DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed

DKCERT Trendrapport 2020

Redaktion: Henrik Larsen og Nicolai Devantier, DeiC.

Tak til vore øvrige bidragydere:

Thomas Kristmar, Senior Manager KPMG og medlem af Fagrådet for informationssikkerhed i Dansk IT.

Alf Moens, Corporate Security Officer, SURFnet.

Frederik Helweg-Larsen, Expert Director, Devoteam.

Thomas Lund-Sørensen, Chef for Center for Cybersikkerhed.

Jan Kaastrup, chief technology officer, CSIS Security.

Simon Nexø Jensen, DKCERT.

Johnson Akpotor Scott, DKCERT.

Morten Eeg Ejrnæs Nielsen, DKCERT.

Eskil Sørensen, DKCERT.

Design og layout: Kiberg & Gormsen

DeiC-journalnummer: DeiC-JS 2020-01

DKCERT - en del af DeiC

DTU, Asmussens Allé, Bygn. 305

2800 Kgs. Lyngby

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 DKCERT's 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.

På denne baggrund udvikler DKCERT services, der skaber merværdi for institutionerne på forskningsnettet og sætter dem i stand til bedre at sikre deres it-systemer.

DKCERT er en del af DeiC, Danish e-Infrastructure Cooperation. DeiC understøtter Danmark som e-science-nation gennem levering af e-infrastruktur (computing, datalagring og netværk) til forskning og forskningsbaseret undervisning. DeiC er en enhed under Uddannelses- og Forskningsministeriet, etableret ved aktstykke 70 af 19. april 2012.

DKCERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om informationssikkerhed med grundidé i CERT/CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DKCERT om informationssikkerhed i uddannelsessektoren i Danmark. DKCERT er fuldt medlem af FIRST (Forum of Incident Response and Security Teams) samt akkrediteret medlem af Trusted Introducer og TF-CSIRT (Task Force Computer Security Incident Response Team) under GÉANT.

Indholdsfortegnelse

1. Velkomst

Velkommen til DKCERT's Trendrapport 2020.

I år har vi valgt krisehåndtering som omdrejningspunkt for rapporten. Ikke mindst fordi 2019 bød på et par rigtigt grimme cyberangreb, hvor kriseberedskabet hos eksempelvis Norsk Hydro og Demant blev sat på en alvorlig prøve.

Endnu har vi ikke set store angreb med ransomware mod danske universiteter, men i slutningen af 2019 blev universiteter i Holland, Belgien og Tyskland ramt. Og cyberkriminalitet kender ingen landegrænser.

I marts 2019 blev Norsk Hydro og virksomhedens datterselskab i Jylland ramt af et angreb, der tvang virksomheden til at gå i manuel drift for en periode. Senere på året var det så høreapparatfirmaet Demant, som meddelte, at der var udfordringer med ransomware i virksomhedens netværk. En episode, som kostede Demant et trecifret millionbeløb. Måske kan du også huske lidt længere tilbage, hvor Mærsk-koncernens it-systemer kom under belejring af NotPetya-malware-angrebet. En krise, der varede i ni dage og kostede op mod to milliarder kroner.

Så galt kommer det forhåbentlig ikke til at gå i din organisation, men kriser kommer, og derfor skal du være forberedt på dem, have kommunikeret og øvet det planlagte kriseberedskab, så alle ved, hvad der skal gøres.

De tre alvorlige episoder, der er beskrevet ovenfor, er eksempler på, at uheldet kan ramme alle, og at alle er nødt til at have kriseberedskabet i orden - for når uvejret bryder løs, bedømmes man på sin forberedelse.

I DKCERT deltager vi jævnligt i kriseøvelser, og vi arbejder på at kunne tilbyde både uddannelse og rådgivning til de institutioner, der er tilknyttet forskningsnettet, hvor vi holder øje med sikkerheden. Det bliver således et af de områder, som vi vil have skarpt fokus på i 2020, så vi kan bidrage til det forberedende arbejde.

Selv om kriseøvelser er fiktive og udtænkt bag et skrivebord, så er det rigtig god træning i at være klar til at håndtere det unormale og i visse tilfælde det ekstreme. Hvis du er godt forberedt og har øvet din plan, så kan du også nemmere improvisere og tilpasse dig situationen. Det er det, der skal til for at vinde slaget, hvilket vi gerne bidrager til i DKCERT.

Et andet tiltag, som vi er stolte af, er udarbejdelsen af en trusselsvurdering for universitetssektoren. Her foretages en vurdering af troværdigheden og alvoren af en potentiel trussel såvel som sandsynligheden for, at truslen bliver en realitet. Selve trusselsvurderingen kan du finde sidst i rapporten.

I Trendrapport 2020 kan du naturligvis også finde statistikker fra DKCERT's sikkerhedsanalytikere om forskningsnettet. Samtidig har vi fornøjelsen af at kunne give et bredere perspektiv om krisehåndtering gennem indlæg fra eksterne skribenter.

Sidst, men ikke mindst, er Telesektorens Decentrale Cyber- og Informationssikkerhedsenhed flyttet ind hos DKCERT i 2019, hvilket er til gavn for teleselskaberne og samtidig bibringer værdi til DeiCs medlemmer.

God fornøjelse med læsningen!

Henrik Larsen
Chef for DKCERT

2. Resumé

DKCERT har som noget nyt udarbejdet en Trusselsvurdering for uddannelses- og forskningssektoren, og telesektorens Decentrale Cyber- og Informationssikkerhedsenhed er blevet en del af DKCERT. Awareness, phishing, ransomware og lækager står stadig øverst på sikkerhedsdagsordenen.

DKCERT informerer løbende om aktuelle trusler, sårbarheder og sikkerhedshændelser på web via fem ugentlige nyhedsbreve og via Twitter. I 2019 blev der udgivet 289 artikler omhandlende informationssikkerhed på cert.dk. Antallet af unikke sidevisninger var 78.976.

Twitter bliver en stadig mere populær kanal til information om informationssikkerhed, hvilket også kan læses i antallet af følgere. 2.841 fulgte således DKCERT på Twitter ved udgangen af 2019. I 2018 var tallet på 2.439, hvilket er en stigning på 402 følgere eller mere end 16 procent.

DKCERT registrerede 4.081 sikkerhedshændelser på forskningsnettet i 2019. Det udmøntede sig i 1.426 rapporter (Incident Reports) og herudfra 57 sager, der har gennemgået en nærmere efterforskning.

I 2019 registrerede USA's National Vulnerability Database 18.938 indberetninger om sårbarheder, hvilket svarer til 1.578 pr. måned. Knap 7 procent af sårbarhederne blev vurderet til lav risiko, 67 procent til middel og i den højeste risiko findes 26 procent af årets sårbarheder.

I 2019 har DKCERT gennemført 52 scanninger for medlemsinstitutionerne på forskningsnettet. Der blev desuden udsendt 37.308 advarsler fra tredjeparter til forskningsnettets medlemmer.

Som noget helt nyt har DKCERT i 2019 udarbejdet en Trusselsvurdering for uddannelses- og forskningssektoren, og så er telesektorens Decentrale Cyber- og Informationssikkerhedsenhed (DCIS) blevet en del af DKCERT.

2.1. TENDENSER FRA ÅRET DER GIK

Uddannelse af brugere på alle niveauer er en af nøglerne til forbedret informationssikkerhed i Danmark.

Danmarks deltagelse i den europæiske cybersikkerhedsmåned satte eksempelvis fokus på cyber- og informationssikkerhed i hele oktober ved at støtte projekter og afholde aktiviteter, der var med til at løfte danskernes viden om, hvordan de digitalt beskytter sig selv og deres informationer.

Men det er langt fra den eneste begivenhed på området. Der er udgivet undervisningsmateriale til både unge og uddannelsesinstitutioner, til bestyrelser og til offentligt ansatte. Ligeledes er der sat fokus på konkrete områder som dataetik, industrielle kontrolsystemer og Internet of Things, hvilket er en meget positiv tendens.

Phishing er stadig en af de mest effektive metoder til at begå it-kriminalitet, og i den forbindelse har 2019 ikke været noget undtagelse. Phishing som fænomen er i støt stigning, hvilket de fleste nok også har bemærket i form af indbakker, sociale medier og telefoner, der bugner med falske beskeder. På telefonen kalder vi det "smishing" (SMS) eller "vishing" (voice).

Ransomware – digital afpresning – er ofte relateret til phishing, og i 2019 har eksempelvis angrebet mod høreapparatfirmaet Demant brændt sig ind i hukommelsen.

Der er flest penge at tjene for de it-kriminelle med virksomheder som deres ofre, men ransomware er absolut også en udfordring blandt almindelige brugere. Ligeledes har dette været et globalt fænomen i 2019.

Danskere, der rammes af onlinesvindel eller anden form for digital kriminalitet, er en bekymring i e-handelssamfundet, og fupbutikker har gennem det forgangne år været et område i kraftig stigning.

I 2019 har e-mærket spottet hele 150.000 webshops, som er det rene fup. I 2018 blev der ifølge sikkerdigital.dk spottet 10.000.

I maj 2018 kom den nationale strategi for cyber- og informationssikkerhed (temaet for sidste års Trendrapport). I 2019 blev regeringen også klar med planerne for den kritiske infrastruktur til beskyttelse mod cyberangreb inden for seks samfundskritiske sektorer. Herunder teleindustriens DCIS, der er en del af DKCERT.

2019 har desværre været endnu et år med enorme datalæk. Mest bemærkelsesværdigt var en enkelt episode, hvor personlige oplysninger om potentielt 1,2 milliarder mennesker blev offentliggjort i forbindelse med en massiv datalækage. Universiteterne var i den forbindelse også berørt.

Sikkerhedsproblemer i forbindelse med indholdsstyringssystemer, eller CMS, har ligeledes været et område, som 2019 har været plaget af.

2. Resumé

2.2. TENDENSER I 2020

Temaet for årets Trendrapport er krisehåndtering, og når angrebet eller nedbruddet kommer, er det vigtigste punkt på dagsorden at få forretningsdriften op at køre hurtigst mulig, så de negative konsekvenser holdes på et minimum.

Nedetid koster nemlig både på bundlinjen og på goodwill-kontoen, hvilket der er flere eksempler på fra 2019. Og de erfaringer vil stadig være på dagsordenen i 2020.

Selv om det amerikanske præsidentvalg foregår på et helt andet kontinent, kan det – set i lyset af sidste valg – komme til at betyde, at nettet vil blive ramt af bølger af falske informationer og uægte/beskidte data.

