkendte trusler. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er konkrete trusler. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.



4. 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.

4.1 HÆNDELSER, ADVARSLER OG TEKNISKE ANALYSER

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 kontakt ved henvendelser vedrørende alle forskningsnettets IP-adresser. Det er DKCERTs 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.

4.1.1 Årets sikkerhedshændelser

DKCERT modtog i 2020 oplysninger om 130 hændelser, hvoraf DKCERT har undersøgt 92 af dem, mens de resterende 38 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.

Fordelingen af hændelser og undersøgelse henover året fremgår af Figur 10.

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.

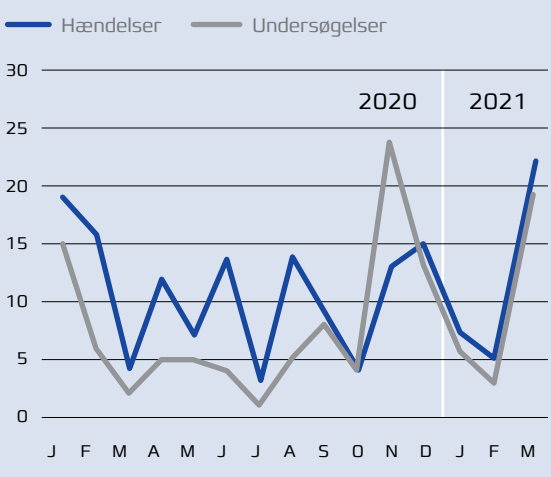
Ud over de nævnte hændelser har DKCERT behandlet sager om spam og phishing samt forsøg på målrettede angreb mod institutioner på forskningsnettet.

4.1.2 Advarsler fra tredjeparter

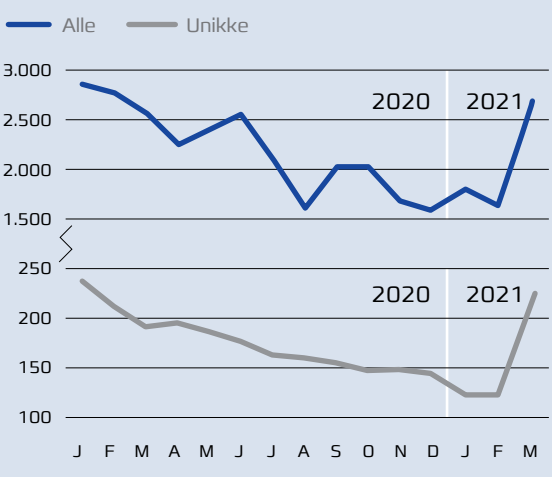
I 2020 modtog og udsendte DKCERT advarsler om 38 forskellige typer sårbarheder, som er identificeret på det danske forskningsnet. Denne service, som blev introduceret i slutningen af 2014, hjælper det danske forskningsnet med at afdække, hvilke mulige angrebspunkter, som ondsindede aktører nemt kan finde. Advarslerne kommer fra samarbejdspartnere, der dagligt scanner internettet for en række hyppige sårbarheder.

Størstedelen af sårbarhederne er kun blevet fundet i en håndfuld servere, og det vurderes, at de relativt hurtigt er blevet patchet, hvorved risikoen for kompromittering er blevet afhjulpet.

Figur 10: Hændelser og undersøgelser



Figur 11: Advarsler fra tredjeparter



4. Året i tal og ord

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.

Hvis sårbarhederne ikke håndteres, kan de derfor godt fremgå flere gange af opgørelsen.

Nogle sårbarheder medfører i sig selv ikke nogen reel risiko. Det kan fx være en server, der på applikationslaget afviser trafik, som den modtager på port 443. Men idet forbindelsen tillader forældet kryptering (fx SSL-POODLE), kan systemet stadig blive udsat for et Man-in-the-middle angreb, hvor en angriber får adgang til at 'lytte med'. Det eneste, en angriber får som udbytte, er viden om, at porten er lukket.

En mulig, men ikke anbefalet løsning på håndtering af dette uden at patche sårbarheden er at afvise trafikken på et firewall-lag, hvorved en krypteringskanal ikke skal oprettes før afvisningen.

På månedsbasis er der i 2020 blevet udsendt mellem 150 og 200 unikke advarsler om sårbarheden på forskningsnettet. Det anslås, at omkring 60-70 pct. af disse er sårbarheder, der af forskellige årsager ikke er afhjulpet, hvorfor de er dubletter.

Over de fem år, hvor DKCERT har automatiseret udsendelsen af disse advarsler, er antallet af advarsler sendt til det danske forskningsnet generelt faldende fra i gennemsnit 650 på måned i 2016 til 176 pr. måned i 2020. Dette fald skyldes efter DKCERTs opfattelse, at forskningsnettets institutioner generelt er blevet bedre til at tage hånd om sårbarhederne, og at de i højere grad har implementeret patch management-procedurer som følge af krav i ISO27001 eller lign. Det kan også være en følge af bedre segmentering af institutionernes netværk.

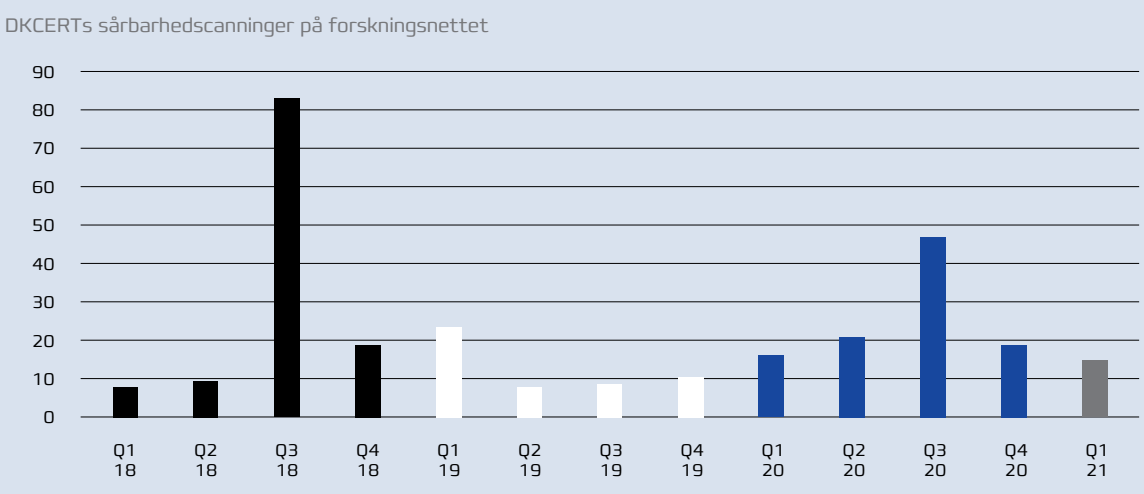
4.1.3 Sårbarhedsscanninger

DKCERT tilbyder institutioner tilknyttet DeiC sårbarhedsscanninger.

Scanningerne undersøger, om it-systemer har kendte sårbarheder, som angribere kan udnytte. DKCERT scanner IP-adresser på institutionerne og samler resultaterne i en rapport.

I 2020 har DKCERT gennemført 103 scanninger for medlemmerne af forskningsnettet. I 2018 var antallet på 121 og i 2019 52. Enkelte institutioner

Figur 12: I 2020 udførte DKCERT 103 scanninger på forskningsnettet



4. Året i tal og ord

får gennemført scanninger en gang årligt, mens andre får scannet hyppigere, fx hver andet måned.

Det samlede antal af scannede host-enheder/IP-adresser var i 2020 300.081, mens det i 2019 var på 474.730 host/IP-adresser og 184.698 i 2018.

Informationerne om de fundne sårbarheder i institutionerne kombineres med en redegørelse om hvilke tiltag, som bør iværksættes for at højne sikkerheden for den enkelte institution. Scanningstjenesten tilvejebringer således rapporter, der 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 systemet. CVSS er den internationalt anerkendte metode til scoring af sårbarheder på en skala fra 1-10.

De eksterne scanninger for 2020 viser, at tre pct. af sårbarhederne er kritiske, 17 pct. har vurderingen høj, 69 pct. er middel og 11 pct. er lav. I alt er der fundet 1.567 sårbarheder.

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

Sårbarheder findes i services, applikationer, operativsystemer og konfigurationer.

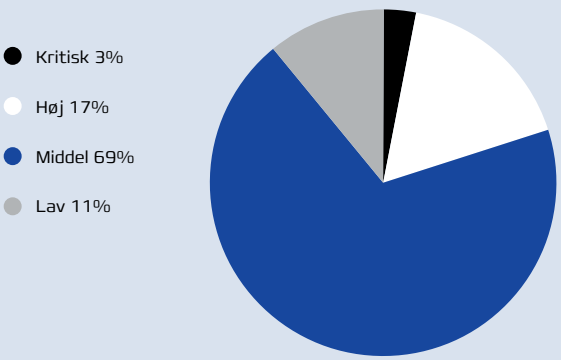
Sårbarhedernes opdeling er baseret på OWASP TOP 10 Web Application Security Risks 2020[35].

4.1.4 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, januar og marts 2021 i forbindelse med Sunburst-hændelsen på to universiteter i Danmark (Solarwinds Orionhændelsen, se side 21).

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

Figur 13: De i alt 1.567 fundne sårbarheder i DKCERTs eksterne scanninger i 2020 fordelt på kritikalitet



Ransomware

Det økonomiske guldæg for store og små spillere.

I sin seneste halvårs trendrapport Threat Matrix[A] har sikkerhedsfirmaet CSIS Security Group opgjort udviklingen inden for ransomware. Det fremgår her, at der globalt har været en øgning på 435 pct. i ransomware-angreb i 2020 i sammenligning med 2019. I over en tredjedel af ransomwareangreb er Ryuk-ransomwaren blev anvendt.

Ransomware kan distribueres direkte ved udnyttelse af sårbarheder i software, men også via trojanske heste som fx Emotet, som blandt andet spredes ved hjælp af spearphishingangreb. Både Emotet og den lige så kendte TrickBot startede som trojanske heste rettet mod banksektoren, men har i de senere år udviklet sig markant til at have en avanceret modulær funktionalitet, der muliggør alt fra cryptojacking og ransomware til sofistikerede datatyverier. I stigende grad bliver de brugt til at give angribere adgang og opretholde en tilstedeværelse i et netværk. Dette kan være en forløber for yderligere downloads af malware, fx ransomware.

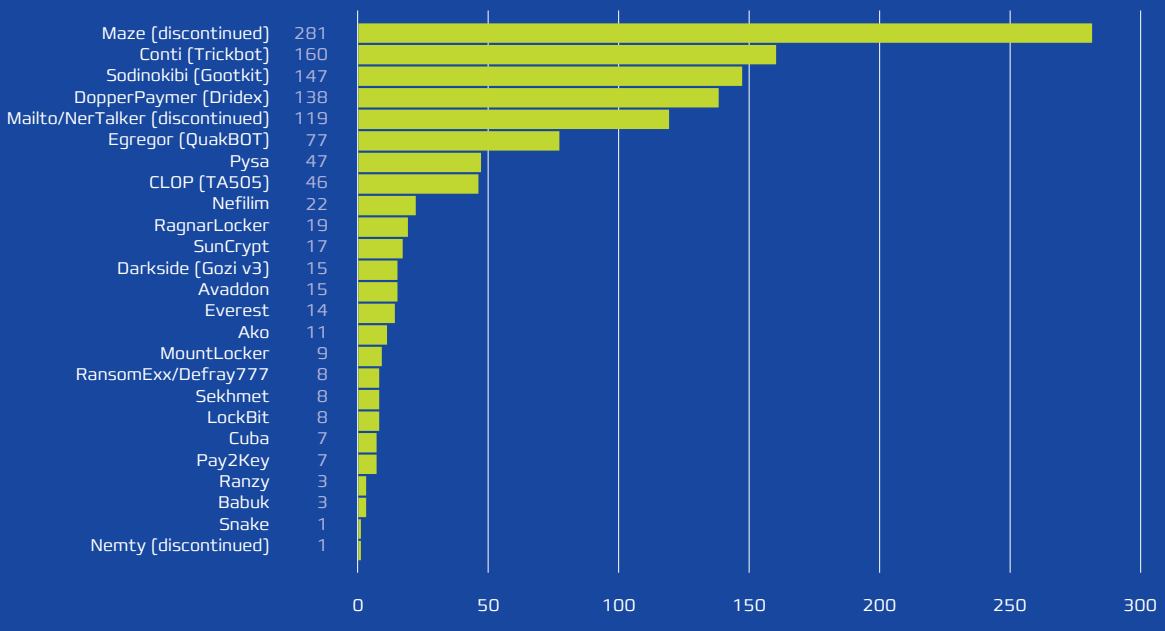
Trickbots Command&Control-servere (C&C eller C2) blev i oktober 2020 forsøgt taget ned for at hindre distributionen af Trickbot-malwaren. Dette skete i en koordineret indsats med deltagelse af Microsoft og US Cyber Command op til det amerikanske præsidentvalg i november. Indsatsen bar frugt i første omgang, og det amerikanske valg blev af CISA (USAs Cybersecurity and Infrastructure Security Agency) betegnet som det sikreste nogensinde. Selv om 90 pct. af de inficerede enheder blev taget ned, opretholdt trusselsaktørerne bag Trickbot kontrol over ca. 10 pct. af botnettet efter ændringer i konfigurationen. I forlængelse af dette blev en ny version af Trickbot distribueret ved hjælp af BazarLoader, SmokeLoader og Emotet, som ikke blev ramt af operationen.

CSIS Security Group skriver i halvårsrapporten, at antallet af bots stiger dagligt, og hurtigt har trusselsaktøren med nye C2-servere etableret botnets med mere end 40.000 computere. Trickbot er på vej tilbage til tidligere tiders styrke.