Der er i denne forbindelse risiko for, at datasæt og nyhedshistorier er unøjagtige, partiske eller direkte forkerte. Da datadreven beslutningstagning fra kunstig intelligens og algoritmer bliver mere og mere udbredt, vil der i 2020 komme et øget behov for (offentlig) kontrol af udgivelsesplatformene. Phishing, ransomware og malware udnyttes med ønske om økonomisk vinding ud fra politiske motiver og i forbindelse med destruktive angreb – eller i en kombination af disse elementer. Angrebsmetoderne er ikke nye, men de er fortsat et af de øverste punkter på dagsordenen i 2020.

Vi står på tærsklen til udrulningen af 5G i Danmark, og sikkerheden i den kommende teknologi er et yderst vigtigt område. Truslerne fra ondsindede personer, organisationer eller stater kan blive høj, da angrebsfladen vil blive mange gange større, når 5G kan anvendes til at forsyne 'alt' med internet.

Angreb mod forsyningsselskaber og kritisk infrastruktur er fortsat et oplagt offer for cyberangreb. Tendensen underbygges af trusselsvurderingerne fra de samfundskritiske sektorer og Center for Cybersikkerheds samlede trusselsvurdering. DKCERT har i 2019 udarbejdet en trusselsvurdering for universitetssektoren, der ligeledes bekræfter dette billede.

2. Resumé

2.3. TRUSSELSVURDERING FOR UDDANNELSES- OG FORSKNINGSSEKTOREN

For første gang indeholder denne trendrapport en trusselsvurdering for uddannelses- og forskningssektoren. Trusselsvurderingen er udarbejdet efter samme metode som trusselsvurderingerne fra Center for Cybersikkerhed og har til formål at hjælpe institutionerne med at kende og forstå deres modstandere i cyberspace, så de bedre kan vurdere den risiko, som aktørerne udgør, og så de bedre kan forsvare sig mod dem.

Hovedkonklusionerne er følgende:

- 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 muligt, 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 awareness vedrørende truslen og konsekvenserne heraf, hvilket øger sandsynligheden for menneskelige fejl, uanset om disse er bevidste eller ubevidste.

Når det er vigtigt at have en selvstændig trusselsvurdering for universitetssektoren skyldes det, at sektoren arbejder med data, der er væsentlig anderledes end de andre kritiske sektorer, finans, tele, sundhed, energi, transport og søfart. Af den grund er formålene med angreb fra fx statssponserede aktører forskellige, og derfor ses også forskellige angrebsmønstre. Af samme grund skal de forebyggende tiltag også igangsættes ud fra en anden tilgang, som tager højde for de driftsmæssige og kulturelle forskelle.

Trusselsvurderingen for universiteterne kan læses i sin helhed i kapitel 9.

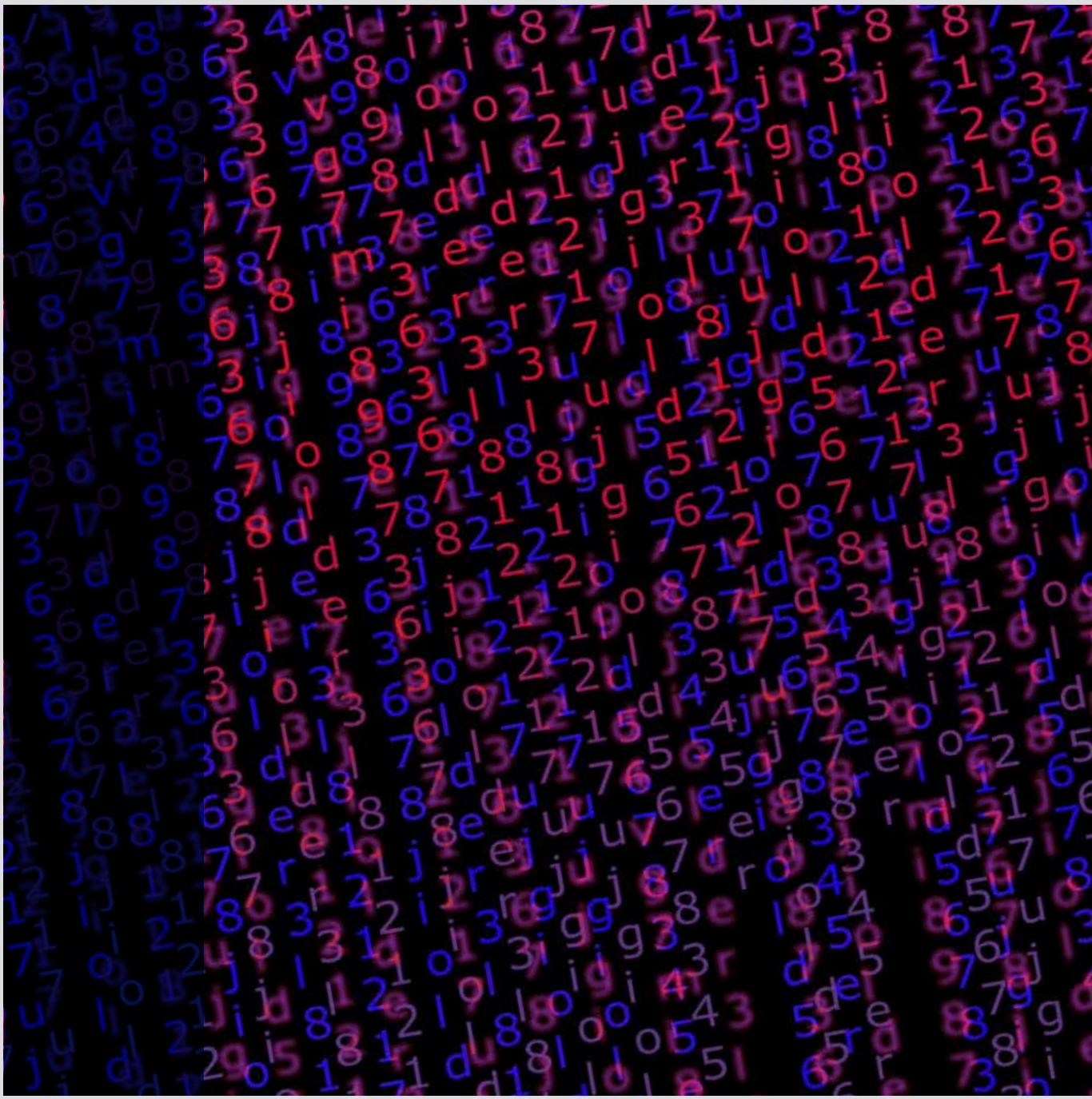
2. Resumé

3. 2019 – året i tal

DKCERT behandlede 4.081 sikkerhedshændelser og har herudfra efterforsket 57 sager i 2019.

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

DKCERT svarer på henvendelsen, sorterer, analyserer og sender henvendelsen videre til den institution, der anvender den pågældende IP-adresse.



3. 2019 – året i tal

3.1. ÅRETS SIKKERHEDSHÆNDELSER

DKCERT behandlede 4.081 sikkerhedshændelser på forskningsnettet i 2019 (se Figur 1), hvilket er en smule mere end sidste år, hvor antallet var på 3.782 sikkerhedshændelser.

Det lyder måske af mange, men angreb finder i højere og højere grad sted på andre niveauer end netværkslaget, hvor disse tal stammer fra. Derfor er det ikke organisationer som DKCERT, der hører om dem. Det er således ikke alle angreb, der anmeldes direkte til DKCERT som en sikkerhedshændelse. Et eksempel på det er ransomware-angreb.

Tallet omfatter heller ikke advarsler fra tredjeparter om sårbare systemer, da de ikke er egentlige sikkerhedshændelser. Tredjepartstallene behandles i et selvstændigt afsnit senere i rapporten.

Puljen af de 4.081 registreringer filtreres for trivielle sikkerhedshændelser, som eksempelvis spammail, der ikke udgør en risiko i denne sammenhæng og derfor ikke bliver undersøgt i dybden.

De tilbageværende og mere alvorlige sager kræver nærmere analyse og indsamling af flere oplysninger fra eksempelvis angrebsramte institutioner for en nærmere gennemgang og vurdering. DKCERT har bearbejdet 1.426 rapporter (Incident Reports) og herudfra efterforsket 57 sager i 2019 (se Figur 2).

Sagerne har typisk handlet om inficerede systemer på forskningsnettet.

DKCERT opdeler sikkerhedshændelserne i forskellige kategorier. Her gennemgår vi eksempler på de mest fremtrædende typer af sager.

Portscanninger var nummer et på listen over de hyppigste sagstyper i 2019. En portscanning går ud på, at man undersøger, om en computer på et netværk svarer på henvendelser. I sig selv udgør en portscanning ikke et angreb, men den kan være en del af rekognosceringen, der foregår op til et angreb.

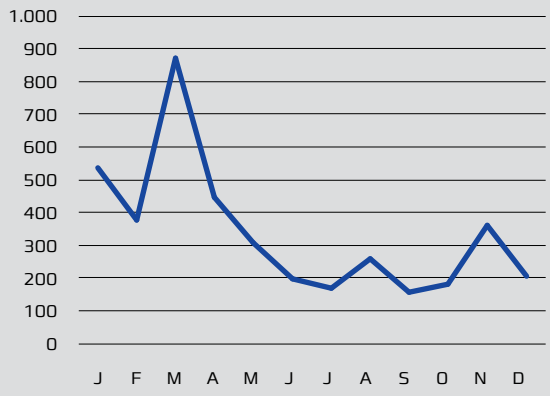
Sager om spam er ligeledes en hyppig sagstype. DKCERT tager sig ikke af klager fra folk, der har modtaget spam. Sagerne handler i dette tilfælde om servere, der misbruges til udsendelse af spam.

Et tredje område er uautoriseret adgang, som opdeles i tre undertyper: Kompromitterede systemer, angrebsforsøg og systemer, der potentielt kan overtages, fordi de er sårbare. Hele kategorien dækker over hændelser, hvor uvedkommende har forsøgt at få adgang til ressourcer, vedkommende ikke har ret til at tilgå.

Desuden har DKCERT behandlet sager om eksempelvis phishing og henvendelser fra politi/myndigheder.

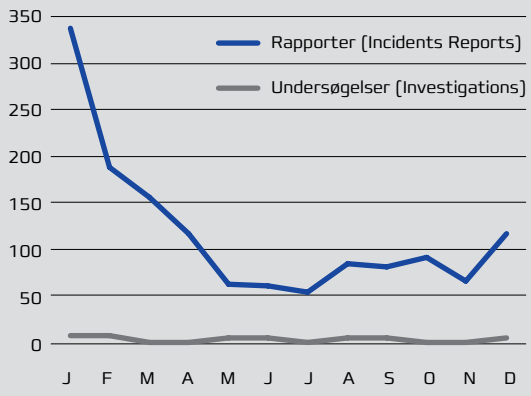
Figur 1: Sikkerhedshændelser pr. måned

Sikkerhedshændelser behandlet af DKCERT i løbet af 2019.



Figur 2: Rapporter og undersøgelser

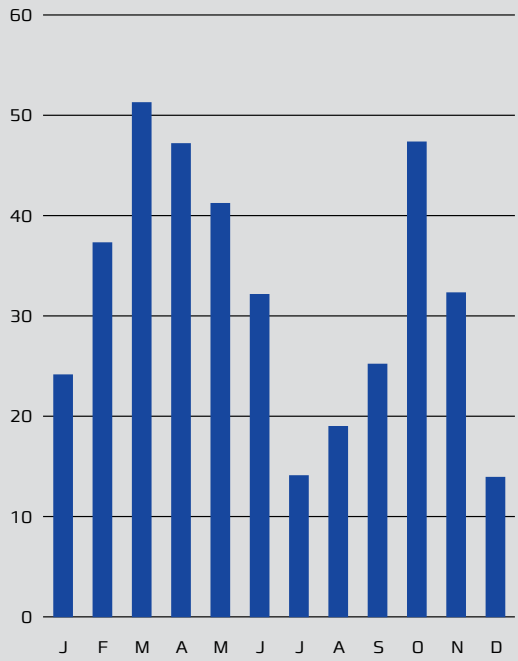
Efter filtrering af de trivielle sikkerhedshændelser, som eksempelvis spam, har DKCERT udarbejdet følgende rapporter og undersøgelser i 2019.



3. 2019 – året i tal

Figur 3: Emotet-infektioner

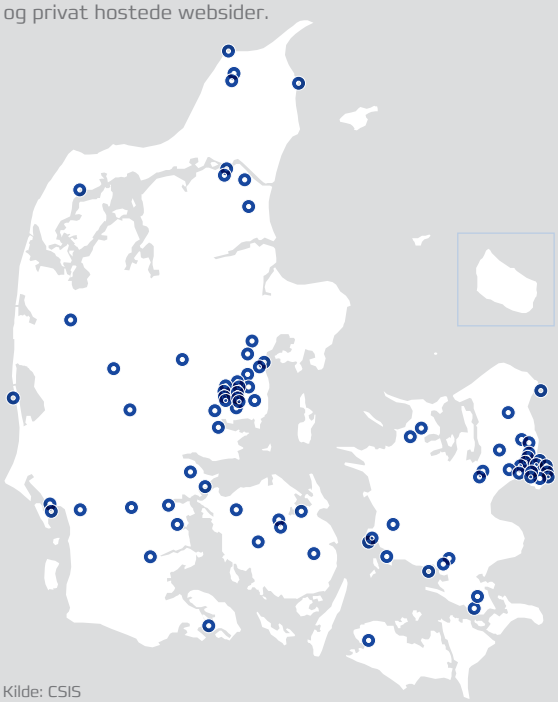
Emotet-infektioner på danske websider i 2019.



Kilde: CSIS

Figur 4: Observerede Emotet-Infektioner

Danmarkskortet viser, hvor Emotet-infektioner er observeret. Det er en skøn blanding mellem hosting-selskaber og privat hostede websider.



Kilde: CSIS

3.2. MALWARE OG PHISHING I DANMARK

Noget af det mest udbredte og skadelige malware er Emotet, Trickbot og Ryuk.

Emotet er en såkaldt trojansk hest, der anvendes til at indsamle oplysninger fra den inficerede maskine. Emotets infrastruktur er vokset enormt og er distribueret i hele verden, heriblandt Danmark. Malwaren spredes typisk via spearphishing emails. Bliver en maskine inficeret, kan malwaren spredes til andre maskiner. Over de senere år har Emotet specialiseret sig i at inficere virksomheder og sælge adgangen videre til bl.a. gruppen bag Trickbot. ISS og Demant er eksempler på danske virksomheder, der netop oplevede dette.

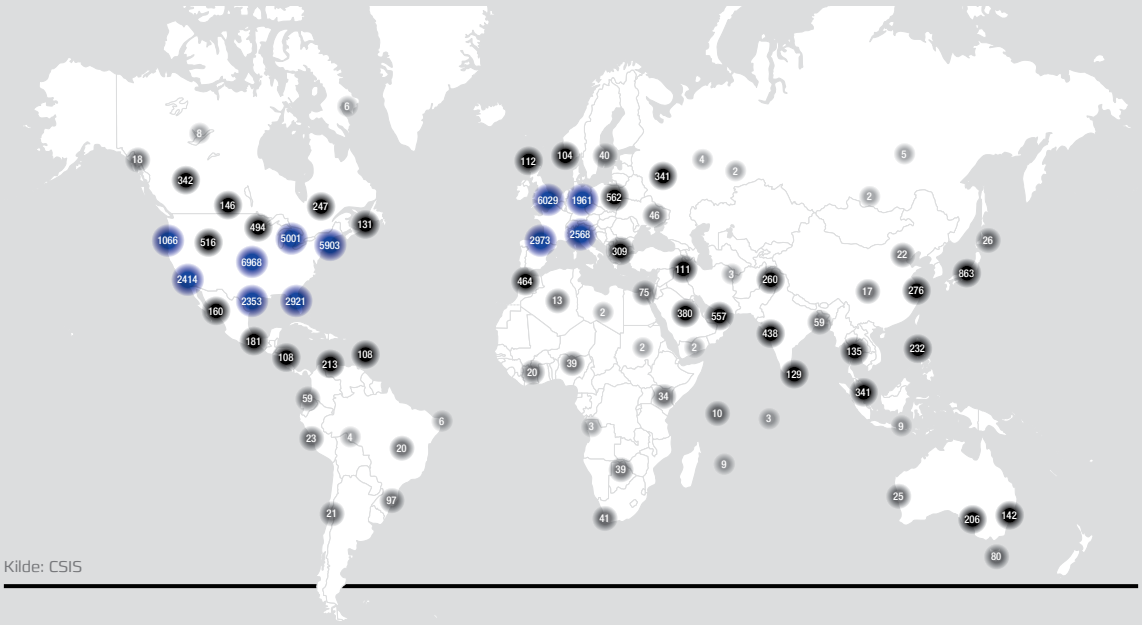
Trickbot er ligeledes en trojansk hest, der ligger skjult i et offers maskine, indtil den aktiveres. Trickbot er blandt andet kendt for at stjæle kreditkortoplysninger ved at omgå to-faktor autentificering og iværksætte såkaldte man-in-the-middle-angreb, hvor offerets loginoplysninger anvendes til at overføre penge. Trickbot kan yderligere anvendes til at levere ransomwaren Ryuk eller Clop, som bl.a. ramte universitet i Maastricht. Her traf ledelsen på universitetet beslutning om at indbetale løsesum på 30 bitcoins svarende til ca. 1.7 mio. kroner for at få data tilbage.

I Danmark har sikkerhedsfirmaet CSIS Security Group A/S opgjort, at der på nuværende tidspunkt er ca. 20 inficerede virksomheder. I gennemsnit bliver 12 danske websider ugentligt kompromitteret via Emotet og misbrugt til at sprede og lancere angreb mod andre danske virksomheder eller offentlige institutioner. CSIS' datagrundlag for denne beregning er baseret på et års tæt observation af transmissionen af Emotet, den såkaldte payload, og webshells på toplevel.dk. Webshell er et program, som gør det muligt at tilgå en webserver udefra og kan installeres uden en systemadministrators vidende. Herved kan det anvendes til kriminelle formål.

3. 2019 – året i tal

Figur 5: Inficerede maskiner med malwaren, Trickbot

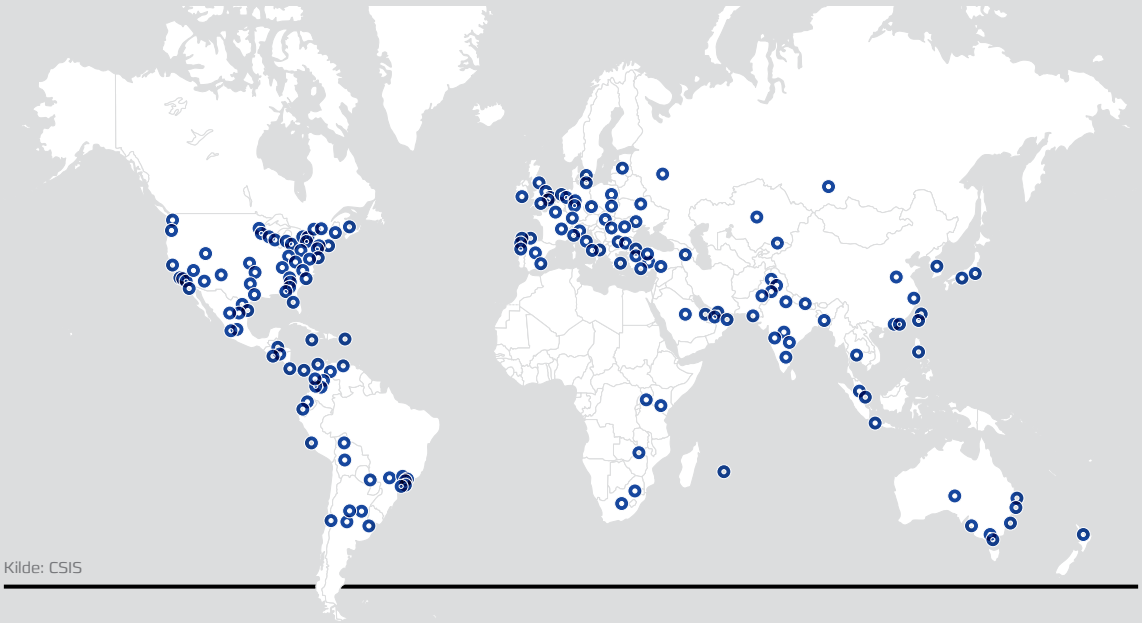
Tallene for Trickbot infektioner er baseret på faktuelle infektioner.