[A] https://www.csisgroup.com/engagement-hub

Figur 14: Antal af angreb med datalækage

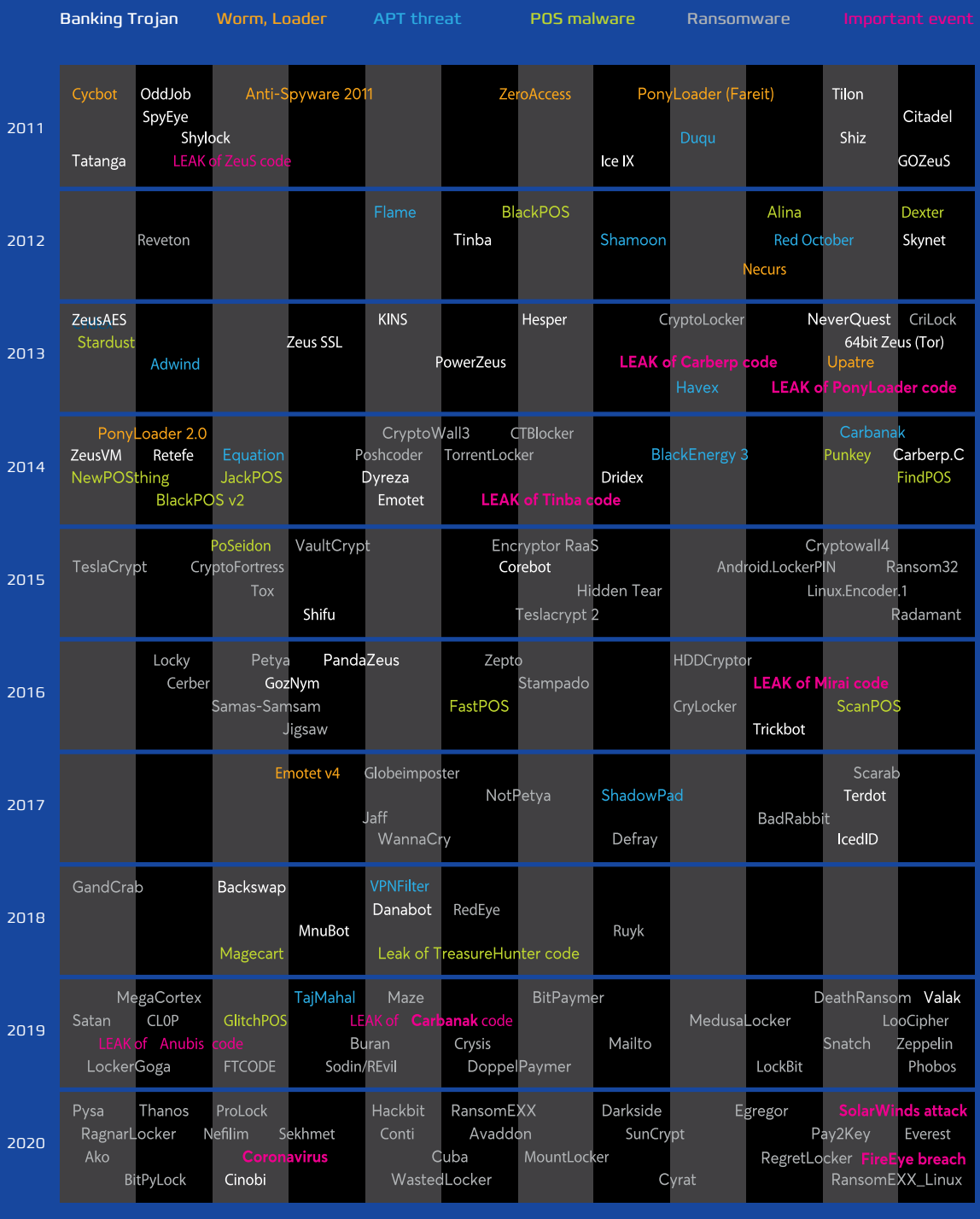
Grafen viser antallet af angreb med datalækage, hvor trojanere har medført installation af malware på et offers netværk. De fleste typer af malware på listen er oprindeligt kendt som ransomwaretyper, men de anvendes nu også til læk af data i forbindelse med et ransomwareangreb.



Ransomware

Figur 15: Malware timeline

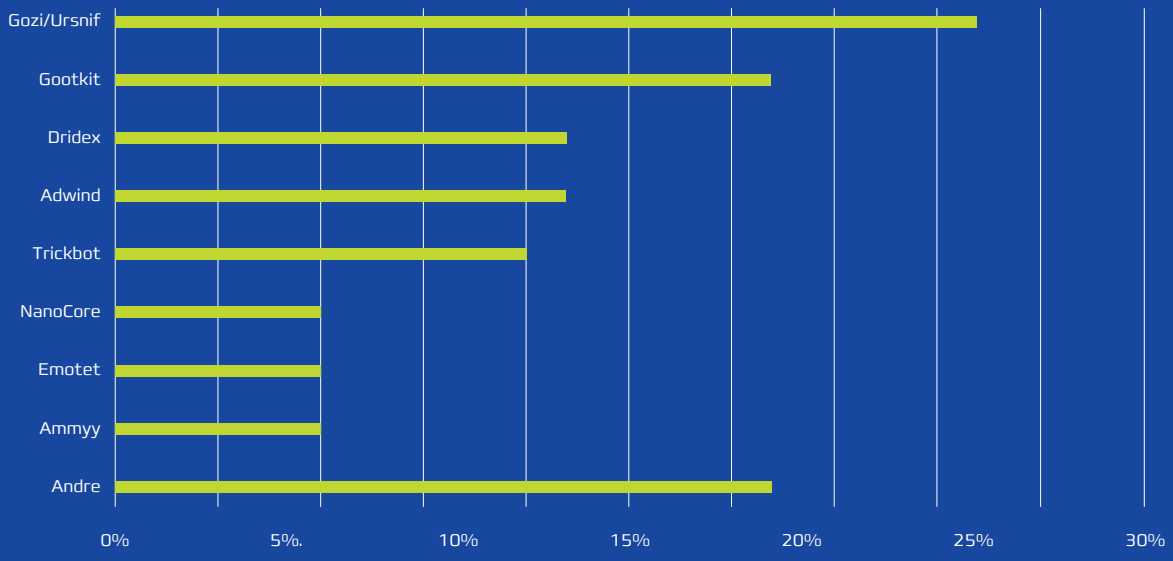
CSIS' optegnelse over internationale cybersikkerhedshændelser i de sidste ti år. Inden for de sidste to år er der blevet lanceret flere typer ransomwaretyper end fra 2011 til 2018 til sammen.



Ransomware

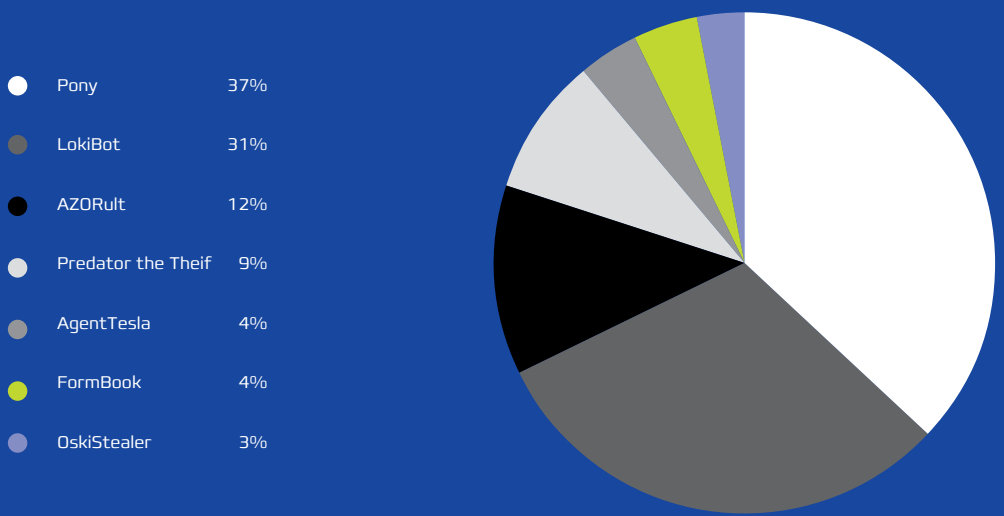
Figur 16: Kendte malware- og ransomwaretypers angreb på Danmark

Danske virksomheder og myndigheder slipper ikke for at blive angrebet. Data fra CSIS' incident response kit (CIRK) viser, at Danmark også bliver udsat for angreb fra internationalt kendte malware og ransomwaretyper.



Figur 17: Infostealers 2. halvår 2020

Infostealers er malware, der forsøger at stjæle information fra ofrene. Informationen kan både være loginoplysninger til onlinetjenester eller emailkorrespondancer, som vil kunne indgå i business email compromise-kampagner, hvor social engineering spiller en vigtig rolle. Grafen viser den internationale fordeling mellem forskellige typer af infostealers.



4. Året i tal og ord

4.2 VIDENDELING

4.2.1 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 facilitering af 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.

Aalborg universitet: Hurtig reaktion afgørende for at begrænse skaderne

I sommeren 2020 blev Aalborg Universitet ramt af en alvorlig hændelse. DKCERT blev kontaktet af AAU umiddelbart efter, at AAU havde foretaget den første problemafdækning, som viste, at angriberne anvendte metoder, hackeraktiviteter og værktøjer som kendes fra målrettede ransomware-angreb.

DKCERT bidrog med kontakt til CFCS og med at levere logdata fra NetFlow – fra vores dataanalysetjeneste. Derudover medvirkede DKCERT i kommunikationen med omverdenen om hændelsen.

4.2.2 Faglig videndeling i netværk

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

SikRef blev etableret i 2020, hvor der blev gennemført tre møder. Møderne omhandlede bl.a. hændelsen på Aalborg Universitet, danske myndigheder og aktørers roller og ansvar i hændelsessituationer, værktøjer og platforme til videndeling og advarsler om aktuelle trusler, malware og angrebsvektorer.

Der deltager hver gang ca. 30 sikkerhedsmedarbejdere til møderne.

For at styrke det faglige fællesskab på DPO-området driver DKCERTs DPO-tjeneste endvidere et netværk for universiteter og professionshøjskolers GDPR-professionelle. Se afsnit 4.3.1.

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 mødtes under coronakrisen i foråret 2020 ugentligt, senere hver anden uge og i 2. halvår ca. en gang om måneden. I 2021 er der planlagt månedlige møder.

DKCERT-CAB (Change Advisory Board), et rådgivende panel med repræsentanter for DKCERTs brugere, er nedlagt i forbindelse med ny referencegruppestruktur i DeiC. Panelet afholdt to møder i 1. halvår 2020.

4. Året i tal og ord

4.2.3 Strategisk videndeling 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. Rådets primære opgave i 2021 er at færdiggøre arbejdet med regeringens nye cyber- og informationssikkerhedsstrategi.

Uddannelses- og forskningssektoren er endvidere repræsenteret i rådet ved universitetsdirektør Georg Dam Steffensen, ITU, vicedirektør for it og digitale medier Peter Bruun Nielsen, AU, og lektor Christian Damsgaard Jensen, DTU.

4.2.4 Videndeling blandt ligesindede i Rådet for digital sikkerhed

DKCERT er medlem af Rådet for Digital Sikkerhed med Henrik Larsen som bestyrelsesmedlem. Endvidere deltager projektleder Morten Eeg Ejrnæs Nielsen i Rådets arbejdsgruppe for personoplysninger og GDPR.

Rådet er en privat forening, 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.

4.2.5 International videndeling

CERT/CSIRT'erne[36] for de fem nordiske forskningsnet holder videomøder sammen med NORDUnet-CERT en gang om måneden. På møderne diskuterer deltagerne aktuelle sikkerhedshændelser og erfaringer med værktøjer og metoder.

DKCERT er akkrediteret medlem af Trusted Introducer og dermed af TF-CSIRT, der er en organisation for CERT/CSIRT'er i Europa, det vestlige Asien og den tidligere Sovjetunion. Netværket, der nu har mere end 400 medlemsteams, faciliteres af de europæiske forskningsnets paraplyorganisation GÉANT.

DKCERT er også medlem af FIRST.org (Forum of Incident Response and Security Teams), som er en organisation for p.t. 574 CERT/CSIRT-teams i 97 lande. DKCERT-medarbejdere deltager jævnligt i seminarer samt på årskonferencen og generalforsamlingen.

Endvidere deltager Henrik Larsen og projektleder Morten Eeg Ejrnæs Nielsen i den globale Academic Security SIG, der traditionelt mødes fysisk en gang årligt i forbindelse med FIRST.org's årskonference og en til to gange via videokonference.

Henrik Larsen deltager i GÉANTs SIG-ISM (Special Interest Group Information Security Management) og i styregruppen for den nordiske regionale gruppe under SIG-ISM. SIG-ISM beskæftiger sig med de nationale forsknings- og uddannelsesnetværks (NRENs) interne sikkerhed og har halvårlige fysiske møder, heraf et årligt fællesmøde WISE Community, som er et globalt netværk for sikkerhed i forsknings-it-infrastrukturer (bl.a. udsprunget af CERN). I 2020 har alle møder i de nævnte grupper været virtuelle.

[36] CERT® er siden 1997 et registreret varemærke og stod oprindeligt for Computer Emergeny Response Team. CERT blev tidligere anvendt bredt, men må kun bruges, hvis en organisation (som fx DKCERT) er autoriseret til det af ejeren af varemærket, Software Engineering Institute, Carnegie Mellon University. I stedet anvendes det mere generiske CSIRT (Computer security incident response teams). DKCERTs officielle navn er således Danish Computer Security Incident Respons Team).

4. Året i tal og ord

4.2.6 Nyhedsformidling

DKCERT publicerer dagligt eller næsten dagligt nyheder om trusler, sårbarheder, hændelser og andre forhold, der har relevans for sikkerhedsdagsordenen i Danmark på cert.dk og via Twitter. Selv om mange af nyhederne baserer sig på internationale medier, udvælger DKCERT dem, der er relevante i en dansk kontekst og perspektiverer dem ind i danske forhold.

Vores mål med den formidlingstilgang er at skabe en bredere forståelse af cyber- og informationssikkerhed blandt vores modtagere og derigennem øge bevidstheden om betydningen af det enkelte individs handlinger og adfærd i forhold til informationssikkerheden – både i en professionel og en privat sammenhæng.