Kilde: CSIS

Figur 6: Observerede Emotet-Infektioner globalt

Emotet infrastruktur er distribueret i hele verden, heriblandt Danmark, som grafen viser. Emotet infrastruktur er vokset helt enormt.

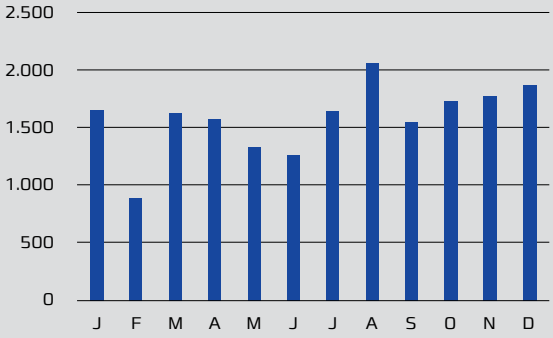


Kilde: CSIS

3. 2019 – året i tal

Figur 7: Indberetninger om sårbarheder i 2019

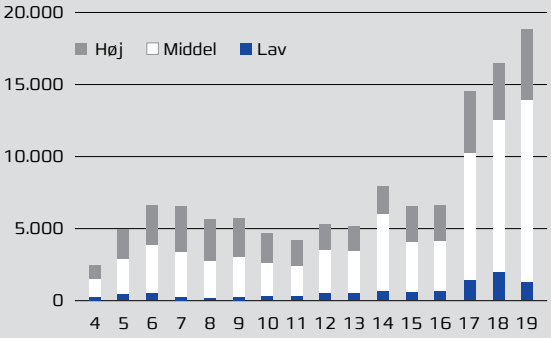
Opgørelse over sårbarheder pr. måned i 2019 fra National Vulnerability Database.



Kilde: National Vulnerability Database.

Figur 8: Sårbarheder pr. år siden 2004

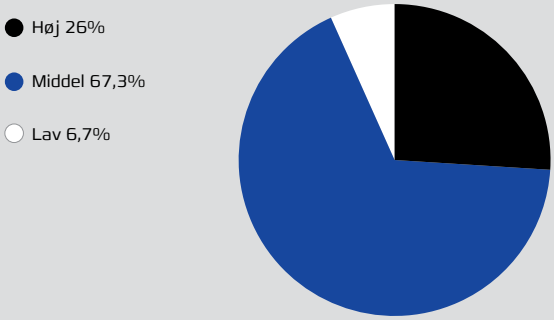
2014 til 2019 data fra National Vulnerability Database.



Kilde: National Vulnerability Database.

Figur 9: Sårbarhedernes CVSS i 2019

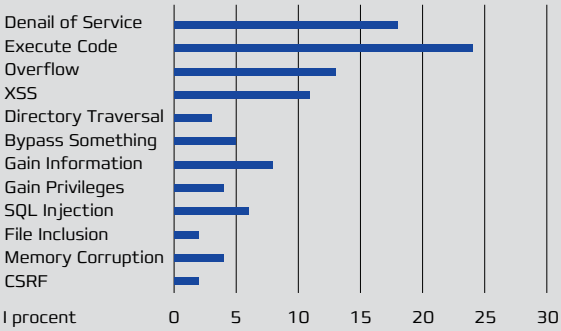
Risikovurdering af sårbarheder gennem 2019 i procent.



Kilde: National Vulnerability Database og CVE Details.

Figur 10: Sårbarheder fordelt på typer

Procentvis fordeling af sårbarheder efter type i 2019.



Kilde: National Vulnerability Database og CVE Details.

3.3. ÅRETS SÅRBARHEDER

I 2019 registrerede USA's National Vulnerability Database 18.938 indberetninger om sårbarheder, hvilket svarer til 1.578 pr. måned. På figuren kan du se fordelingen for hver måned (se Figur 7). Det er en stigning i forhold til 2018, hvor antallet var på 16.555 sårbarheder. Du kan følge antallet af registrerede sårbarheder siden 2004 via Figur 8.

Knap syv procent af sårbarhederne blev vurderet til en CVSS-score på mellem 0 og 3, hvilket er kategorien: lav risiko. CVSS (Common Vulnerability Scoring System) er en åben standard, der anvendes til at beskrive, hvor alvorlig en sårbarhed er. Skalaen går fra 0 til 10, hvor 10 er mest alvorlig.

Den største kategori er middel, hvor lige godt 67 procent af alle sårbarheder befinder sig. CVSS-vurderingen i denne kategori er mellem 3 og 7. I den højest risikovurdering findes 26 procent af årets sårbarheder sig med en CVSS-score på mellem 7 og 10 (se Figur 9).

Sårbarhedernes procentvise fordeling efter forskellige typer kan du få overblikket over med Figur 10.

3. 2019 – året i tal

3.4. SÅRBARHEDSSCANNINGER/-VURDERINGER

DKCERT tilbyder institutioner tilknyttet DeiC gratis 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. Informationerne om de aktuelle sårbarheder, der bliver fundet, kombineres med en redegørelse om hvilke tiltag, som bør foretages for at højne sikkerheden på den enkelte institution. Scanningstjenesten har således udviklet sig fra at udføre traditionelle sårbarhedsscanninger til at tilvejebringe meget mere grundige rapporter, der indeholder en egentlig vurdering af de fundne sårbarheder og anbefalinger til institutionens prioritering og håndtering af disse.

I 2019 har DKCERT gennemført 52 scanninger for medlemmerne af forskningsnettet (se Figur 11). I 2018 var antallet på 121, men med tredje kvartal som en meget atypisk periode med mere end 80 scanninger.

Antallet af scannede host-enheder/IP-adresser er dog steget betydeligt. I 2019 var det på 474.730 host/IP-adresser, mens det i 2018 var 184.698. DKCERT har således scannet langt flere enheder pr. scanning i 2019.

Risikovurderingerne i forbindelse med de eksterne scanninger fortæller, at syv procent af sårbarhederne er kritiske, 29 procent er høj, 55 procent er middel og ni procent er lav (se Figur 12).

Vær dog opmærksom på, at hvis institutionen samtidig er længe om at opdatere software, tæller den samme sårbarhed med i flere scanninger.

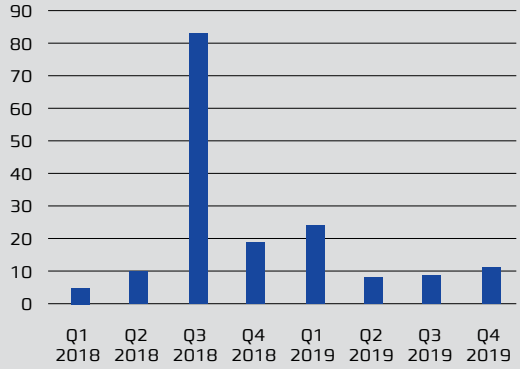
Kilden til sårbarheder opstår typisk i services, applikationer, operativsystemer og konfigurationer. Nedenfor har vi kategoriseret de sårbarheder, der optræder oftest i vores eksterne scanninger af institutionerne på forskningsnettet.

Sårbarhedernes opdeling er baseret på OWASP TOP 10 web-applikationer 2019 og er markeret med en de tre mest anvendte sårbarheds-identifikationsmærker:

> CVE: Common Vulnerabilities and Exposures.
> CWE: Common Weakness Enumeration.
> BID: Bugtraq ID.

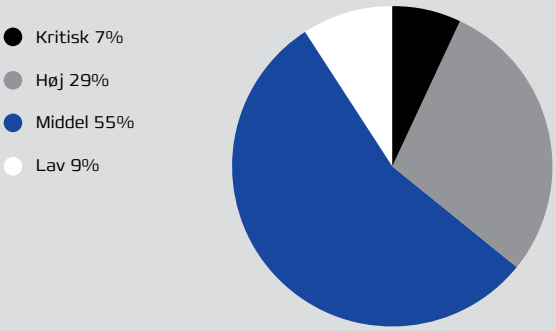
Figur 11: Antal sårbarhedsscanninger i 2018 og 2019

I 2019 udførte DKCERT 52 scanninger på forskningsnettet.



Figur 12: Risikovurdering 2019

Langt hovedparten af sårbarhederne, der blev fundet i de eksterne scanninger på forskningsnettet i 2019, fik risikovurderingen middel.



3. 2019 – året i tal

DE HYPPIGST FUNDNE SÅRBARHEDER I 2019:

Unix Operating System Unsupported Version Detection
- Fedora release 13
- Debian 6.0 & 7.0
- Red Hat Enterprise Linux 3
- Unix FreeBSD 8.3
- CentOS release 5
- Ubuntu 10.04

Microsoft Operating System/Servers Unsupported Version Detection
- Microsoft Windows Server 2003 Unsupported Installation Detection
- Microsoft Exchange Server Unsupported Version Detection
- Microsoft IIS 6.0 Unsupported Version Detection

CVE-2014-3566
SSL Version 2 and 3 Protocol Detection
CVE-2016-2183
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
CVE: CVE-2011-3389
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
CVE-2016-0702, CVE-2016-0705
OpenSSL 1.0.2 < 1.0.2g Multiple Vulnerabilities (DROWN)
CVE: CVE-2014-3566
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
CVE: CVE-2014-8730
TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
CVE: CVE-2004-2761
SSL Certificate Signed Using Weak Hashing Algorithm
CVE-2019-0196
Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
CVE-2015-5589
PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)
CVE-2019-11043
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability
CVE: CVE-2019-6798, CVE-2019-6799
phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities (PMASA-2019-1) (PMASA-2019-2)
CVE-2019-15028
Joomla! 1.6.x < 3.9.11 Joomla 3.9.11 Release (5775-joomla-3-9-11)
CVE: CVE-2016-1287, CVE-2016-1344
Cisco ASA / IOS IKE Fragmentation Vulnerability
CWE: 20, 77, 89, 928
Variants CGI Generic SQL Injection
CWE: 20, 74, 79, 80, 81
Variant CGI Generic XSS

3. 2019 – året i tal

3.5. ADVARSLER FRA TREDJEPARTER

I 2019 udsendte DKCERT 37.308 advarsler fra tredjeparter (Figur 13). Denne service, som blev introduceret i slutningen af 2014, giver institutionerne på forskningsnettet advarsler om potentielt sårbare systemer på deres netværk. Advarslerne kommer fra tredjeparter, der løbende scanner internettet for kendte sårbarheder, som angribere kan udnytte.

DKCERT udsender automatisk disse advarsler mandag til fredag. Derfor kan det samme sårbare system i princippet optræde fem gange på en uge på grafen, der viser alle advarsler. På grafen, der viser unikke advarsler fraregnes dubletter, hvilket giver et antal på 3.366 advarsler i 2019.

Tallene siger dog ikke noget om, hvorvidt angribere har forsøgt at udnytte sårbarhederne. Tallene kan således primært bruges til at give indtryk af, hvordan udbredelsen af de forskellige sårbarheder udvikler sig hen over året.

Institutionerne har ligeledes mulighed for at fravælge advarsler. Det kan eksempelvis skyldes, at man er klar over, at en IP-adresse er sårbar, men at man først kan fjerne sårbarheden om nogen tid. I mellemtiden kan institutionen slippe for at få advarsler om den. Herunder kan du se de fire mest almindelige advarsler.

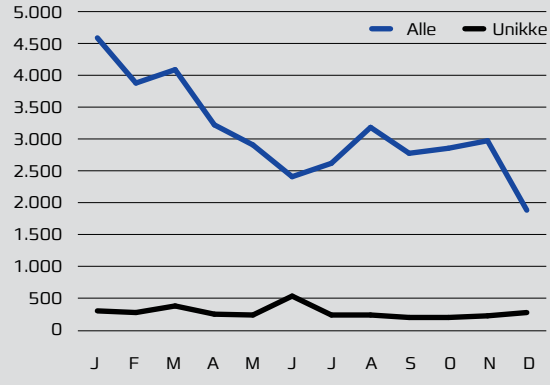
3.5.1. POODLE-sårbarheden

Med en hyppighed på 11.606 handlede hovedparten af advarslerne om sårbarheden POODLE (Padding Oracle On Downgraded Legacy Encryption) (se Figur 14).

POODLE er en udbredt sårbarhed i behandlingen af SSL-kryptering (Secure Sockets Layer), der blev kendt i foråret 2014. En stor del af advarslerne må dog formodes at handle om de samme systemer, som ikke bliver opdateret. I 2018 var tallet på 16.424.

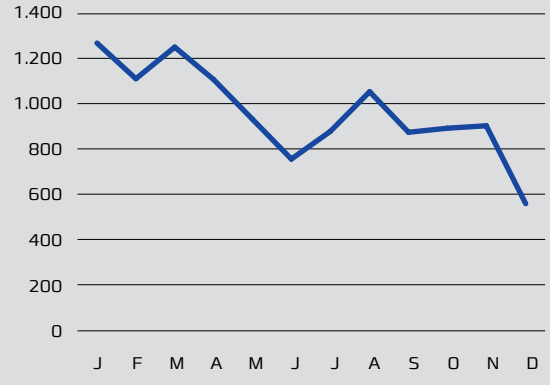
Figur 13: Alle advarsler fra tredjeparter

Advarsler fra tredjepart modtaget i 2019.



Figur 14: Alle advarsler om POODLE 2019

Advarsler om systemer med sårbarheden POODLE.



3. 2019 – året i tal

3.5.2. Åbne RDP-computere

Advarsler om åbne RDP-computere (Remote Desktop Protocol) tegnede sig for 7.643 af årets advarsler. I 2018 var tallet på 12.190. RDP giver mulighed for at fjernstyre en computer. Hvis en RDP-computer kan nås via internettet, kan en hacker afprøve forskellige kombinationer af brugernavn og password. Hvis hackeren er heldig, er der fri adgang til computeren (Se Figur 15).

3.5.3. Åbne tidsservere

Nummer tre på listen over de hyppigst forekommende advarsler med 4.052 forekomster var NTP (Network Time Protocol). NTP-servere bruges til at stille uret på computere via netværk. I 2018 var antallet 4.668.

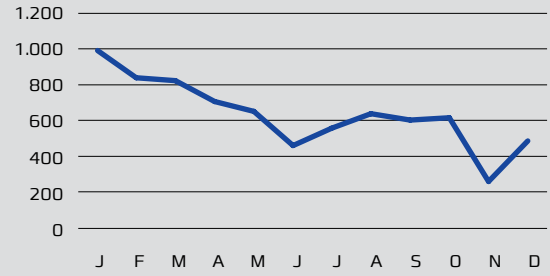
NTP-tjenesten kan misbruges til reflekterede DDoS-angreb (Distributed Denial of Service). Her sender angriberen en forespørgsel til NTP-serveren, hvor afsenderadressen er angivet til offerets adresse. NTP-serveren sender svaret til offeret, hvis computer kan blive overbelastet (se Figur 16).

3.5.4. Portmapper

Portmapper dækker over host-maskiner, der har Portmapper-tjenesten kørende og tilgængelig på det offentlige internet. Det kan udnyttes i forbindelse med Denial of Service-angreb (se Figur 17). fra tredjepart modtaget i 2019.

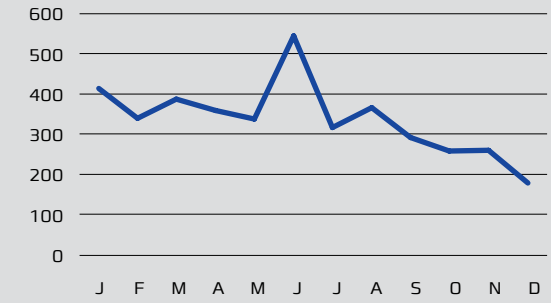
Figur 15: Advarsler om RDP

Advarsler om RDP (Remote Desktop Protocol), der giver mulighed for fjernstyring.



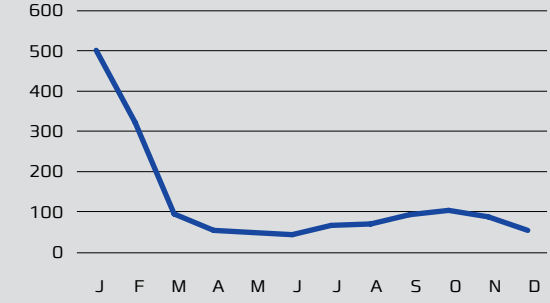
Figur 16: Åbne NTP-servere

Advarsler om NTP-servere (Network Time Protocol).



Figur 17: Registreringer om Portmapper

Registreringer af Portmapper-tjenesten.



4. 2019 – året i ord

Som noget helt nyt har DKCERT i 2019 udarbejdet en Trusselsvurdering for uddannelses- og forskningssektoren og så er telesektorens Decentrale Cyber- og Informationssikkerhedsenhed (DCIS) blevet en del af DKCERT.

4.1. DKCERT'S AKTIVITETER I ÅRETS LØB

4.1.1. Information om sikkerhed

DKCERT informerede løbende om aktuelle trusler, sårbarheder og sikkerhedshændelser på web via fem ugentlige nyhedsbreve og Twitter. I 2019 blev der udgivet 289 artikler omhandlende informationssikkerhed på cert.dk.

Cert.dk havde 55.749 besøgende i 2019. I 2018 var antallet på 51.408. Antallet af unikke sidevisninger var i 2019 på 78.976 (Se Figur 18).

Ved udgangen af 2018 abonnerede 1.577 personer på et af DKCERT's nyhedsbreve. Tallet er faldet en smule i 2019, hvor antallet af abonnenter landede på 1.510.

Twitter bliver dog en stadig mere populær kanal til information om informationssikkerhed, hvilket også kan læses i antallet af følgere. 2.841 fulgte således DKCERT på Twitter ved udgangen af 2019. I 2018 var tallet på 2.439, hvilket er en stigning på 402 følgere (se Figur 19).

Chefen for DKCERT, Henrik Larsen, optrådte jævnligt som ekspertkilde og klummeskribent i medierne i årets løb. DKCERT har samlet information om hvilke medier, der anvender DKCERT som kilde. Det samlede antal medieklip i perioden var på 62 (se Figur 20).

Henrik Larsen er desuden medlem af en række danske og europæiske netværk, udvalg og paneler på it- og informationssikkerhedsområdet. Blandt andet er han medlem af regeringens nye cybersikkerhedsråd og af bestyrelsen for Rådet for Digital Sikkerhed.

4.1.2. DKCERT-CAB

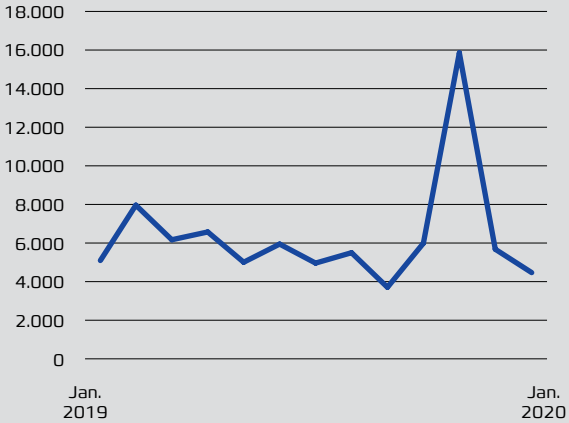
DKCERT-CAB (Change Advisory Board) er et rådgivende organ med repræsentanter for brugerne af DKCERT's tjenester. Gruppen består af en repræsentant for Danske Universiteters CIO-gruppe, to fra CISO-forum, en for NetTekRef og en for øvrige institutioner. Gruppen mødtes fire gange i 2019.

4.1.3. 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 har DKCERT etableret en tjeneste, der kan analysere trafikdata fra routerne på nettet. Tjenesten anvendes til efterforskning af sikkerhedshændelser for institutionerne og i forbindelse med politisager.

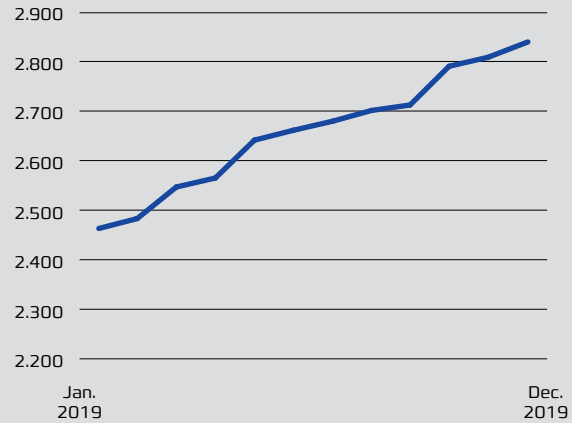
Figur 18: Unikke page views på cert.dk

Antallet af unikke page views på cert.dk.