Hver mandag udsender vi nyhedsbreve til det sikkerhedsprofessionelle segment ved uddannelses- og forskningssektoren, øvrige ansatte ved forskningsnetinstitutionerne og DKCERTs interessenter generelt. Borgere og små og mellemstore virksomheder også har mulighed for at modtage et nyhedsbrev, der er målrettet dem. Endelig sendes nyhedsbrevene til pressen.

Derudover skriver chefen for DKCERT, Henrik Larsen, hver måned en klumme i Computerworld, hvor aktuelle problemstillinger om cyber- og informationssikkerhed bliver bragt på banen.

I 2020 blev der udgivet 307 artikler omhandlende informationssikkerhed på cert.dk mod 289 i 2019.

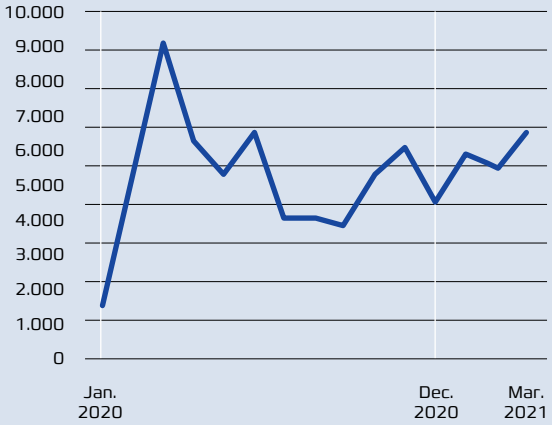
Cert.dk havde 55.749 besøgende i 2019. I 2018 var antallet på 51.408. Antallet af unikke sidevisninger var i 2020 på 81.288 mod 78.976 i 2019.

Ved udgangen af 2020 abonnerede 1.539 personer på et af DKCERTs nyhedsbreve. Tallet er steget en smule i forhold til 2019, hvor antallet af abonnenter landede på 1.510.

DKCERT har ved udgangen af 2020 3.074 følgere på Twitter. En stigning fra 2.841 i slutningen af 2019.

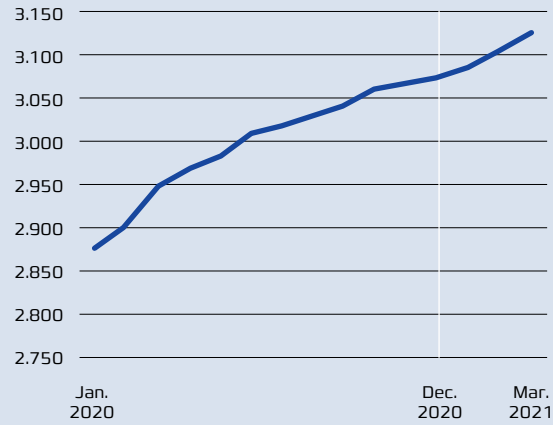
Figur 18: Unikke page views på cert.dk

Antallet af unikke page views på cert.dk.



Figur 19: DKCERT på Twitter

Antallet af følgere på Twitter.



Klummer i Computerworld

Hver måned skriver Henrik Larsen en klumme i Computerworld, hvor der sættes spot på en aktuel problemstilling i forhold til cyber- og informationssikkerhed.

- **JANUAR:** En ny dreng i klassen. Velkommen til Danish Hub for Cybersecurity.
  https://cert.dk/da/cert.dk/da/klumme/2020-02-03/en-ny-dreng-i-klassen

- **FEBRUAR:** Cyber, cyber, cyber. Glem ikke at det først og fremmest handler om informationssikkerhed - at sikre informationer mod tab af integritet, tilgængelighed og fortrolighed. Har vi informationssikkerheden på plads, får cyberkriminelle, -spioner, -terrorister og -hacktivister ikke mange ben til jorden.
  https://cert.dk/da/cert.dk/da/klumme/2020-02-03/cyber-cyber-cyber

- **MARTS:** I en krisetid er det afgørende at have en beredskabsplan. Den verdensomspændende corona-epidemi viser betydningen af at være godt forberedt på selv det mest uventede. Men at være godt forberedt er ikke kun afgørende i forhold til virusudbrud og pandemier. Det skal man også være i forhold til cyberangreb.
  https://cert.dk/da/klumme/2020-27-03/I-en-krisetid-er-det-afgoerende-at-have-en-beredskabsplan

- **APRIL:** Hvad vi kan lære af corona-krisen? Sikkerhedsfolk kan lære flere gode ting af corona-krisen - ikke mindst når det handler om styring og overblik.
  https://cert.dk/da/klumme/2020-24-04/Hvad-corona-krisen-kan-laere-os

- **MAJ:** Coronakrisen er på retur. Cyberkrisen fortsætter. DKCERTs Trendrapport 2020 er på gaden.
  https://cert.dk/da/klumme/2020-05-30/Coronakrisen-paa-vej-retur-cyberkrisen-fortsaetter

- **JUNI:** Endelig sommer: Men du kan ikke slappe helt af. Sommerferien står for døren og mange af os kan lægge en hektisk og anderledes periode bag os – noget ingen af os har prøvet før. Kan vi så læne os tilbage og slappe af?
  https://cert.dk/da/klumme/2020-06-26/endelig-sommer-men-du-kan-ikke-slappe-af

Klummer i Computerworld

- **JULI:** NemID 10 år. Et jubilæum værd at fejre. At vi har NemID – en gratis, statsanerkendt digital identitet med et højt sikkerhedsniveau – giver Danmark et stort forspring i digitaliseringen. Men historien om NemID minder os også om, at ingenting er 100 pct. sikkert, og at man skal holde øje med udviklingen omkring sig for at være med.
  https://cert.dk/da/klumme/2020-08-03/NemId-10-aar

- **AUGUST:** Du har selv ansvaret for dine data. På samme måde som borgerne har ejerskabet over deres eget køleskab og tager ansvar for risikoen ved at spise indhold, hvis 'bedst før'-dato er overskredet, har dataejeren også selv ejerskabet over egne data og tager ansvaret for selv at tjekke holdbarhedsdatoen.
  https://cert.dk/da/klumme/2020-08-28/Du-har-ansvaret-for-dine-data

- **SEPTEMBER:** Bare det var oktober hele året rundt. Oktober er en fantastisk måned for informationssikkerheden i kraft af sikkerhedsmånedens fokus. I år er familiers informationssikkerhed på dagsordenen.
  https://cert.dk/da/klumme/2020-09-27/Bare-det-var-oktober-hele-aaret-rundt

- **OKTOBER:** Holder MitID også 10 år? Vi har netop fejret NemIDs 10 år jubilæum, og nu er afløseren MitID på vej. Lad os se lidt nærmere på, hvad MitID egentlig er, og om forudsætningerne for om MitID også kan blive 10 år er til stede.
  https://cert.dk/da/news/2020-10-30/Holder-MitID-ogs%C3%A5-10-aar%3F

- **NOVEMBER:** Hvorfor videnssektoren er (næsten) lige så kritisk som de kritiske sektorer. Den viden, som kommer fra universitets- og forskningsverdenen skal beskyttes. Dels for at understøtte vores samfundsmodel og dermed beskytte samfundet, dels for at hindre, at den kan understøtte cyberkriminaliteten i at udnytte den.
  https://cert.dk/da/klumme/2020-11-27/Hvorfor-videnssektoren-er-%28naesten%29-lige-saa-kritisk-som-de-kritiske-sektorer

- **DECEMBER:** Et kig ind i krystalkuglen. Her er mine forudsigelser om cybersikkerhed for det kommende år.
  https://cert.dk/da/klumme/2020-12-23/Et-kig-i-krystalkuglen-for-2021

4.3 TJENESTER

4.3.1 DPO-tjenesten

DeiC introducerede i 2017 DPO-tjenesten, der fungerer som en fleksibel ressource i forhold til databeskyttelsesopgaver, og som kan fungere som ekstern databeskyttelsesrådgiver (DPO, Data Protection Officer). Dette gav institutionerne mulighed for at få løst de databeskyttelsesopgaver, som lovgivningen kræver, men som fx ikke nødvendigvis kræver en fuldtidsansat DPO.

Tjenesten er hjemmehørende hos DKCERT og har indgået aftaler med en række uddannelsesinstitutioner om dels fast rådgivning, dels mere ad hoc-hjælp. I 2020 varetog tjenesten DPO-funktionen hos følgende institutioner:

- Roskilde Universitet (RUC)
- IT-Universitetet (ITU)
- Professionshøjskolen Absalon.
- Det Kongelige Akademi – Arkitektur, Design, Konservering (KADK).
- Arkitektskolen Aarhus (AARCH).
- Designskolen Kolding.
- Dansk Dekommissionering.
- Studievalg Danmark.

Yderligere er der indgået aftaler om ad hoc-bistand med opgaver inden for databeskyttelsesområdet med både Journalisthøjskolen (DMJX) og UC SYD.

I slutningen af 2020 blev der ansat endnu en medarbejder til DPO-tjenesten, samtidig med at Den Frie Lærerskole og en række maritime skoler og maskinmesterskoler blev tilknyttet tjenesten fra 2021.

Derudover løste DPO-tjenesten opgaver med jævne mellemrum for Uddannelses- og Forskningsministeriet i form af assistance til ministeriets tilsynskoncept for de fælles studieadministrative systemer, udarbejdelse af databehandleraftaler, rådgivning og i 2020 også en gennemgang af sikkerheden og databeskyttelsen i det kommende studieadministrative programfællesskab, Kopernikus.

I forlængelse af tjenestens opgave med at varetage DPO-funktionen hos en række forsknings- og uddannelsesinstitutioner driver DPO-tjenesten et netværk for institutionernes DPO'er, hvor der i 2020 blev afholdt fire møder. Alle universiteter og professionshøjskoler samt de kunstneriske uddannelser under UFM: (KADK, AARCH og Designskolen Kolding) deltager i netværket.

Mellem møderne udveksler og deler netværket løbende informationer om den nyeste praksis og fortolkning om implementeringen på forsknings- og uddannelsesinstitutionerne. Ligeledes har netværket nedsat en række arbejdsgrupper og koordinerer indstillinger til Danske Universiteter og til Datatilsynet.

4.3.2 TeleDCIS

DKCERT er vært for telesektorens decentrale cyber- og informationssikkerhedsenhed, TeleDCIS. Telesektoren er en af de seks kritiske sektorer, der som en følge af den nationale cyber- og informationssikkerhedsstrategi fra 2018 skal have sin egen strategi og koordinerende enhed. De danske teleoperatører oprettede derfor en TeleDCIS-forening i 2019 og outsourcede samtidigt den operative opgave til DKCERT, der ansatte en leder og en sikkerhedskoordinator til at drive enheden.

En decentral cyber- og informationssikkerheds-enheds (DCIS) primære opgave er at formidle, efterspørge, skabe og validere informationer om relevante informationssikkerhedsforhold mellem sektorens operatører og Center for Cybersikkerhed (CFCS). På den måde fungerer DCIS'en som et udvekslingspunkt for informationssikkerheds-informationer både til de enkelte operatører fra CFCS og til CFCS fra operatørerne. Formålet er, at der sker en udveksling og behandling af informationer begge veje så simpelt og gnidningsløst som muligt. For telesektorens vedkommende varetager TeleDCIS ud over de nævnte opgaver også koordination af informationsudveksling af cyber- og informationsmæssige hændelser, som har betydning for stabiliteten af den danske kritiske digitale infrastruktur.

Den viden, som TeleDCIS' har indsamlet og videregivet i 2020, har dannet baggrund for en opdateret risiko- og sårbarhedsvurdering, hvor også de væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester i Danmark har bidraget.

Ligesom i 2019 viste risiko- og sårbarhedsvurderingen for 2020, at teleoperatørerne opfatter IP-transmission som den mest sårbare tjeneste. Til sammenligning blev det i 2019 vurderet, at menneskelige fejl / insidertrusler er de største risici for de danske teleoperatører. I 2020 er de største trusler mod stabiliteten på den digitale infrastruktur med tilhørende serviceydelser vurderet til at være ransomware, phishing og menneskelige fejl.

I betragtning af den øgede afhængighed af internettjenester vil vigtigheden af en pålidelig og stabil IP-transmissionskapacitet kun vokse. Således vil udveksling af 'best practice' til opretholdelse af stabil IP-transmission mellem operatører være en vigtig del af handlingsplan som følge af risiko- og sårbarhedsvurderingen for sektoren.

Disse risici og sårbarheder vil sammen med andre fund i vurderingen for 2020 blive prioriteret og indarbejdet i forskellige initiativer i opdateringen af cyber- og informationssikkerhedsstrategien for telesektoren.

I 2021 vil der derfor være fokus på, hvordan TeleDCIS sammen kan sikre en mere optimal deling af hændelser og varslinger. Én af initiativerne er, i fællesskab med teleoperatørerne, at inddrage flere kilder som kan bidrage med information om cyber- og informationsmæssige hændelser. Samtidig skal der tages hensyn til, at der ikke opstår et informationsoverload, hvor for meget, ikke-relevant information skygger for den væsentligste, hvorved informationsdelingen mister sin værdi.

En af metoderne til dette er deltagelse i den fælles MISP for DCIS'erne, hvor TeleDCIS har spillet en aktiv rolle i etableringen (se også afsnit 4.4.2), hvis etablering blev afsluttet i 2020.

I 2021 vil TeleDCIS fortsat arbejde for, at MISP'en bliver den primære kommunikationsplatform for sektoren i forhold til deling af viden om malware og indicators of compromise (IoC). Endvidere vil TeleDCIS påbegynde arbejdet med en ny cyber- og informationssikkerhedsstrategi for telesektoren, når en ny national strategi for cyber- informationssikkerhed bliver lanceret – forventeligt i 2. halvår 2021.

4.3.3 Awarenesstjenesten Phish

DKCERTs awarenesstjeneste Phish tester brugeres reaktion på phishingangreb. Universiteter og andre institutioner på forskningsnettet kan bruge tjenesten til at få udsendt fingerede phishing-mails til ansatte og studerende mhp. at monitorere reaktionsmønstre hos brugerne. DKCERT hjælper således med gennemførelsen af en phishingkampagne, der afsluttes med en detaljeret og anonymiseret rapport.

Tjenesten kan bruges som led i en awarenesskampagne med henblik på at øge opmærksomheden på phishing-mail.

I 2020 er der gennemført kampagner for Aarhus Universitet, University College Lillebælt, DeiC og CBS.

4.4 NYE TJENESTER I 2021

4.4.1 Beredskabsøvelser

DKCERTs udvikler Simon Nexø Jensen har i flere år deltaget i og bidraget til planlægning og afholdelse af den europæiske beredskabsworkshop CLAW. CLAW-workshoppen er et tilbud fra GÉANT, som har til formål at styrke kriseberedskabet på tværs af alle europæiske forskningsnet.

CLAW er en workshop med en interaktiv kriseøvelse, som giver deltagerne mulighed for i et realistisk scenarie at afprøve de forskellige aktiviteter og fagligheder, der skal i spil i forbindelse med håndtering af kriser. De hidtidige workshops har været afviklet over to dage på universiteter og datacentre i Europa, mens konceptet i 2020 blev gennemført virtuelt på en dag.

I 2021 vil DKCERT tilbyde institutionerne på forskningsnettet at deltage i en beredskabsworkshop efter inspiration i CLAW-konceptet.

I februar 2021 har konceptet været afprøvet sammen med Det Kongelige Bibliotek, og det er nu klart til at blive tilbudt andre institutioner. I første omgang er workshoppen tilrettelagt i et virtuelt format, men når der senere bliver mulighed for det, vil den kunne gennemføres fysisk.

4.4.2 Universitetssektorens MISP

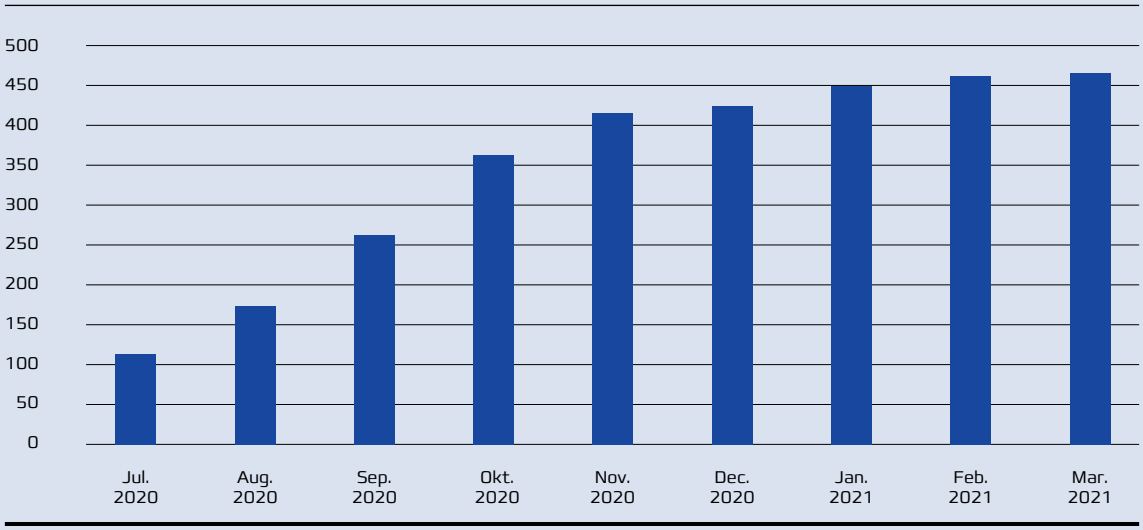
Uddannelses- og forskningssektorens MISP åbnede som pilotprojekt for de første brugere i juli 2020. MISP'en er fortsat under opbygning, men er fra primo 2021 gået i officiel drift. I dag er otte institutioner – heriblandt de fleste universiteter – tilknyttet MISP'en.

MISP står for Malware Information Sharing Platform. Det er en open source platform, der første gang så dagens lys i 2011, da en sikkerhedsmedarbejder i det belgiske forsvar var frustreret over at få tilsendt advarsler og indicators of compromise (IoC'er) pr. email. Siden har tanken om en mere systematisk deling af viden om malware bredt sig, så der i dag er mere end 6000 organisationer på verdensplan, der bruger MISP[37].

En MISP kan sikre hurtigere deling, kommunikation og alarmering på tværs af aktører og sektorer. Det er muligt i en MISP at opsætte regler for en struktureret automatisk deling, hvilket betyder, at deling af information, herunder varsler og sårbarhedsinformationer, vil kunne blive segmenteret, så aktører kun modtager den information, der er relevant for deres organisation. Delingen foregår enten manuelt eller automatisk ved integration til virksomhedens filtre eller logsystemer.

[37] https://www.misp-project.org/

Figur 20: Antallet af hændelser i universiteternes MISP siden pilotdriften i juli 2020



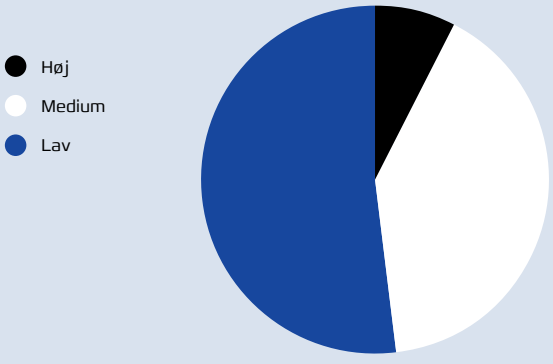
En MISP kan også automatisk samle data fra flere kilder. På denne måde behøver aktører ikke gennemgå adskillige varselsmails fra flere abonnementskilder for at skabe et overblik over sårbarheder. Ved gennemgang af disse informationer er det muligt for aktører at få en hurtigere forståelse af trusler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

At være tilknyttet MISP'en betyder, at institutioner kan tilføje IoC'er og hændelser og få information om, hvad andre institutioner tilføjer. Samtidig kan brugerne søge tilbage i databasen efter hændelsestype, frekvens og andre relevante oplysninger, der kan medvirke til analyse af et aktuelt trusselslandskab.

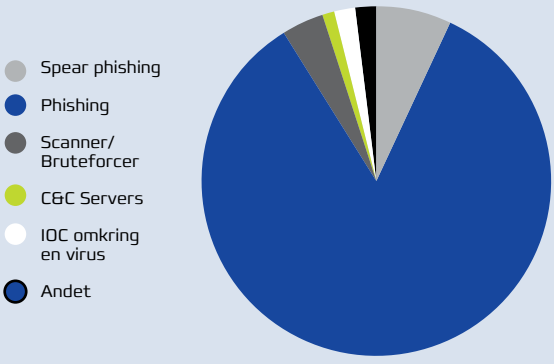
MISP'en er modulerbar og kan – afhængig af konfigurationen – implementeres med henblik på deling af viden med andre sektorer, brancher eller organisationer, både nationalt og internationalt. I Danmark indgår telesektoren i en MISP i samarbejde med de andre decentrale cybersikkerhedsenheder i de øvrige samfundskritiske infrastruktursektorer, finans, søfart, sundhed, energi og transport. Universitetssektoren er p.t. ikke medlem af denne overordnede MISP, da uddannelses- og forskningssektoren ikke er udpeget som samfundskritisk sektor.

Universitetssektorens MISP er i første omgang sat op til at dele information mellem aktørerne internt i sektoren, men vil kunne dele oplysninger med en kommende nordisk MISP mellem de fem nordiske forskningsnet, ligesom den allerede i et vist omfang manuelt deler hændelser med den sektorfælles MISP. Den vil også kunne tilkobles den omtalte sektorfælles MISP, idet man kan 'tagge' hændelserne til at blive delt inden for specifikke grupper i MISP'en.

Figur 21: Hændelser i universitetssektorens MISP fra 1. juli 2020 til 31. marts 2021 fordelt på kritikalitet



Figur 22: Fordelingen af hændelser, der er registreret i universitetssektorens MISP fra 1. juli 2020 til 31. marts 2021



4.5 DANSKERNES INFORMATIONSSIKKERHED 2020

I 2020 har DKCERT i samarbejde med Digitaliseringsstyrelsen, KL og Danske Regioner for sjette gang gennemført analysen Danskernes Informationssikkerhed[38]. Analysen udmøntede sig i en rapport, der er udarbejdet som led i Den fællesoffentlige digitaliseringsstrategi 2016-2020.

Undersøgelsen giver en status på oplevelser med, kendskab til og adfærd inden for informationssikkerhed hos to grupper: Borgere og offentligt ansatte.

Hvor de tidligere års rapporter har fokuseret på de hændelser, som borgere og offentligt ansatte blev udsat for, har 2020-rapporten suppleret med en mere systematisk analyse af danskernes efterlevelse af anbefalingerne til sikker adfærd, som fremgår af portalen sikkerdigital.dk.

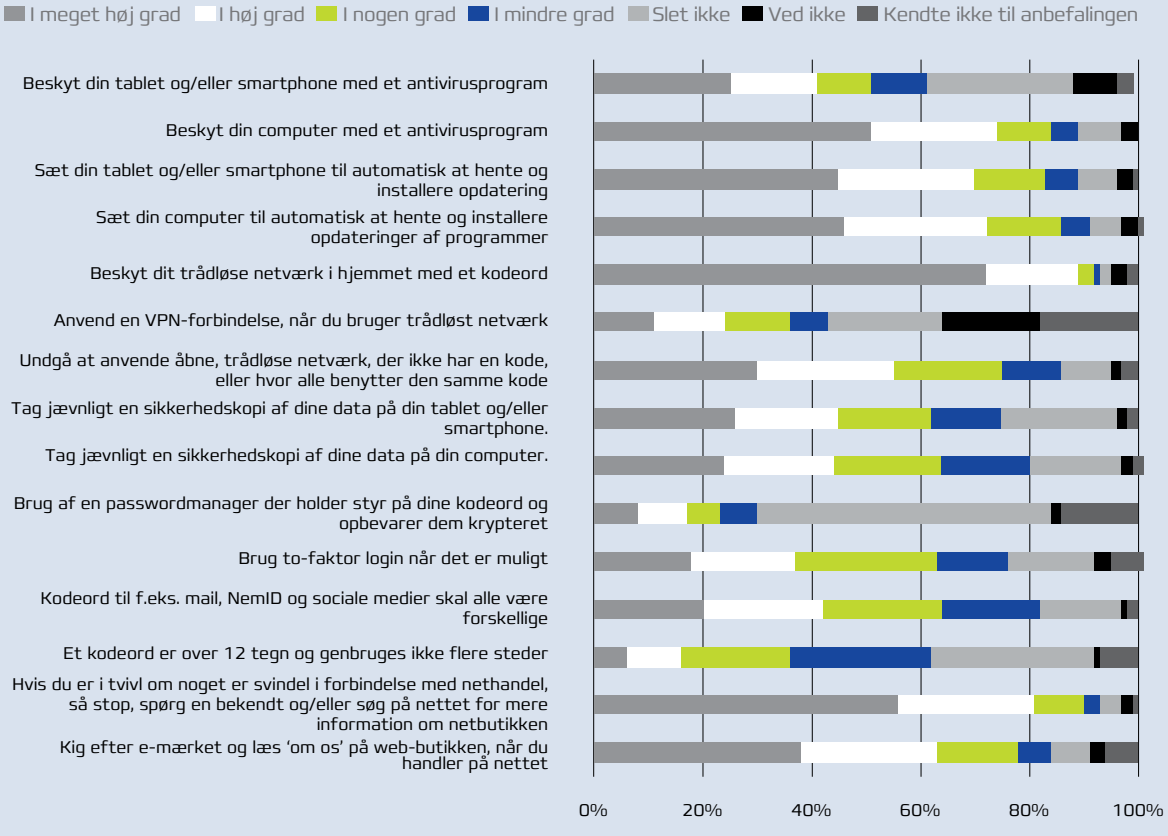
Borgerne har det nemmest med de nemmeste anbefalinger

Rapporten konkluderer overordnet, at borgerne – forventligt nok – oftere efterlever de 'nemme' anbefalinger om god sikkerhedsadfærd end de svære.

Fx angiver ni ud af ti borgerne, at de i høj/meget høj grad efterlever anbefalingen om at beskytte deres trådløse netværk i hjemmet med en kode, mens syv ud af ti borgere oplyser, at de i høj/meget høj grad efterlever anbefalingerne om automatisk opdatering af deres computer (71 pct.) og telefon/tablet (70 pct.). Til gengæld er

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

Figur 23: Danskernes (18-74 år) efterlevelse af anbefalingerne vedr. sikker adfærd



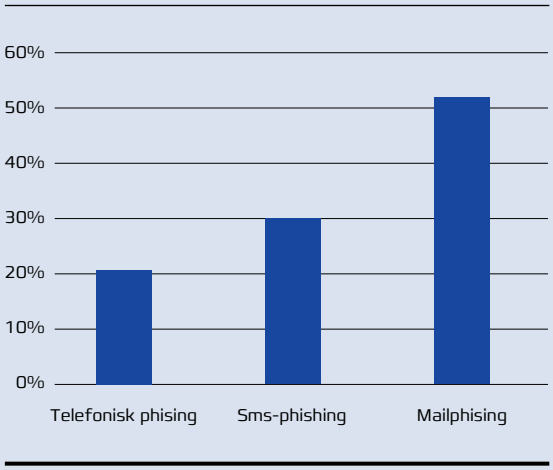
det kun godt halvdelen af borgerne (54 pct.), der angiver, at de i høj/meget høj grad efterlever anbefalingen om at undgå at anvende åbne trådløse netværk, mens 24 pct. oplyser, at de efterlever anbefalingen om anvendelse af VPN-forbindelse, når de bruger trådløse netværk. 44 pct. angiver, at de i høj/meget høj grad efterlever anbefalingen om jævnligt at tage sikkerhedskopi af data på computer (44 pct.).

Anbefalingen om stærke kodeord er den, de færreste oplyser at efterleve. Kun 16 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen om, at et kodeord er over 12 tegn og ikke genbruges flere steder. 17 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen om brug af en passwordmanager, mens 37 pct. oplyser, at de i høj/meget høj grad efterlever anbefalingen om to-faktorlogin.

Generelt ses det, at det er relativt få borgere, der ikke kender de gode råd og anbefalinger. Dette falder godt i tråd med det, at de fleste borgere (74 pct.) angiver at være opmærksomme på risikoen for bedrageri og cyberkriminalitet. Samtidig mener op mod 90 pct. af borgerne, at risikobetonet adfærd medfører øget risiko for tab af data. 64 pct. oplyser, at de føler sig godt klædt på til at beskytte sig mod de digitale trusler.