Figur 19: DKCERT på Twitter

Antallet af følgere på Twitter.



4. 2019 – året i ord

4.1.4. Telesektorens DCIS

Regeringen offentliggjorde i foråret 2018 en ny national cyber- og informationssikkerhedsstrategi. I strategiens initiativ 3.1 fastlægges det, at der skal oprettes decentrale cyber- og informationssikkerhedsenheder (DCIS'er) for hver af de seks sektorer, der i strategien er defineret som samfundskritisk infrastruktur. En af disse sektorer er telesektoren.

En DCIS skal fungere som et samlende kommunikationspunkt for sektoren. DCIS'ens primære opgave er at formidle, efterspørge, skabe og validere informationer om relevante informationssikkerhedsforhold mellem sektorens operatører og Center for Cybersikkerhed (CFCS). En DCIS fungerer som et udvekslingspunkt for informationssikkerhedsinformationer, 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.

Etablering af TeleDCIS

For Telesektorens vedkommende er der den særlige situation, at CFCS både er leverandør og modtager af sikkerhedsinformationer og samtidig regulerende myndighed for Telesektoren. Det har betydet, at der var et ønske om en armslængde mellem CFCS og Telesektorens DCIS. Det blev løst ved at Telesektorens 12 kritiske virksomheder i foråret 2019 dannede en forening, som er ansvarlig for driften af TeleDCIS. Virksomhederne betaler et gebyr til foreningen, som finansierer den daglige drift af TeleDCIS. I 2019 har CFCS bidraget med et tilskud til huslejen. Den daglige drift er outsourcet til DKCERT, som er CERT for Forskningsnettet.

Efter foreningens oprettelse blev der indgået kontrakt med DeiC/DKCERT om den operationelle drift af TeleDCIS. Foreningen besluttede, at TeleDCIS skulle bemandes med to medarbejdere.

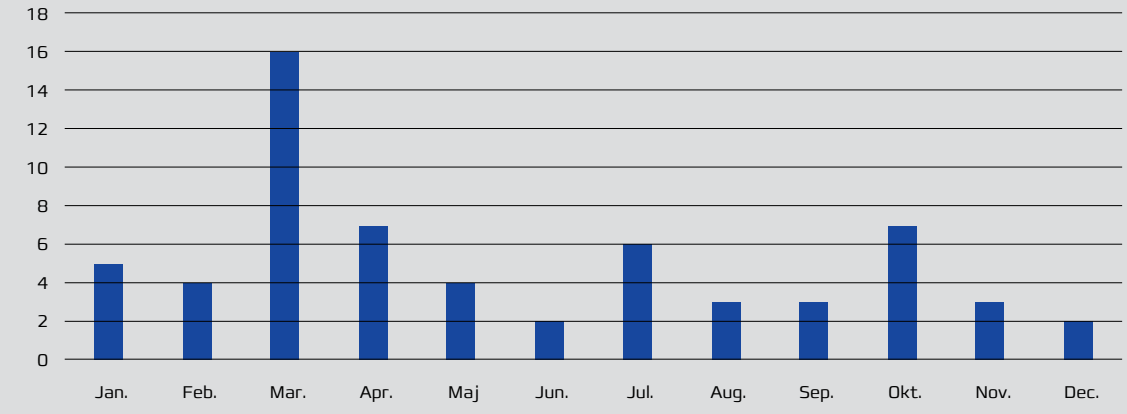
Strategi og varetagelse af politiske forhold er ikke overdraget til TeleDCIS, men varetages af Telesektorens deltagere i foreningen for TeleDCIS.

DeiC/DKCERT står for de praktiske forhold i relation til den daglige drift af TeleDCIS, herunder lokaler hos DTU og ansættelse af de medarbejdere, som skal varetage den daglige drift. På baggrund af opslag blev der ansat en leder af TeleDCIS pr. 1. august 2019.

I regeringens strategi forudsættes det, at der for hver af de seks udpegede sektorer i 2018 udarbejdes sektorspecifikke strategier i forlængelse af den nationale strategi. Telesektoren udarbejdede derfor, på baggrund af input fra de teleudbydere,

Figur 20: Presseomtaler i 2019

DKCERT-presseklip/interviews.



4. 2019 – året i ord

der var udpeget som kritiske, en risiko- og sårbarhedsvurdering, som kom til at danne grundlaget for den første samlede cyber- og informationssikkerhedsstrategi for telesektoren i slutningen af 2018. Strategien er blevet til på baggrund af et bredt samarbejde mellem Teleindustrien, DI Digital, Dansk Energi, ITB og Dansk Erhverv.

Indtil Telesektorens DCIS kunne blive operationel, varetog CFCS rollen som TeleDCIS fra januar 2019. Pr. 1. juni 2019 overtog DKCERT den daglige, operationelle drift.

4.1.5. Trusselsvurdering for uddannelses- og forskningssektoren

Som noget helt nyt har DKCERT i 2019 udarbejdet en trusselsvurdering for universitetssektoren, hvor der foretages en vurdering af troværdigheden og alvoren af en potentiel trussel.

Trusselsvurderingen er opbygget efter samme skabelon som den, der anvendes i forbindelse med trusselsvurderinger fra CFCS.

I vurderingsarbejdet anvender DKCERT en række af både eksterne og interne kilder som eksempelvis indberetninger til CERT-tjenester, phishingkampagner, sårbarhedsscanninger eller erfaringer fra DPO-netværket og tjenester.

Trusselsvurderingen findes bagerst i denne rapport i afsnit 9.

4.1.6. Rådgivning om databeskyttelsesforordningen (DPO-tjeneste)

Universiteter og andre institutioner på forskningsnettet skal som alle andre overholde EU's databeskyttelsesforordning, hvis regler skulle håndhæves fra den 25. maj 2018. Til at hjælpe dem med opgaven, introducerede DeiC i 2017 DPO-tjenesten, der fungerer som en ekstern databeskyttelsesrådgiver (DPO, Data Protection Officer), og som en fleksibel ressource for de uddannelsesinstitutioner, der måtte ønske det. Tjenesten er knyttet til DKCERT.

DPO-tjenesten har indgået aftaler med en række uddannelsesinstitutioner både om fast regelmæssig rådgivning eller mere ad hoc-hjælp. I 2019 varetog tjenesten DPO-funktionen hos nedenstående forsknings- og uddannelsesinstitutioner:

- Roskilde Universitet (RUC).
- Professionshøjskolen Absalon.
- Det Kongelige Danske Kunstakademis Skoler for Arkitektur, Design og Konservering (KADK).
- Arkitektskolen Aarhus (AARCH).
- Designskolen Kolding.
- Dansk Dekommissionering.
- Studievalg Danmark
- Aarhus Universitet anvendte DPO-tjenesten, der vikarierede for DPO-funktionen, i perioden fra 1. august til 31. december.

I forlængelse af tjenestens opgave med at varetage DPO-funktionen hos en række forsknings- og uddannelsesinstitutioner, har DPO-tjenesten også oprettet og driver et netværk for uddannelsesinstitutionernes DPO'er, hvor der i 2019 blev afholdt fire møder. Samtlige universiteter, professionshøjskoler deltager i netværket sammen med repræsentanter fra KADK, AARCH og Designskolen. Mellem møderne udveksler og deler netværket løbende informationer om den nyeste praksis og fortolkning i implementeringen på forsknings- og uddannelsesinstitutionerne.

4. 2019 – året i ord

4.1.7. Awareness-tjenesten Phish

DKCERT har udviklet en awareness-tjeneste, kaldet Phish, til test af brugeres reaktion på phishing-angreb. Universiteter kan bruge tjenesten til at udsende phishing-mails til ansatte og studerende og se, hvor mange der går i fælden. Tjenesten kan bruges som led i en awareness-kampagne med undervisning i, hvordan man genkender en phishing-mail.

I 2019 er der foretaget flere kampagner blandt andet for CBS og SDU. Sidstnævnte udførte eksempelvis en awareness-kampagne med fokus på phishing blandt de ansatte og studerende på universitetet. Der blev i den forbindelse udsendt mere end 30.000 falske beskeder.

Andre institutioner, der anvender forskningsnettet, kan naturligvis også benytte løsningen til uddannelse af brugere.

4.1.8. Internationalt samarbejde

CERT'erne (Computer Emergency Response Team) for de 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'er under de europæiske forskningsnets paraplyorganisation GÉANT.

DKCERT er også medlem af FIRST.org (Forum of Incident Response and Security Teams), som er en organisation for cirka 450 CERT/CSIRT-teams i mere end 90 lande. DKCERT-medarbejdere deltager jævnligt i seminarer samt på årskonferencen og generalforsamlingen.

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 årlige fysiske møder, heraf et årligt fællesmøde WISE Community, som er et globalt netværk for sikkerhed i forsknings-it-infrastrukturer (bl.a. udsprunget af CERN).

Endelig deltager Henrik Larsen i den globale Academic Security SIG, der mødes fysisk en gang årligt i forbindelse med FIRST.org's årskonference og en til to gange via videokonference.

Projektleder Morten Eeg Ejrnæs Nielsen har været med til at etablere en arbejdsgruppe under GÉANT, TF-DPR (Task Force Data Protection Regulation). Han blev valgt til formand for styregruppen i taskforcen og indtager stadig denne position.

Dataanalytiker Simon Jensen deltager i Crisis Management Workshop-arbejdsgruppen (CLAW), som styres af GÉANT, og som udvikler - og afholder seminarer.

4. 2019 – året i ord

4.2. TENDENSER OG TRUSLER I 2019

4.2.1. Awareness i fokus

Uddannelse af brugere på alle niveauer er en af nøglerne til forbedret informationssikkerhed i Danmark, og på awareness-området har 2019 været bemærkelsesværdig.

Den nationale cybersikkerhedsmåned satte eksempelvis fokus på cyber- og informationssikkerhed i hele oktober ved at støtte op om projekter og afholde aktiviteter, der var med til at løfte danskernes viden om, hvordan de digitalt beskytter sig selv og deres informationer.

Men det var langt fra den eneste begivenhed på området. Der er således udgivet undervisningsmateriale til både unge og uddannelsesinstitutioner, til bestyrelser og til offentligt ansatte.

Ligeledes er der sat fokus på konkrete områder som dataetik, industrielle kontrolsystemer og Internet of Things (IoT), hvilket er en meget positiv tendens.