Samlet set tyder det på, at forudsætningerne for, at danskerne har sikker adfærd, er til stede, men alligevel halter det på visse områder i forhold til efterlevelsen, jf. Figur 23.

Figur 24: Andelen af borgere, der har været udsat for forskellige typer af phishing inden for de seneste år



Overordnet tegner der sig et billede af, at de anbefalinger, hvor man 'blot' skal slå en funktion til som fx automatisk opdatering eller beskyttelse af netværk med kode, i højest grad bliver efterlevet. De anbefalinger, der kræver aktive handlinger (fx sikkerhedskopi), kognitiv energi (lange og unikke kodeord) eller teknisk indsigt (VPN og passwordmanager) efterleves sjældnere.

Selv om man efterlever de gode råd, kan man ikke hindre at blive udsat for forsøg på phishing, som atter viser sig at være den helt store trussel for borgerne. Således har 64 pct. af borgene oplevet phishingforsøg via mail, sms ('smishing') eller telefon ('vishing') inden for de seneste år, mens otte pct. har oplevet alle tre former for phishing, jf. Figur 24. De færreste (under 1 pct.) oplyser dog, at de er faldet i fælden.

Samlet er der sket en stigning fra 51 pct. i 2018.

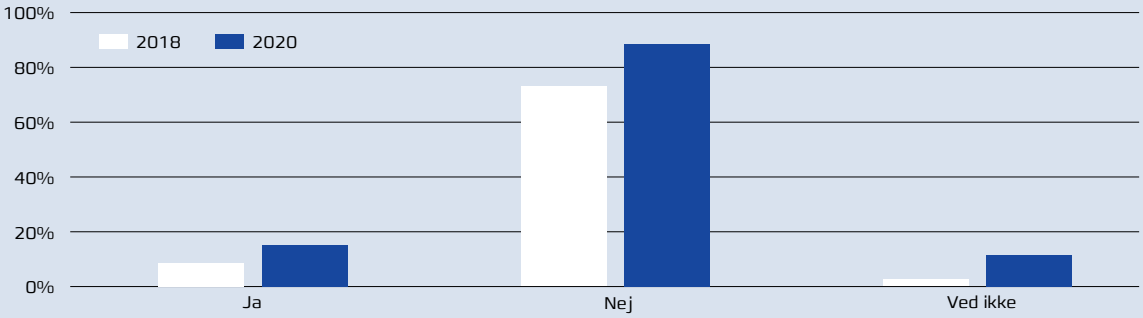
Offentligt ansatte følger ikke altid retningslinjerne

Også offentligt ansatte oplever phishing som den mest nærværende trussel. Således er der 46 pct., der i forbindelse med deres arbejde har prøvet at modtage mail, sms eller chat-besked fra en ukendt person med link, som afsenderen opfordrede til at klikke på. I modsætning dertil er det de færreste offentligt ansatte (3 pct.), der har oplevet virus eller andre typer skadelige programmer i forbindelse med arbejdet inden for det seneste år.

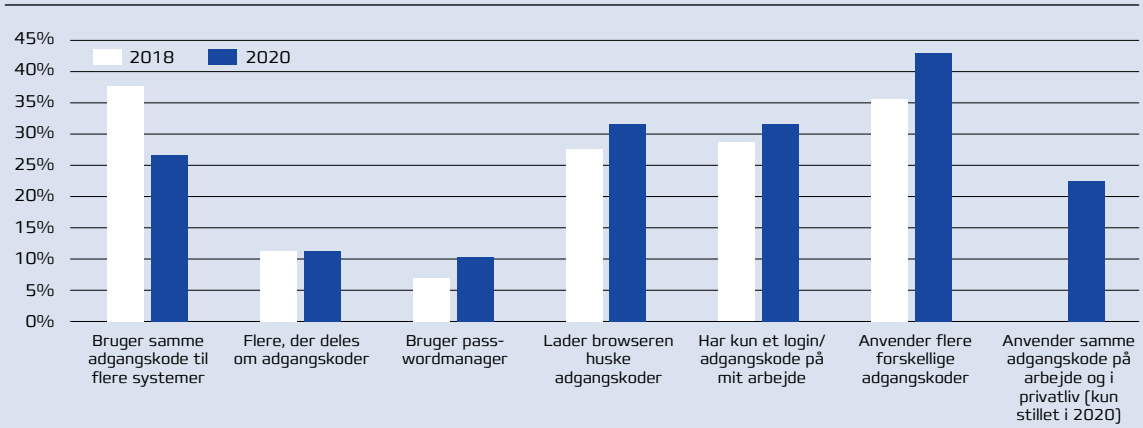
Mens der for borgerne opstilles anbefalinger for sikker adfærd, er det arbejdspladsernes informationssikkerhedspolitikker og retningslinjer, der bestemmer den ønskede adfærd. Kendskabet hertil og efterlevelsen er derfor en afgørende faktor for sikkerhedsniveauet.

Ganske mange – 65 pct. – angiver, at de i høj eller meget høj grad er bekendte med de retningslinjer og politikker, der er gældende for deres arbejdsplads. Dette er en logisk følge af, at 69 pct. at de offentligt ansatte oplyser, at de har modtaget undervisning eller information om retningslinjerne. Dette er en stigning fra 63 pct. i 2018, hvor undersøgelsen blev gennemført sidst.

Figur 25: Dobbelt så mange offentligt ansatte svarer i 2020 'ja' på spørgsmålet, om de nogle gange undlader at efterleve informationssikkerhedspolitikker og/eller -retningslinjerne for deres arbejdsplads, som i 2018



Figur 26: Offentligt ansatte er blevet bedre til at håndtere adgangskoder ift. 2018



Til gengæld er der sket en stigning i antallet af respondenter, der angiver, at de til tider undlader at følge retningslinjerne: I 2018 undlod otte pct. til tider at følge retningslinjerne, men det gælder for 15 pct. i 2020, jf. Figur 25. At disse 15 pct. oplyser 32 pct, at de enten ikke ved eller at de mindst en gang om ugen eller oftere undlader at efterleve retningslinjerne.

Blandt de offentligt ansatte, der svarer, at de til tider undlader at efterleve arbejdspladsens informationssikkerhedsretningslinjer og -politikker, svarer flest, at de skyldes, at det gør deres daglige arbejde besværligt/umuligt at udføre (61 pct.). 32 pct. angiver, at de selv vurderer, om det er nødvendigt at efterleve i de enkelte arbejdssituationer.

En retningslinje, som burde være gældende for alle arbejdspladser, er et forbud mod genbrug af kodeord. 22 pct. af de offentligt ansatte oplyser, at de anvender samme adgangskoder på arbejde og privatlivet. Med dette vil en kompromittering af private data og tjenester ikke alene gå ud over de private oplysninger, men også sikkerheden på arbejdspladsen.

Ganske vist tyder resultaterne, som er gengivet i Figur 26 på en positiv udvikling, men alligevel ser gode vaner og kultur omkring kodeord ikke at være forankret godt nok i den offentlige sektor endnu.

Rapporten kan i sin helhed downloades på cert.dk. https://cert.dk/sites/default/files/uploads/Dankernes%20informationssikkerhed%202020.pdf

5. Det eksterne perspektiv

Fire af DKCERTs samarbejdspartnere giver her indblik i, hvordan de kommunikerer om cyber- og informationssikkerhed.

Hvad er den bedste metode til at kommunikere om cyber- og informationssikkerhed? Kan vi lære noget af hinanden, når der skal arbejdes med adfærdskommunikation?

Vi har inviteret fire af vores samarbejdspartnere til at skrive et indlæg om den strategi, de lægger til grund for deres kommunikation om cyber- og informationssikkerhed.

Bidragyderne er:

> Trude Talberg-Furulund,
Seniorrådgiver, NorSIS, Norsk senter for informasjonssikring, der skriver om skellet mellem de proaktive og reaktive råd i kommunikationen

> Torben B. Sørensen,
Security Communication Specialist, Group Security Governance, Nets Denmark A/S, der inddrager gamification i opretholdelse af awareness i en stor organisation som Nets

> Eva Elisabeth Roland,
Specialkonsulent, Erhvervsstyrelsen, om betydningen af en løbende indsats og brug af værktøjer til at skærpe opmærksomheden i målgruppen

> Anders Due,
Kommunikationskonsulent, Datatilsynet, om de fem måder et tørt område som databeskyttelse og GDPR gøres tilgængeligt.

5. Det eksterne perspektiv

5.1 CYBERSIKKERHET – HVORFOR SKULLE CYBERKRIMINELLE VÆRE UTE ETTER LILLE MEG?

AV: TRUDE TALBERG-FURULUND,
SENIORRÅDGIVER, NORSIS/ NORSK SENTER FOR INFORMASJONSSIKRING

En av utfordringene med å kommunisere om cybersikkerhet, er at mange tenker at dette ikke gjelder dem. Hvorfor er jeg et attraktivt mål for en svindler? Hva har jeg av verdi for dem og hvorfor skal de plukke ut akkurat meg? Og hvorfor skal noen angripe min virksomhet, når det er så mange andre virksomheter de vil få mer igjen for å angripe?

Samtidig er de aller fleste av oss påkoblet internett og aktive brukere av digitale tjenester, både hjemme og på jobb, hver eneste dag. Det betyr at vi alle er potensielle mål for cyberkriminelle.

Rammer for vår kommunikasjon

Helt overordnet jobber Norsk senter for informasjonssikring (NorSIS) for 'en tryggere digital hverdag for alle'. Det er en stor oppgave. Det gir oss også et bredt spekter både av målgrupper og tema. I tillegg bør vår kommunikasjon være relativt samstemt med det andre aktører formidler av kunnskap og råd om samme tema. Andre formidlere kan være alt fra myndighetene, forvaltere av lovverket og tjenestetilbydere til medlemsorganisasjoner og interesseorganisasjoner.

Mottagere som får ulike budskap eller i noen tilfeller motstridene budskap vil, heller enn å forstå og ta til seg budskapet, bli forvirret og kanskje til og med apatisk overfor sikkerhetsbudskapet.

Det er derfor svært viktig for oss å ha god dialog med andre formidlere og alltid være oppdatert på nye rapporter, undersøkelser, mediesaker, hendelser og annet som rører seg. Da har vi, selv om vi ikke er enige i budskapet, mulighet til å møte andre meninger eller budskap på en måte som fortsatt gir målgruppene og mottagerne et klart budskap.

Hva trenger den enkelte mottager?

Deler vi målgruppene våre i to utfra situasjonen de er når vi kommuniserer med dem, snakker vi som regel enten til folk som kan rammes av en cybertrussel eller de som er rammet av cyberkriminalitet. Rådene våre deles derfor grovt sett inn etter om de er; proaktive råd, det vi si å forklare hva som kan ramme og hva du gjør for å unngå det, eller reaktive råd, det vil si veiledning til de som har havnet i trøbbel og trenger hjelp til å rydde opp.

Et av målene for NorSIS' kommunikasjon er å skape engasjement og deling fra brukerne. Her er et eksempel på, hvordan en bruker av NorSIS' Secflix-videoer har opprettet sin egen avstemning om bruk av totrinnspålogging på Facebook.

5. Det eksterne perspektiv

Proaktive råd om cybersikkerhet
Først og fremst er det viktig å fange mottagerens oppmerksomhet. Vi streber etter at budskapet skal være relevant, troverdig, engasjerende og enkelt. Vi tror den beste måten å oppnå dette på er å være så konkrete som mulig, både i beskrivelsen av utfordringen eller trusselen og i rådene vi gir. Dersom det er rom for det bruker vi eksempler eller illustrasjoner de kan kjenne seg igjen i. Litt avhengig av målgruppe og kanal bruker vi også tall og fakta, gjerne sammen med følelser og historiefortelling for å nå frem.

Innholdet vårt tar som regel utgangspunkt i budskap vi ønsker å formidle, som sikker passordbruk eller å sørge for å oppdatere. I tillegg reagerer vi på nyhetssaker, hendelser eller annet som rører seg. Da er budskapet som oftest knytte til hva dette betyr for deg og hvordan du håndterer dette eller lignende situasjoner. I tillegg lager vi ulike e-læringskurs. Både kurs du selv kan gå inn på nettsiden å ta og kurs arbeidsgivere kan bestille til sine ansatte.

Reaktive råd om cybersikkerhet
Kommunikasjon til deg som er rammet av en cybertrussel, handler først og fremst om å hjelp til å få kontroll over situasjonen. Kort, konsis informasjon, gjerne med konkrete huskelister eller sjekklister er vår tilnærming til dette. Gjerne også med henvisning til hvor du kan finne ut mer. Eksempler og illustrasjoner brukes for å vise at du ikke er den eneste som har opplevd dette.

For all vår kommunikasjon er det grunnleggende at den ikke på noen måte er 'dømmende'. Vi ønsker ikke å være moraliserende og dømmer deg ikke for at du har blitt utsatt for cyberkriminalitet. Dersom vi påfører noen skam for at de har blitt rammet gjør vi det vanskelig å søke hjelp eller veiledning.

Hvor kommuniserer vi?
Hvor du mottar budskapet innvirker på hvordan du tar det i mot. Både hvor du mottar det og hvor mye tid du har til å ta inn budskapet. I tillegg krever ulike kanaler ulik formidling og tilpasning av innholdet.

Dette løser vi ved å være i flere ulike kanaler med samme budskap. I tillegg til egne nettsider, nyhetsbrev og sosiale medier som Facebook og LinkedIn har vi også lansert en egen videoportal for informasjonssikkerhetsfilm, Secflix. Presseoppslag, podcaster, foredrag og andre eksterne kanaler er også svært viktig for oss. Dette gjelder særlig for å treffe dem som ikke kjenner til oss og dem som ikke opplever at vårt budskap er viktig for dem.

Hva kommuniserer vi?
Det er krevende å nå frem i dagens mediebilde. Vi opplever at vi lykkes best når vi spiller på følelser, humor, har med overraskelsesmomenter eller er gode historiefortellere. Vi tar og har rollen som eksperter i alt vi kommuniserer, men mener det ikke bør begrense vår mulighet til å by på oss selv og være så direkte som mulig. Tvert i mot mener vi at et klart, direkte og aktivt språk fungerer for å nå gjennom med vårt budskap.