Et eksempel fra universitetsverdenen var, da SDU igangsatte en awareness-kampagne med fokus på phishing blandt de ansatte og studerende. I den forbindelse blev der udsendt mere end 30.000 falske beskeder afsted til indbakkerne på universitetet.

Kampagnen blev afviklet med DKCERT's-awareness værktøj, Phish, der fungerer efter samme principper som en ondsindet phishing-kampagne, men hvor alt foregår i et krypteret og afgrænset miljø.

4. 2019 – året i ord

DKCERT MENER

Et af de svage led i forbindelse med informationssikkerhed er personen bag skærmen. Det er her, mange sikkerhedskomplikationer opstår, da brugeren ofte står direkte i cyberskudlinjen. Derfor er det også glædeligt, at der har været stor opmærksomhed på området.

Uddannelse og adfærdsreguleringer er et vedvarende og vigtigt element i informationssikkerheden i et trusselsbillede, der er stigende.

Men der hviler samtidig et tungt ansvar på teknologien. Det er vigtigt, at brugerne bliver støttet af teknologi, så deres data eller systemer ikke let bliver kompromitteret. Der er således også et krav om, at de hjælpes på vej med eksempelvis multifaktor-beskyttelse eller mail-systemer, der filtrerer så meget uønsket post fra, som det er muligt. Awareness og teknologi skal gå hånd i hånd.

Udvalgte referencer fra cert.dk:

SDU sender tusindvis af falske mails i stor awareness-kampagne
https://www.cert.dk/da/news/2019-10-08/phishing

Bestyrelsesforeningen udgiver vejledning om cybersikkerhed
https://www.cert.dk/da/news/2019-12-18/cfcs

CFCS og flere uddannelsesinstitutioner holder cyberdage
https://www.cert.dk/da/news/2019-09-24/csm

Nyt undervisningsmateriale skal uddanne unge i informationssikkerhed
https://www.cert.dk/da/news/2019-11-20/awareness

En ny kampagne skal sætte fokus på sikkerheden i IoT-produkter
https://www.cert.dk/da/news/2019-11-19/iot

CFCS udgiver vejledning om sikkerhed i industrielle kontrolsystemer
https://www.cert.dk/da/news/2019-11-14/cfcs

Awareness-materiale til undervisning af offentligt ansatte
https://www.cert.dk/da/news/2019-11-05/awareness

Cybersikkerhedsmåned: Gå-hjem-møde om dataetik
https://www.cert.dk/da/news/2019-10-10/rfds

4. 2019 – året i ord

4.2.2. Phishing virker stadig

Phishing er stadig en af de mest effektive metoder til at begå it-kriminalitet. 2019 har ikke ændret ved det forhold. Phishing som fænomen er i støt stigning, hvilket de fleste nok også har bemærket i form af indbakker, sociale medier og telefoner, der bugner med falske beskeder. På telefonen kalder vi det "smishing" (SMS) eller "vishing" (voice).

Der har været målrettede kampagner mod vores egen verden, hvor kriminelle gik efter universitetsstuderende i svindelkampagner, men den dominerende – dansksprogede – mængde phishing-beskeder har været forsynet med en falsk afsender i form af eksempelvis Nets eller Skat.

I international sammenhæng er det typisk etablerede virksomhedsnavne som Paypal, Microsoft, Google, Outlook og Apple som it-kriminelle udnytter i forsøget på at fiske oplysninger fra ofret.

Direktørsvindel er en specialiseret variant, og Danmark rammes ifølge sikkerhedsfirmaet Trent Micro af 0,8 procent af verdenens direktørsvindel.

DKCERT MENER:

Phishing er den væsentligste angrebsvektor til de fleste typer af cyberangreb, og der skal en samlet strategi til at bekæmpe den.

Det er umuligt helt at undgå det digitale bombardement af ondsindede beskeder, og du skal gå ad tre veje samtidigt for at mindske skadevirkningen. Du skal have styr på:

- Tekniske kontroller.
- Procedurer.
- Den menneskelige faktor.

De gode råd, som vi skal lære brugerne for at undgå phishing-problemer, er:

- Vær altid kritisk over for mails - også selvom du tilsyneladende kender afsenderen. Adressen kan være forfalsket, eller afsenderens konto kan være kompromitteret.
- Lad være med at åbne vedhæftninger, før du er sikker på afsenderen, selvom du er nysgerrig.
- Lad være med at klikke på links i e-mails. Skriv eller kopier i stedet adressen ind i adressefeltet – så kan du også se, om den peger derhen, hvor du forventer.
- Vær opmærksom på, at banker og myndigheder IKKE beder om personlige oplysninger via mail.
- Er du det mindste i tvivl om ægtheden, så slet beskeden. Ring eventuelt til afsenderen for at kontrollere ægtheden.
- Download gerne Forbrugerrådets app "Mit digitale selvforsvar", der advarer om kendte, igangværende phishing-kampagner.

Ved direktørsvindelforsøg er det vigtigt, at man har en fast aftale – helst en nedskrevet procedure – om, at medarbejderen skal ringe til chefen, selvom vedkommende er på ferie. På den måde er medarbejderen ikke utryg ved at ringe, og chefen vil helt sikkert hellere godkende en betaling via et kort telefonopkald end miste penge.

Udvalgte referencer fra cert.dk:

Kriminelle går efter universitetsstuderende i svindelkampagne
https://www.cert.dk/da/news/2019-09-16/phishing

Kriminelle er konstant på jagt efter højtspecialiseret viden
https://www.cert.dk/da/klumme/2019-10-28/sl

Rapport: Danmark rammes af 0,8 procent af verdens direktørsvindel
https://www.cert.dk/da/news/2019-03-05/ceo

Flere advarsler om falske mails med Skat som 'afsender'
https://www.cert.dk/da/news/2019-11-14/skat

Advarsel: Mange fupbeskeder i omløb
https://www.cert.dk/da/news/2019-10-07/phishing

Ny omgang phishing med Nets som falsk afsender
https://www.cert.dk/da/news/2019-07-15/phishing

Finans Danmark: Netbankmisbrug er i stigning
https://www.cert.dk/da/news/2019-07-08/netbank

Disse navne udnyttes mest til phishing
https://www.cert.dk/da/news/2019-05-21/phishing

4. 2019 – året i ord

4.2.3. Ransomware og sextortion til afpresning

En tendens fortsatte uændret i 2019, og det er de kriminelles afpresning af ofre for at opnå økonomisk gevinst. To metoder er populære.

Ransomware

Ransomware er en form for skadelig software, der spærrer/krypterer for adgangen til offerets computer eller data. For at få genoprettet adgangen skal offeret betale en løsesum til bagmændene.

Der er flest penge at tjene for de it-kriminelle, når de går efter virksomheder, men ransomware er absolut også en udfordring blandt almindelige brugere. Ligeledes har dette været et globalt fænomen i 2019.

Sextortion

Specielt i den førte halvdel af 2019 var de såkaldte sextortion-udsendelser meget udbredte. Året bød også på en ny variant af sextortion-beskeder med vedhæftede og password-beskyttede filer, der beskrives som 'beviser' for ofrets handlinger.

De kriminelles arbejdsgang er typisk, at de udsender en mail, som påstår, at afsenderen har billeder eller videoer af modtageren i kompromitterende situationer af seksuel karakter. Billeder eller videoer er ifølge den kriminelle optaget med kameraet på ofrets egen computer.

Bagmændene kræver så penge for at ofret kan undgå, at materialet bliver offentliggjort til eksempelvis Facebook-venner.

DKCERT MENER:

Udbredte afpresnings- og ransomware-angreb understreger behovet for sikkerhedskopiering. Med en sikkerhedskopi kan man ofte gendanne data i tilfælde af ransomware-infektioner.

Segmentering/opdeling af netværk kan begrænse ransomware-skaden, idet den skadelige programkode får sværere ved at sprede sig rundt i netværket.

Med hensyn til sextortion er gode password-vaner også et meget effektivt værktøj til god sikkerhed. Betal aldrig løsepenge, men kontakt eventuelt politiet.

Udvalgte referencer fra cert.dk:

En ny type sextortion-beskeder er dukket frem
https://www.cert.dk/da/news/2019-04-09/sextortion

Ny sværm af sextortion-udsendelser
https://www.cert.dk/da/news/2019-03-20/afpresning

Bølge af afpresnings-mails over Danmark
https://www.cert.dk/da/news/2019-07-02/sextortion

NorCERT fortæller om cyberangreb mod stor virksomhed
https://www.cert.dk/da/news/2019-03-20/ransom

Ny NextCry ransomware går målrettet efter NextCloud
https://www.cert.dk/da/news/2019-11-19/php

4. 2019 – året i ord

4.2.4. E-handel og fupbutikker

Danskere, der rammes af onlinesvindel eller anden form for digital kriminalitet, er en bekymring i e-handelssamfundet, fordi fupbutikker er et fænomen i kraftig stigning.

I 2019 er antallet eksploderet, og e-mærket har spottet hele 150.000 webshops, som er det ren fup. I 2018 blev der ifølge sikkerdigital.dk spottet 10.000.

E-mærket er en nonprofitorganisation, som blandt andet certificerer sikre danske webshops og foretager undersøgelser blandt webshops i Danmark, hvor de finder og anmelder fupbutikker.

Det er dog ofte internationale samarbejder, der giver de bedste resultater i forbindelse med butikslukningerne og i den forbindelse spiller Europols samarbejde med de enkelte landes myndigheder en vigtig rolle.

I april lukkede Europol eksempelvis 30.500 internetdomæner på grund af krænkelse af intellektuel ejendomsret. I den mere lyssky ende af skalaen har Europol lukket to illegale handelsportaler, som er blevet anvendt til salg af narkotika, stjålne kreditkortnumre, ondsindet software og andre ulovlige varer.

DKCERT MENER:

Husk, at hvis et tilbud ser ud til at være for godt til at være sandt, så er det nok også tilfældet. Se efter e-mærket, betal med kort, undersøg hvem du handler hos, læs betingelserne og gem kvitteringen som et bevis for dit indkøb.

Vær opmærksom på, at fupbutikker ofte hænger sammen med phishing mails eller tvivlsomme online-reklamer. Derfor skal du altid være kritisk over for mails/reklamer, hvor du ikke kender afsenderen. Lad være med at klikke på links eller vedhæftede filer, selvom du er nysgerrig. Er du det mindste i tvivl, så slet beskeden og undgå 'tilbuddet'.