Lykkes vi?
Evaluering en viktig del av vår kommunikasjonsstrategi. Vi bruker analyseverktøy for nettsider og sosiale medier og gjennomføringsgrad på kursene våre i tillegg til statistikk fra mediedekning og pressemeldingstjenesten, antall og type henvendelser inn til oss, antall foredrag og andre tilbakemeldinger for å analysere om vi når frem.

Alt i alt opplever vi at kommunikasjonen vår er godt mottatt. De siste 6 mnd ser vi at overgangen til mer video i kommunikasjonen har gitt oss bredere rekkevidde og mer engasjement og delinger, særlig i sosiale medier. Derfor satser vi på å videreutvikle dette fremover i tillegg til å videreutvikle innholdet vårt og hvordan vi sørger for å spre dette på tvers av kanalene våre. Vi brenner for å kommunisere enkelt, troverdig, relevant og engasjerende om sikkerhet og jobber hver dag for å bidra til en trygg digital hverdag for alle.

Om NorSIS

NorSIS (Norsk senter for informasjonssikring) er en ideell, ikke-kommersiell organisasjon, som er delvis finansiert av Justis- og beredskapsdepartementet. Vi jobber for en trygg digital hverdag for alle, gjennom veiledning og opplæring innen digital sikkerhet. Våre primære målgrupper er befolkningen og små- og mellomstore virksomheter.
Links: https//www.norsis.no

5. Det eksterne perspektiv

5.2 KOMMUNIKATION DER ÆNDRER ADFÆRD

AF TORBEN B. SØRENSEN,
SECURITY COMMUNICATION SPECIALIST, NETS A/S

Vidste du, at det er skadeligt at ryge?

Ja. Det ved du godt. Der er næppe nogen voksne mennesker i Danmark, der ikke er klar over rygningens skadelige virkninger på helbredet.

Alligevel er der fortsat rygere.

Hvorfor det? De ved det jo godt?

Eksemplet viser, at information sjældent er nok til at få os til at ændre adfærd. Vi har fået at vide, at vi gør noget, der er skadeligt for os. Men der skal mere end viden til, før vi holder op.

Informationssikkerhed består af et samspil mellem mennesker, processer og teknologi. Jeg arbejder med intern security awareness i Nets, så min opgave er at håndtere det menneskelige risikoelement.

Den menneskelige risiko

Den menneskelige risiko kan for eksempel bestå i, at en travl medarbejder klikker på et link i en e-mail. Linket fører til et phishing-websted, og pludselig er medarbejderens brugernavn og password i de forkerte hænder.

Vi informerer om risikoen ved phishing. Der er næppe mange af mine kolleger, der ikke er klar over risikoen. Alligevel viser vores test, at folk jævnligt falder i. Hvis man har travlt, kan man nemt overse faresignalerne i en phishing-mail – for eksempel at linket ikke fører til den adresse, som det ser ud til.

Jeg er oprindelig uddannet journalist. Som journalist informerer man læserne om det, man formoder, de er interesserede i. Men man arbejder ikke på at ændre deres adfærd. Jeg fortæller læserne, hvad jeg har fundet ud af om et emne, og så må de selv afgøre, hvad vil bruge det til.

Nye kompetencer

Da adfærdsændring ikke indgår i journalistuddannelsen, har jeg fået brug for nogle nye kompetencer i mit job. Kompetencer fra områder som markedsføring, psykologi og pædagogik.

Jeg har taget et kursus med tilhørende certificering i at oprette og drive et awareness-program – jeg kan i dag kalde mig SANS Security Awareness Professional (SSAP). På kurset beskæftigede vi os med, hvad der skal til for at ændre en adfærd.

For det første skal personen, der skal ændre adfærd, ønske at gøre det. Vedkommende skal være motiveret. For det andet skal personen være i stand til at ændre sin adfærd. Hvis viljen er der, men man ikke ved, hvad man skal gøre, bliver adfærden ikke ændret. Selv hvis begge elementer er til stede, ændrer personen ikke nødvendigvis adfærd. Der skal mere til. For eksempel må det gerne være sjovt at ændre adfærd. Og det skal helst være let.

Konkurrence om phishing

I Nets har vi arbejdet med en konkret adfærdsændring: Vi har indført en knap til rapportering af phishing-mails. Når medarbejderen modtager en mistænkelig e-mail, skal vedkommende klikke på en knap for at indrapportere den til vores sikkerhedsteam.

Det giver en fordel for os sikkerhedsfolk: Vi opdager det, når phishing slipper igennem vores filtre. For medarbejderen er der ingen umiddelbar fordel. Jo, sikkerheden i Nets bliver nok lidt bedre, men det mærker medarbejderen selv ikke meget til.

Derfor har vi gjort det let: Knappen sidder i mailprogrammet. Den er nem at få øje på og klikke på. Med ét klik har du rapporteret en mistænkelig e-mail. Desuden har vi gjort det sjovt: Vi har kombineret knappen med en konkurrence.

Konkurrencen går ud på, at medarbejderne jævnligt modtager simulerede phishing-mails. Hvis man gør det, skal man reagere, som om det var en rigtig phishing-mail: Klik på knappen.

Men i stedet for den normale rapporteringsmulighed får medarbejderen nu ros for at have genkendt potentiel phishing. Medarbejderen får tildelt to stjerner i konkurrencen – og mulighed for at vinde endnu en stjerne ved at gennemgå nogle få læringspunkter, der demonstrerer, hvordan man kan se, at mailen er mistænkelig.

5. Det eksterne perspektiv

Et leaderboard viser, hvordan medarbejderen klarer sig, og hvem der ligger øverst. Dermed konkurrerer man med sine kolleger om at blive bedst til at genkende phishing. Det kaldes gamification: Man gør en opgave til et spil.

Fordele ved gamification

Systemet har flere elementer, jeg godt kan lide:

- Tilgangen er positiv: du får ros for at udvise korrekt adfærd i stedet for at få ris for at gøre det forkerte.
- Det er let at forstå og benytte.
- Det udnytter vores glæde ved at lege og konkurrere.

Den positive tilgang går igen i alt vores awareness-arbejde i Nets. Vi har således udviklet et univers med sikkerheds-superhelte. Deres rolle er at optræde som medarbejdernes venlige hjælpere. De er ikke politifolk, der uddeler bøder, hver gang nogen har handlet uheldigt.

Superheltene har den yderligere fordel, at de giver informationssikkerhedsteamet et genkendeligt brand: Når medarbejderne ser en tegning af vores superhelte, forbinder de det straks med sikkerhed. Dermed behøver vi ikke at præsentere os hver gang, men kan gå lige til sagen.

Nets' sikkerhedsuperhelte ProtecThor og SecuRita bruges aktivt i kommunikationen

Ofte har sikkerhedsafdelingen ry for at være dem, der sætter hindringer i vejen. Her kan vi bruge awareness-arbejdet til at brande hele sikkerhedsafdelingen som noget, medarbejderne er positive overfor.

Grader af modenhed

På mit kursus lærte jeg også om de niveauer af modenhed, en organisation kan opnå inden for awareness-arbejdet.

Det laveste niveau er, at man ikke har noget program for awareness. Derefter kommer niveauet, hvor ydre krav tvinger organisationen til at gennemføre awareness-kurser. Det kaldes compliance-drevet awareness. På næste niveau bliver det mere spændende: Nu arbejder organisationen aktivt på at opnå opmærksomhed og ændre medarbejdernes adfærd.

Fjerde niveau handler om at indlejre sikkerhedstankegangen i organisationens kultur og få forandringerne til at holde. På det femte niveau styrer organisationen sit program ud fra konkrete målinger af, hvad medarbejderne gør, og hvor effektive awareness-tiltagene er.

I Nets er vi godt på vej op ad trappen, hvor vi fokuserer på kulturændringer.

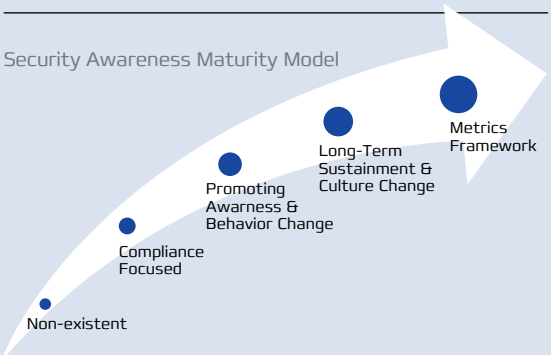
Kommunikation, pædagogik, markedsføring

For mig handler kommunikation om at formidle et budskab. Det er en del af processen her. Men når vi taler om at ændre adfærd, skal vi måske snarere kalde det pædagogik? Eller markedsføring?

Uanset hvad man kalder det, er min erfaring, at security awareness er nødt til at trække på viden fra et bredt felt: Pædagogik, psykologi, kommunikation og informationsvidenskab.

Det er nødvendigt, for at vores indsats mod den menneskelige risiko kan få succes. Når risikoen er menneskelig, er vi nødt til at forstå mennesker for at behandle den.

Figur 27: Organisationer kan bevæge sig op i awareness-modenhed via fem trin



Kilde: SANS Security Awareness

5. Det eksterne perspektiv

5.3 VÆRDIFULDT FOR DIG? VÆRDIFULDT FOR HACKEREN!

AF EVA ELISABETH ROLAND,
SPECIALKONSULENT, ERHVERVSSTYRELSEN

Hvordan kommunikerer man et budskab om digital sikkerhed, så danske virksomheder reagerer og handler? Hvordan bliver en konstant og voksende cybertrussel mod danske virksomheder nærværende uden at føre til handlingslammelse? Disse spørgsmål er omdrejningspunkt for Erhvervsstyrelsens arbejde med at styrke danske virksomheders digitale sikkerhed.

Hver dag rammes danske virksomheder af cyberangreb. Det kan have store omkostninger både for den enkelte virksomhed og på samfundsplan. Selv om danske virksomheder i stigende grad investerer i digital sikkerhed, er der fortsat stort potentiale for at blive bedre. Mange virksomheder mangler at få styr på helt grundlæggende tiltag. Eksempelvis opdaterer lidt over en fjerdedel af de små og mellemstore virksomheder ikke deres styresystemer eller tager backup af data. Begge dele øger sårbarheden, hvis uheldet er ude og en virksomhed lægges ned af et cyberangreb.

Så hvordan får vi budskabet om digital sikkerhed ud over rampen og rammer den brede og forskelligartede målgruppe lige der, hvor vi skaber forandring? Det gør vi ved at

- kende vores målgruppe
- undgå de løftede pegefingre
- signalere tydelig værdi for virksomhederne
- gå fra awareness til handling

Kend din målgruppe, som du kender dig selv
Det handler om at vide, hvor skoen trykker hos virksomhederne – med andre ord: hvis vi forstår, hvor barriererne for at få bedre styr på den digitale sikkerhed ligger, jo bedre er udgangspunktet for at udvikle de rette indsatser og skabe budskaber, som trigger både interesse og fører til handling. Vores udgangspunkt for både kampagner og udvikling af værktøjer og test er funderet i både kvantitativ og kvalitative indsigter om danske virksomheder. For it-sikkerhedsniveau og -behov er vidt forskellig hos det lille konsulenthus, frisøren og pengeinstituttet. En barriere for handling er fx en udbredt manglende risikooplevelse blandt især mindre danske virksomheder. En del virksomheder antager, at de ikke er et oplagt mål for it-kriminelle, fordi de ikke har informationer, der kan interessere andre, for 'vi ligger jo ikke inde med opskriften på Coca-Cola'. Men alle virksomheder er i besiddelse af systemer og data, der er vigtige for den daglige drift.

Et eksempel kan være håndværkeren, hvis system lammes af et ransomwareangreb, som betyder, at han mister sit kundekartotek og igangværende kontrakter, og ikke aner hvad han skal opkræve og af hvem. Hvis data er værdifulde for en virksomhed, kan det udnyttes af it-kriminelle. Det er et centralt budskab, som skal serveres på mange måder.

Ingen løftede pegefingre, men en hjælpende hånd i stedet
Det er afgørende for vores kommunikation til virksomhederne, at vi ikke løfter pegefingeren, men i stedet viser forståelse for, at it-sikkerhed ikke er øverst på virksomhedernes prioriteringsliste. For at nå virksomhederne med netop vores budskaber er det centralt, at virksomhederne kan spejle sig både i problemstillingen og løsningen.

I vores kampagne i den Nationale cybersikkerhedsmåned i oktober 2019 fortalte en række små og store danske virksomheder i en række casevideoer, hvordan deres oplevelse var, den dag virksomheden blev ramt af it-kriminalitet, og samtidig gav de deres dyrekøbte erfaringer og gode råd videre. Disse hverdagshistorier, som vækker genkendelse hos virksomhedsejeren, er med til at understrege budskabet om, at it-kriminalitet kan ramme alle typer virksomheder, men at der også er råd og hjælp at hente.

Sikkerdigital.dk

På sikkerdigital.dk kan borgere, virksomheder og myndigheder finde viden, vejledning og konkrete værktøjer til en sikker digital hverdag.

Bag sikkerdigital.dk står Digitaliseringsstyrelsen, Erhvervsstyrelsen og en række samarbejdspartnere.

5. Det eksterne perspektiv

Gode råd bør ikke være dyre, men handlingsrettede

En uhensigtsmæssig adfærd ændres ikke med den rette viden alene. Hvis virksomhedernes medarbejdere og ledere skal motiveres til reelt at skabe forandring, skal budskabet være relevant og handlingen, der helst skal følge, være overkommelig. Det skal være så nemt som muligt at gøre gode intentioner til virkelighed, når man som virksomhed er blevet mindet om, at it-sikkerheden måske halter nogle steder i virksomheden – fx hvis medarbejderne ikke kender de vigtigste måder at undgå at falde i en phishingfælde. Hvis vi skal lykkes med at få virksomhederne til at handle på de gode råd og stærke budskaber om styrket it-sikkerhed, handler det helt banalt om at gøre information og gode råd så handlingsparate, enkle og ikke mindst så målrettede som muligt.

Vi udvikler løbende værktøjer, som skal gøre det mere overskueligt at styrke sikkerheden, hvor det bedst giver mening for den enkelte virksomhed. For eksempel kan virksomhederne med sikkerhedstjekket.dk, en onlinetest udviklet af Erhvervsstyrelsen i samarbejde med Rådet for Digital Sikkerhed, teste deres it-sikkerhedsniveau og få et resultat med konkrete anbefalinger til, hvor de bør sætte ind for at styrke sikkerheden. Når de vigtigste områder udpeges for virksomhederne, bliver det nemmere at starte i det hjørne, som giver mest værdi. Opgaven skal være overkommelig for at kunne passes ind i en hverdag med mange andre prioriteter, retningslinjer fra myndigheder og krav og behov fra kunder og samarbejdspartnere. Ikke mindst i et år som 2020, der på mange måder har udfordret danske virksomheders robusthed.

It-risikovurderingsværktøj

Få hjælp til at identificere din virksomheds vigtigste it-systemer og vurdere forskellige risikoscenarier.

https://virksomhedsguiden.dk/risikovurderingsværktøj

Løbende indsats og awareness, awareness, awareness

Covid-19-pandemien, som ramte virksomheder hårdt i foråret 2020 og stadig sætter sine spor, viser tydeligt, hvordan cyberkriminelle til stadighed udnytter nye sårbarheder. Hackere udnytter den store interesse i coronarelaterede emner og udvikler phishingangreb med eksempelvis Sundhedsstyrelsen eller Erhvervsstyrelsen som afsender. De cyberkriminelles metoder udvikles og tilpasses løbende, og det kræver en vedvarende indsats både fra virksomhederne selv og fra myndigheder som Erhvervsstyrelsen, Digitaliseringsstyrelsen og Center for Cybersikkerhed at ruste danske virksomheder bedst muligt. Et godt sted at starte er sikkerdigital.dk, hvor Erhvervsstyrelsen og Digitaliseringsstyrelsen giver den hjælpende hånd og de handlingsrettede råd og værktøjer, som kan være med til at løfte den enkelte virksomheds - og dermed hele Danmarks - digitale sikkerhed.

5. Det eksterne perspektiv

5.4 DATATILSYNET: FEM MÅDER AT NÅ BÅDE ADVOKATEN OG FRISØREN

AF ANDERS DUE,
KOMMUNIKATIONSKONSULENT I DATATILSYNET

Retligt grundlag. Oplysningspligt. Indgåelse af databehandleraftaler. Dokumentation, samtykkeerklæringer, fortegnelser. De fleste kan nok godt finde på mere saftige emner end GDPR - eller databeskyttelsesforordningen, som jurister med forstand på området ynder at kalde det regelsæt, der de seneste år har gjort mange medarbejdere i myndigheder, virksomheder og organisationer trætte i blikket.

Pligt og frygt

Ud over, at området er tørt og svært tilgængeligt i manges øjne, er det heller ikke rigtig nyt; der har været regler på området siden 1979. Ikke desto har interessen for GDPR været overvældende. Tilbage i maj 2018, da reglerne fik virkning, var antallet af henvendelser fra selv landsdækkende aviser og tv så stort, at Datatilsynet et par gange måtte takke nej til at stille op.

Når Datatilsynet offentliggør en afgørelse, bliver den studeret nøje, diskuteret livligt og ofte også omtalt i pressen. Og mange virksomheder lever af at følge området tæt og rådgive andre om det evt. ved behov.

Årsagen er simpel. Konsekvensen af ikke at efterleve reglerne kan nu i yderste konsekvens være en bøde på op til 4 % af en virksomheds globale omsætning. Der er med andre ord hårdtslående argumenter for at sætte sig ind i reglerne - og selv om det handler om noget så vigtigt som retten til privatliv, tror jeg det ofte er af pligt, og måske også lidt af frygt, man læser op på lovgivningen.

Fem måder at gøre GDPR tilgængeligt

Da jeg startede som Datatilsynets første kommunikationsmedarbejder for tre år siden, fik jeg indtryk af, at fokus i tilsynet traditionelt havde været på, at informationen især skulle være korrekt, præcis og udtømmende. Det var ikke et problem, hvis man havde adgang til intern juridisk bistand, advokathjælp udefra eller bistand fra fx en brancheorganisation, men det kunne være uoverkommeligt for frisørerne, skakklubberne og de små selvstændige.

Og hvad har vi så gjort ved det? Intet revolutionerende, kan jeg roligt sige, men nogle helt basale kommunikationsfaglige taktikker:

1. Formidlingen skal være mere forståelig

Det kan godt være, det er mest korrekt at skrive 'forordningen finder anvendelse', men hvis ingen forstår, hvad det betyder, kan det i sidste ende være bedre at skrive 'reglerne gælder'. Jurister og kommunikationsfolk har det til fælles, at sproget virkelig betyder noget - vi er bare ikke altid enige om, hvad der er mest hensigtsmæssigt. Vi har set rigtig meget på, hvordan vi formulerer os - og øvelsen er som på så mange andre områder at finde balancen, hvor formidlingen både er korrekt og til at forstå. Her er nøglen selvfølgelig at holde fast i, hvilke forudsætninger modtageren har i den konkrete situation.

2. Informationen skal være tilgængelig på flere kanaler og i flere formater

Vi er forskellige som mennesker, vi finder vores information forskellige steder og forstår tingene bedst på forskellige måder. Derfor har vi i Datatilsynet forsøgt at stille de samme budskaber til rådighed i fx korte tekster, små animerede videoer, podcast - og selvfølgelig også lange juridiske vejledninger til specialisterne. Og så prioriterer vi

5. Det eksterne perspektiv

at dele informationen ikke bare på hjemmesiden, men også på relevante sociale medier, ligesom vi bruger kræfter på at være tilgængelige for pressen. Her har man mindre kontrol over formidlingen, men man når til gengæld ud til langt flere mennesker end i ens egne kanaler.

3. Kommunikationen skal gøres mere konkret
Det er banalt, men vigtigt: Langt de fleste mennesker har lettere ved at forstå noget nyt, hvis formidlingen veksler mellem det generelle og det konkrete. Et eksempel: Du skal have samtykke til at offentliggøre billeder af folk, hvis de med rimelighed kan føle sig udstillet eller krænket - du kan fx ikke dele billeder af mennesker hos lægen eller på et natklub uden at spørge om lov. GDPR er et meget generelt regelsæt, som beskriver nogle overordnede principper, der skal gøre sig gældende både nu og i alle mulige fremtidige hypotetiske situationer. Der er altså et indbygget underskud af konkret information, og derfor øver vi os i altid at give konkrete og nærværende eksempler, når vi formidler reglerne.

4. Vejledningen skal times nøje med juraen
Vi arbejder på at koordinere den håndfaste jura med relevant vejledning, så dem, der skal efterleve reglerne, bliver hjulpet godt videre. Sidste år afgjorde Datatilsynet en meget principiel sag om den måde, man indhenter samtykke til at behandle oplysninger om folk, der besøger ens hjemmeside. Da afgørelsen blev offentliggjort, var det i en samlet pakke med en overskuelig nyhedstekst, en helt ny vejledning med en masse konkrete eksempler og en ny podcast-episode, hvor vi talte om afgørelsen og dens betydning. Sådan skal vi gerne tænke, hver gang der kommer noget vigtigt nyt.

5. Vi skal ikke være bange for at vise, at vi er mennesker
Traditionelt har Datatilsynet været en myndighed uden et ansigt. Man har tilstræbt at vise en kompetent, uafhængig, grundig og upersonlig myndighed, og det har man haft held med på godt og ondt. Men de fleste af os kender følelsen af, at et rigtigt menneske i den anden ende gør noget svært lidt lettere at gå til. Et rigtigt menneske er lige, hvad man får i røret, hvis man ringer til os - men vi har også billeder på hjemmesiden, som vi selv har taget af medarbejdere på kontoret, i vores podcast gør vi en dyd ud af at få det til at lyde som en hyggesnak, selv når vi taler om dataansvarliges tilsyn med underdatabehandlere - og når vi deler indhold på LinkedIn, prøver vi at gøre det lidt uformelt, uden at det ligefrem bliver, som når den lokale slagter skriver på Facebook. Det sidste gælder fx, når vi i 'mandagsmyten' hver uge afliver en udbredt myte om GDPR.

Hvad nu?
De sidste tre år er antallet af følgere på LinkedIn steget fra ca. 300 til over 20.000. Mere end 80.000 gange er en af vores 20 podcast-episoder blevet afspillet, og en større interessentanalyse viste i 2020, at vores omverden opfatter os som noget mere åbne og tilgængelige end før.

Er vi så i mål? Langt fra. Men vi arbejder videre på at gøre det bedre, og i løbet af det sidste halve år er vi gået fra en enkelt medarbejder og en studerende til at være fire kommunikationsmedarbejdere. De nye kræfter skal vi især bruge på et endnu tættere samarbejde med juristerne i Datatilsynet - som også er blevet mere bevidste om kommunikation - så der er mere konkret og let forståelig vejledning i alt, hvad vi melder ud til vores mange målgrupper.

Selv om de fleste nok stadig synes, det er lidt tørt.

6. Trends og anbefalinger

2020 har repræsenteret en ny normal på cyberområdet. En normal, som har været forudset længe, men som først i kraft af pandemien er gået op for verdenssamfundet.

Med udgangspunkt i det aktuelle trusselsbillede giver DKCERT her et bud på cybertrends i 2021 og anbefalinger til hhv. ledelsen og de it-ansvarlige på uddannelses- og forskningsinstitutioner.

6.1 TRENDS 2021

1 Cybertruslen bliver mainstream

Forståelsen for alvoren af cybertruslen er blevet bredt længere ud. Det får aktørerne på denne dagsorden til at udvikle nye samarbejder, nye værktøjer og metoder til bekæmpelse af cyberkriminalitet og cyberspionage. Der bliver tilført flere midler til området, det vil tiltrække flere investeringer og flere aktører, der konkurrerer om at være med på dagsordenen.

Flere uddannelser, kurser og læringsplatforme vil se dagens lys og arbejdspladserne vil i højere grad tage opgaven om læring på sig. Det vil ske en specialisering og både bredden og dybden.

https://cert.dk/da/cert.dk/da/klumme/2020-02-03/en-ny-dreng-i-klassen
https://cert.dk/da/news/2020-10-05/Bliv-ambassadoer-for-cybersikkerhed
https://cert.dk/da/cert.dk/da/news/2020-03-02/kandidat-i-cybersikkerhed

2 Intensiteten i hjemmearbejde udfordrer sikkerheden

Trods udbredelse af vacciner mod coronavirus vil mange i den danske arbejdsstyrke fortsat arbejde hjemmefra, dog sandsynligvis i mindre omfang. Det øger risikoen for, at medarbejdere bliver ubevidste insidere, eftersom disciplinen om håndtering af informationer – hygiejnen – kan være dårligere på hjemmekontoret, end den er på arbejdspladsen. Også det høje niveau af onlinehandel vil udfordre sikkerheden – ikke kun for onlinebutikkerne, men også for de handlende, deres familier og arbejdspladser.

https://cert.dk/da/news/2020-12-17/COVID-19-udfordrer-sikkerheden-paa-hjemmearbejdspladserne
https://cert.dk/da/news/2020-16-03/Hjemmearbejde-i-en-Corona-tid

3 Phishingplagen fortsætter

Ifølge Center for Cybersikkerhed er phishing involveret i 80 pct. af alle cyberangreb, og 64 pct. af danskerne har inden for det seneste års tid været udsat for phishingforsøg. Phishing, vishing og smishing vil fortsætte og bruges både til at lokke fortrolige informationer ud af brugerne, give adgang til credentials og spredning af malware.

Phishingstrømmen vil følge nyhedsstrømmen. Menneskers higen efter verdensnyheder vil blive udnyttet til phishing. Nyheder om skovbrande i Brasilien, flygtningekatastrofe i krigshærgrede regioner eller optøjer i europæiske hovedstæder vil tiltrække sig en opmærksomhed, som kriminelle vil bruge til at sprede malware via phishing. Lige så vel som søgemaskineoptimering bruges til markedsføring af legitime produkter, bruges det til udbredelse af scam.

https://cert.dk/da/news/2020-12-03/Pas-paa-kort-om-Corona-virus
https://cert.dk/da/news/2020-10-08/Phishing-udnytter-Trumps-Covid-19-sygdom
https://cert.dk/da/news/2020-03-04/cfcs-hackere-forsoeger-at-udnytte-pandemien-til-egen-fordel
https://cert.dk/da/news/2020-16-03/mange-forsoeg-paa-phishing

6. Trends og anbefalinger

4 Specialisering af cyberdisciplinerne fortsætter

Hård konkurrence i kriminalitetsverdenen betyder, at specialiseringen af de forskellige cyberkriminalitetsdiscipliner intensiveres. Dem, der er gode til henholdsvis telefon-, sms- og mailphishing bliver dygtigere til deres arbejdsområde, og prisen sættes derefter. Andre bliver dygtigere til at finde og udnytte sårbarheder, sælge dem (eller få hjælp til det).

https://cert.dk/da/news/2020-10-29/Ny-trusselsvurdering-fra-CFCS-giver-indblik-i-cyberkriminelles-samarbejdsformer
https://cert.dk/da/news/2020-12-07/Ransomwaregrupper-bruger-callcentre
https://cert.dk/da/news/2020-08-18/Gaester-p%C3%A5-luksushotels-restaurant-udsat-for-avanceret-svindelforsoeg

5 Konkurrencen blandt cyberkriminelle intensiveres

Cyberkriminelle grupperinger opererer på markedsvilkår i hård konkurrence med hinanden. Grupper konkurrencer med hinanden om at være først med nye produkter, udvikler strategier og metoder, som i udpræget grad er genstand for kopiering. Visse grupper lukker deres aktiviteter, mens andre indleder strategiske samarbejder.

https://cert.dk/da/news/2020-06-04/Ransomwaregrupper-teamer-op
https://cert.dk/da/news/2020-09-21/Maze-kopierer-Ragnar-Locker
https://cert.dk/da/2020-05-13/Dobbelt-op-paa-ransomware
https://cert.dk/da/news/2020-04-04/Shade-ransomware-laegger-vaabnene

6 Store cyberangreb bliver større og længerevarende

Succes'en med kompromitteringen af SolarWinds til spredning af Sunburst-malwaren vha af opdateringer vil tiltrække flere trusselsaktører til at forsøge sig med samme metode, den såkaldte supply chain-attack.

https://cert.dk/da/news/2020-12-15/Saarbarhed-i-SolarWinds-brugt-i-angreb
https://cert.dk/da/news/2021-01-04/CISA-Opdater-eller-afmonter-Orion

7 Videnssektoren bliver i højere grad mål for cyberkriminelle

Coronopandemien har afdækket hvor vigtig en sektor, videnssektoren er for opretholdelse af et samfund. Det har gjort værdien af viden endnu højere; særligt vaccineviden har været efterspurgt, hvilket gør medicinalindustrien og institutioner inden for vaccineforskning udsat over for cybertruslen. Cyberspionagen øges, særligt med APT-aktører som initiativtagere.

https://cert.dk/da/news/2020-08-05/Aalborg-Universitet-udsat-for-kritisk-haendelse
https://cert.dk/da/news/2020-09-16/Stigning-i-DDoS-angreb-mod-universiteter
https://cert.dk/da/news/2020-11-02/Varsel-fra-Center-for-Cybersikkerhed-om-cyberangreb-mod-medicinalindustrien
https://cert.dk/da/news/2021-01-18/Manipulerede-vaccine-data-fra-EMA-offentliggjort

8 Ransomware

Ransomwareaktiviteter har gennemgået en voldsom udvikling inden for det seneste år. Fra at have krævet relativt høje kompetencer med kryptering af filer hos ofrene mhp betaling for frigivelse af data er det udviklet på mange fronter bl.a. ved gennemførelse af auktioner over gidseldata og eksfiltrering af følsomme eller fortrolige data, som angribere truer med at offentliggøre, hvis ofrene ikke betaler.

DDoS-angreb, hvor cyberkriminelle kræver sig betalt for at stoppe DDoS-angreb mod fx webshops ses også i vækst og et eksempel på, at cyberkriminelle fokuserer deres indsats mod steder, hvor der er høj aktivitet, og hvor der er mulighed for at indhøste nemme data. Ikke mindst må værdien af persondata formodes at være steget, dels fordi det i kraft af GDPR kan bruges i en afpresningssammenhæng, dels fordi persondata altid kan bruges i sammenhæng med phishingangreb, distribution af malware mm.

https://cert.dk/da/news/2020-11-30/Firedobling-af-DDOS-angreb
https://cert.dk/da/news/2020-08-24/DarkSide-en-ny-spiller-paa-ransomwaremarkedet
https://cert.dk/da/2020-06-03/Auktioner-om-gidseldata

6. Trends og anbefalinger

6.2 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.

1. 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.
2. Gør det tydeligt, at ledelsen er aktivt og løbende involveret i arbejdet med informationssikkerhed.
3. Afsæt ressourcer til uddannelse og kompetenceudvikling af alle medarbejdere i informationssikkerhed.
4. Sørg for løbende at adressere behovet for at efterleve retningslinjer for informationssikkerhed i organisationen, og monitorer efterlevelsen. Det er ikke nok, at medarbejderne undervises.
5. Overvej evt. disciplinære forholdsregler og mulige konsekvenser ved overtrædelse af sikkerhedspolitikken og -retningslinjerne.
6. Understøt en kultur, hvor risiko og sikkerhed er tænkt ind fra starten i udviklingen af produkter og tjenester.
7. Sørg for, at der er ressourcer til, at der kan føres tilsyn med overholdelse af databeskyttelsesforordningen.
8. Hold de ansatte, studerende og gæster informeret om informationssikkerhedspolitikken og aktuelle problemer.
9. Etabler et beredskab, udarbejd en beredskabsplan for kritiske hændelser og gennemfør øvelser med jævne mellemrum.
10. Prioriter og synliggør risikostyring.
11. Foretag løbende risikovurderinger af forretningskritiske systemer – også ved hændelser, der rammer lignende institutioner.
12. Arbejd sammen med andre institutioner om informationssikkerhed, del viden og erfaringer.
13. Afsæt tid, penge og personale til håndtering af informationssikkerhed.
14. Understøt en kultur, hvor dialog om informationssikkerhed er en del af sikkerhedsarbejdet.

6. Trends og anbefalinger

6.3 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.

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

7. Ordliste

7. Ordliste

A

A

Awareness-kampagner:
Tiltag eller aktiviteter, der skaber opmærksomhed og påvirker ansattes, studerendes eller borgeres viden og adfærd i forhold til informationssikkerhed.

B

Botnet:
Et botnet er et netværk af computere, som en angriber kan fjernstyre fra centralt hold. Navnet kommer af 'robot' og 'net'. Ejerne af computerne ved ikke, at deres maskine er inficeret og indgår i botnettet. Angriberen udnytter gerne sine 'robotter' til at foretage koordinerede denial of service-angreb eller udsende spam- og phishing-mails.

Brute force:
Dækker i datalogien over en udtømmende afsøgning af et løsningsrum. Inden for informationssikkerheden betegner det afprøvningen af kombinationer af brugernavne og kodeord, ofte ud fra foruddefinerede lister og ordbøger.

C

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.

Credential stuffing
I credential stuffing-angreb bruger aktører oplysninger fra tidligere databrud til at forsøge at logge ind på forskellige loginsider. Typisk anvendes lister med brugernavne og / eller e-mail-adresser og deres korresponderende adgangskoder til at få uautoriseret adgang til brugerkonti. Det sker gennem automatiserede loginanmodninger mod en webapplikation. Angriberne bruger således ikke brute force til at gætte adgangskoderne, men oplysninger der har været anvendt af brugere til login, evt. i andre sammenhænge.

Cross-site scripting (XSS):
En sårbarhed på et websted, der gør det muligt at afvikle scriptkode i browseren hos en bruger, der besøger det. Der er forskellige former for cross-site scripting, som gør det muligt at udføre komplekse angreb. Metoden kan for eksempel anvendes til phishing, hvor brugeren bliver omdirigeret til et forfalsket website. En angriber kan udnytte et website, som en bruger har tillid til, til at få adgang til fortrolig information.

CVE, CVE-nummer:
Common Vulnerabilities and Exposures (CVE) indgår i National Vulnerability Database, der er en liste over offentligt kendte sårbarheder i software. Listen dækker sårbarheder i de fleste kendte og alment udbredte programmer, men ikke i skræddersyet eller internt udviklet software.

CWE:
Common weakness enumeration er en liste med software- og hardware- sårbarhedstyper. CWE™ fungerer som et fælles sprog, en målestok for sikkerhedsværktøjer, og en baseline til at identificere sårbarheder mhp. afhjælpning og forebyggelse.

D

DDoS-angreb:
Et distribueret Denial of Service-angreb (se dette), hvor mange computere på samme tid angriber offeret.

DeiC:
Danish e-Infrastructure Cooperation blev dannet i april 2012. DeiC har til formål at understøtte udviklingen af Danmark som eScience nation gennem levering af e-infrastruktur (computing, datalagring, netforbindelser og understøttende tjenester), vejledning og initiativer på nationalt niveau. DeiC er en virtuel enhed under Uddannelses- og Forskningsministeriet og resultatet af en aftale indgået mellem de otte universiteter og Styrelsen for Forskning og Uddannelse. DKCERT er en del af DeiC. Se også www.deic.dk

Denial of Service (DoS):
Et angreb, der sætter en tjeneste, funktion eller et system ud af drift eller på anden måde gør det utilgængeligt for brugerne. Et eksempel kan være et angreb, der overbelaster en webserver ved at sende mange forespørgsler. Disse angreb udføres ofte fra flere computere samtidig. Det kaldes distributed denial of service (DDoS).

Direktørsvindel:
(også kaldet CEO-fraud) Falske e-mails eller sms'er ofte sendt til regnskabsafdelingen, der angiver at komme fra en ledende medarbejder, der beder modtageren hurtigt gennemføre en pengeoverførsel til udlandet.

7. Ordliste

Drive-by attacks, drive-by download:
Angreb, hvor tilfældige besøgende på en kompromitteret hjemmeside forsøges inficeret med skadelige programmer. Den inficerede hjemmeside vil ofte være en sårbar legal side, som brugeren har tillid til, og infektionen foregår uden dennes vidende. Infektionen udnytter som regel sårbarheder i programmer på brugerens pc, ofte browseren eller udvidelser som Flash og Java.

E **Exploit:**
Et angrebsprogram, som forsøger at udnytte sårbarheder i software med det formål at kompromittere systemet.

Exploit kit:
Software, der placeres på et website og afsøger de besøgendes computer for sårbarheder i browseren og tilhørende programmer. Er computeren sårbar, kompromitteres den med et af programmets exploits. Indeholder ofte også funktioner til opdatering, statistik med mere.

F **Forskningsnettet:**
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.

G **GDPR (General Data Protection Regulation):**
Databeskyttelsesforordning, vedtaget af EU-parlamentet og medlemsstaternes regeringer. Trådte i kraft maj 2018. Forordningen stiller krav til beskyttelsen af persondata.

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.

H **Hacker:**
På dansk betyder hacker en person, der uden foregående tilladelse forsøger at kompromittere computersystemers sikkerhed. Inden for it-kredse betyder det blot en person, der finder ud af, hvordan en ting fungerer. På engelsk kan man skelne mellem en hacker og en cracker eller whitehat hackere og blackhat hackere, afhængigt af om aktivitetens formål er at forbedre kode og/eller sikkerhed, eller det er at udføre it-kriminalitet.

Hacktivisme:
Politisk motiveret hacking. Ordet er en sammentrækning af 'hack' og 'aktivisme'. Det dækker forfølgelse af politiske mål ved hjælp af midler som defacement, DDoS-angreb, informationstyveri og lignende.

I **Identitetstyveri:**
Brug af personlige informationer til misbrug af en andens identitet. Det modsvares i den juridiske terminologi af dokumentfalsk og bedrageri. Personlige informationer indsamles og misbruges ved phishing, hacking eller infektion med trojanske heste. Informationerne kan fx være kreditkortinformationer, personnumre eller adgangsoplysninger til mailkonti, internetbutikker, sociale netværkssider, onlinespil og lignende.

Internet of Things (IoT):
Enheder på internettet, der ikke er traditionelle computere. Det kan fx være termostater, udstyr til industriel automatisering, overvågningskameraer og videooptagere.

ISO/IEC 27001:
En normativ standard for informationssikkerhed. Den beskriver kravene til et ledelsessystem for informationssikkerhed.

ISO/IEC 27005:
En vejledning i risikovurdering og risikostyring.

ISO/IEC 27701:
Et tillæg til ISO/IEC 27001, der udvider kravene i forhold til beskyttelse af persondata.

M **Malware:**
Skadelig software. Ordet er en sammentrækning af 'malicious software'. Malware er en samlebetegnelse for virus, orme, trojanske heste, keyloggere, spyware, adware, botnetprogrammer og lignende.

N **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.

O **Orm:**
Et program, der spreder sig i netværk ved at udnytte sårbarheder i dets computere. I TCP/IP-verdenen sker det typisk ved, at ormeprogrammet kontakter den port, som det sårbare program lytter på.

7. Ordliste

P **Phishing:**
Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på phishing optræder ofte i e-mails, der henviser til websider med fx kriminelle hensigter. Websiden angiver at tilhøre offerets bank, kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol. Findes også som sms-phishing (såkaldt smishing), hvor et link i sms'en fører til websiden.

R **Ransomware:**
Sammentrækning af ordene 'ransom' (løsesum) og 'malware'. Skadelig software, der tager data som gidsel, ofte ved kryptering.

S **Scanning, portscanning:**
Kortlægning af åbne porte på internettet, der har til formål at identificere sårbare services knyttet til dem. En portscanning foregår typisk ved, at der forespørges efter mange porte på få maskiner, eller én port på mange maskiner. Oftest benyttes et program til at foretage portscanninger.

Single sign-on:
Mulighed for at logge ind på flere systemer ved kun at angive et enkelt brugernavn og password.

Social engineering:
Manipulation, der har til formål at få folk til at afgive fortrolig information eller udføre handlinger som fx at klikke på links, svare på mails eller installere malware.

Spam:
Uopfordrede massedistribuerede reklamemails med henblik på salg af produkter eller services.

Spear phishing:
Svindelmails målrettet til bestemte personer i organisationen. Mailen vil ofte indeholde information, der får den til at se troværdig ud, fx navne på kolleger og afdelinger.

SQLinjection:
Et angreb, der sender kommandoer til den bagvedliggende SQL-database (eller det bagvedliggende styresystem) gennem usikre input-felter på websiden, som for eksempel søgefelter eller kommentarfelter, eller gennem usikre parametre i websidens URL'er. Formålet med SQL-injection er oftest at opnå kontrol over en maskine.

Sårbarhed:
En fejl i et it-system, som en angriber kan udnytte til at få adgang til systemet, forhindre det i at fungere eller på anden måde misbruge det.

Sårbarhedsscanning:
Kortlægning af kendte sårbarheder knyttet til services på et systems åbne porte. Benyttes ofte efter foregående scanning.

T **To-faktor-autentifikation:**
Autentifikation, der rummer to uafhængige faktorer, som brugeren skal angive for at få adgang. Det kan være en RFID- eller USB-nøgle, en engangskode, der sendes til brugerens mobiltelefon, et fingeraftryk, der angives via en fingeraftrykslæser, en kode fra et papirkort eller det gammelkendte brugerid/password.

Trojansk hest:
Et program, der har andre funktioner end dem, som det foregiver at have. Trojanske heste indeholder malware, som aktiveres på den ramte computer.

Trojaniseret version:
En version af et ellers legitimt softwareprogram, der i forbindelse med en opdatering indeholder funktioner som en trojansk hest.

V **Virus:**
Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres virussen, og den inficerer andre programfiler. Oprindelig kunne kun egentlige programmer indeholde virus, men dokumenter med makroer kan også gøre det.

W **Websårbarheder:**
En sårbarhed på en webapplikation, eller et tilknyttet system, som kan udnyttes gennem webapplikationen.

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