Udvalgte referencer fra cert.dk:

Europol lukker 30.500 piratsider
https://www.cert.dk/da/news/2019-12-04/europol

Sikkerhedsfirma advarer om 10.000 fupbutikker i forbindelse med Black Friday
https://www.cert.dk/da/news/2019-11-26/blackfriday

Europol lukker to illegale handelsplatforme
https://www.cert.dk/da/news/2019-05-08/europol

Rapport: Hver anden dansker rammes af digital kriminalitet
https://www.cert.dk/da/news/2019-05-03/ida

Non-profit samarbejde har nu lukket 100.000 malware-sider
https://www.cert.dk/da/news/2019-01-23/urlhaus

4. 2019 – året i ord

4.2.5. Sektorstrategier, der skal sikre den kritiske infrastruktur

I maj 2018 kom den nationale strategi for cyber- og informationssikkerhed (temaet for sidste års Trendrapport). I 2019 blev regeringen så klar med planerne for den kritiske infrastruktur til beskyttelse mod cyber-angreb inden for seks samfundskritiske sektorer.

De seks sektorer er sundheds-, finans-, tele-, søfarts-, transport- og energisektoren.

Hver især skal disse områder opbygge decentrale cyber- og Informationssikkerhedsenheder (DCIS'er), der skal sikre informationsudveksling mellem sektorerne og Center for Cybersikkerhed samt forestå vedligeholdelsen af risiko- og sårbarhedsvurderinger.

Telesektoren valgte i denne forbindelse at placere sektorens DCIS hos DKCERT på DTU Campus i Lyngby.

DKCERT MENER:

Det er en meget stor beslutning, når sektorerne på denne måde går sammen på tværs af selskaber og interesser for at styrke den nationale informationssikkerhed.

I et digitalt samfund er det nemlig en forudsætning, at de kritiske tjenester kan levere varen – specielt i krisetider.

Ved at rykke tæt sammen kan vi langt bedre modstå de trusler, der hele tiden er mod Danmark.

Udvalgte referencer fra cert.dk:

Nye sektorstrategier skal sikre den kritiske infrastruktur
https://www.cert.dk/da/news/2019-01-07/strategi

DKCERT skal varetage telebranchens decentrale cyber- og informationssikkerhedsenhed
https://www.cert.dk/da/news/2019-03-25/dcis

DKCERT har ansat leder af TeleDCIS
https://www.cert.dk/da/news/2019-09-11/teledcis

4. 2019 – året i ord

4.2.6. Ny overhaling af adgangskoder

Et brugernavn og en adgangskode er ofte de eneste lag af sikkerhed, man anvender, og derfor var emnet også på dagsordenen i 2019. Det udmøntede sig blandt andet i, at Center for Cybersikkerhed udgav en revideret version af anbefalingerne til gode adgangskoder.

Passwordvejledningens formål er at hjælpe virksomheder og myndigheder med at finde en fornuftig balance mellem sikkerhed og anvendelighed samt hjælpe medarbejdere til en sikker adfærd gennem awareness-tiltag og understøttende teknologi.

Vejledningens hovedområder:

- Større anvendelse af flerfaktorgodkendelse.
- Ny prioritering af længde over kompleksitet i passwords.
- Behovet for større brug af unikke passwords.
- Anvendelse af password manager.
- Beskyttelse mod ofte anvendte eller tidligere lækkede passwords.
- Begrænsning i brug af tvungne passwordskift.

Det ser da også se ud til, at det stadig er nødvendigt at få strammet op. Uafhængige sikkerhedsforskere har i samarbejde med firmaet NordPass udarbejdet en liste over de 200 mest populære adgangskoder i 2019. Datamaterialet er indsamlet via datalæk og består af mere end 500 millioner passwords.

Desværre er der ikke de store overraskelser i forhold til tidligere år. De fem mest anvendte adgangskoder er nemlig:

- 12345
- 123456
- 123456789
- test1
- password

DKCERT MENER:

Et godt password er mindst 12 tegn langt, men gerne længere. Adgangskoden er ikke et ord, man kan finde i en ordbog eller på nettet. Brug altid forskellige passwords til forskellige tjenester. Du kan gemme dine passwords med et program, der beskytter dem med kryptering og adgangskode, en såkaldt password manager.

Institutionerne bør stille password manager-app's til rådighed. Sådanne programmer befordrer brugen af separate passwords til forskellige tjenester.

Et godt råd er, at du udarbejder en oversigt over alle de onlinetjenester, som du anvender og sørger for, at der er forskellige og stærke adgangskoder til alle. Slet eventuelt de konti, du ikke benytter mere.

Udvalgte referencer fra cert.dk:

CFCS udgiver ny password-vejledning
https://www.cert.dk/da/news/2019-10-21/password

Sikkerhedsfirma: Her er de mest populære passwords i 2019
https://www.cert.dk/da/news/2019-12-18/password

Gammelt password kan give adgang til Cisco-produkt
https://www.cert.dk/da/news/2019-02-14/cisco

Så lange er danskernes adgangskoder
https://www.cert.dk/da/news/2019-01-07/password

4. 2019 – året i ord

4.2.7. (Igen) et år med store datalækager

2019 har desværre været endnu et år med enorme datalæk.

Mest bemærkelsesværdigt var en enkelt episode, hvor personlige oplysninger om potentielt 1,2 milliarder mennesker blev offentliggjort i forbindelse med en massiv datalækage. Universiteterne var i den forbindelse også berørt.

Et andet eksempel fra 2019 bestod i, at mange millioner adgangskoder til Facebook og Instagram viste sig at være opbevaret i et internt storagesystem i plain text, altså uden kryptering.

Bloggen, IT Governance, fører statistik over lækager, og du kan følge de enkelte måneder i Figur 21.

GDPR er blevet moden

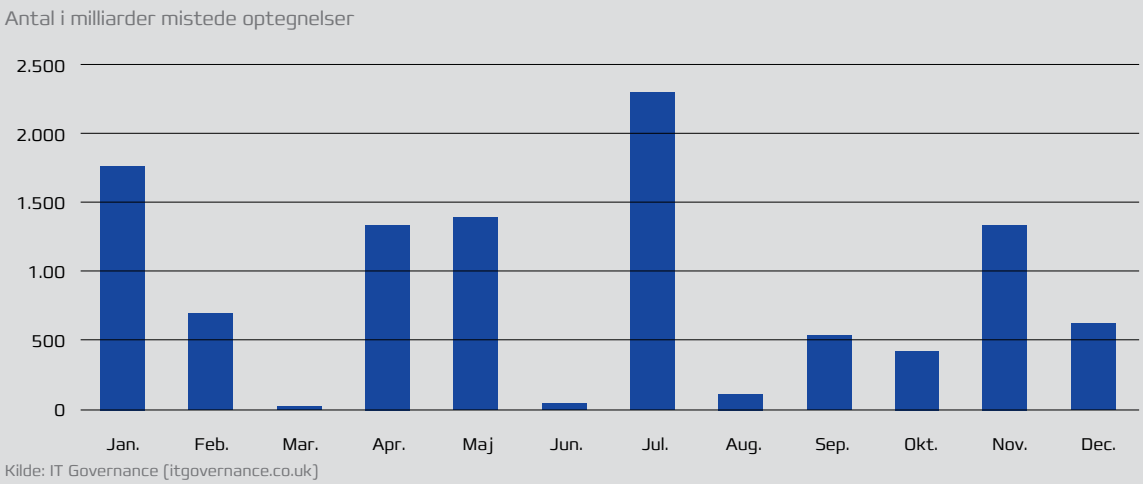
GDPR fyldte et år i 2019, hvilket betyder, at der nu kan samles gode tal til statistikkerne.

Ifølge Datatilsynet var der i løbet af 2019 indberettet 7.307 underretninger om brud på persondatasikkerheden, heraf var 3,7 procent eller 273 af dem fra universiteter og andre uddannelsesinstitutioner. Danmark ligger dermed tredjeøverst i antal indberettede brud på persondatasikkerheden i Europa.

Erfaringen fra DKCERT's DPO-tjeneste er, at universiteterne er ganske godt med i forhold til implementeringen af forordningens regler, og de brud på persondatasikkerheden, der opleves, bunder næsten alle i menneskelige fejl.

Advokatfirmaet DLA Piper samlede informationer om rapporterede databrud i hele Europa i samme tidsrum og kunne oplyse, at der var rapporteret 59.000 databrud siden GDPR-starten.

Figur 21: Antal mistede optegnelser (records) fra databrud i 2019



Kilde: IT Governance (itgovernance.co.uk)

4. 2019 – året i ord

DKCERT MENER:

På grund af GDPR-implementeringen hører vi nu mere om de lækager, der finder sted, hvilket også giver bedre mulighed for at reagere. Hyppige datalæk må dog desværre forventes fremover, og det er svært at gardere sig over for tjenester, der mister data.

Vi anbefaler at være opsøgende i forhold til, om du er berørt af et datalæk både som administrator af brugere og som privatperson. Der findes flere forskellige tjenester på nettet, hvor man kan søge eller abonnere på nyheder om ens digitale fodaftryk. Dette er også en funktion i nogle password-administratorprogrammer, så du har måske allerede funktionen tilgængelig fra en leverandør, du stoler på.

På det danske forskningsnet kan vi se en positiv effekt på flere universiteter, der benytter sig af disse tjenester. Blandt andet Syddansk Universitet (SDU), der i en stor gennemgang af deres domæne har oprettet samtlige deres mail-domæner som abonnent på Haveibeenpwned.com.

Dette har givet dem en stor indsigt i antallet af berørte konti og samtidig en endnu hurtigere reaktionsevne, så de kan advare deres brugere.

Som standard anbefaler DKCERT altid, at hvis dit password er lækket, så skift det til et nyt og følg med i aktivitet på kontoen. I forbindelse med læk, der ikke indeholder dit password, men eksempelvis kontonavn eller mail-adresse, er det stadig en god ide at sørge for, at kontoen har stærk adgangssikkerhed (stærkt kodeord, flerfaktor-sikkerhed). Vi anbefaler altid forskellige passwords til forskellige tjenester.

Hav også tanke for, hvilke data du afgiver til hvem, og om det er er nødvendigt.

Udvalgte referencer fra cert.dk:

Datalækage kan potentielt berøre op mod 1,2 milliarder personer
https://www.cert.dk/da/news/2019-11-26/dataviper

Sikkerhedsforsker: Millioner af adgangskoder til Facebook har ikke været krypteret
https://www.cert.dk/da/news/2019-03-22/facebook

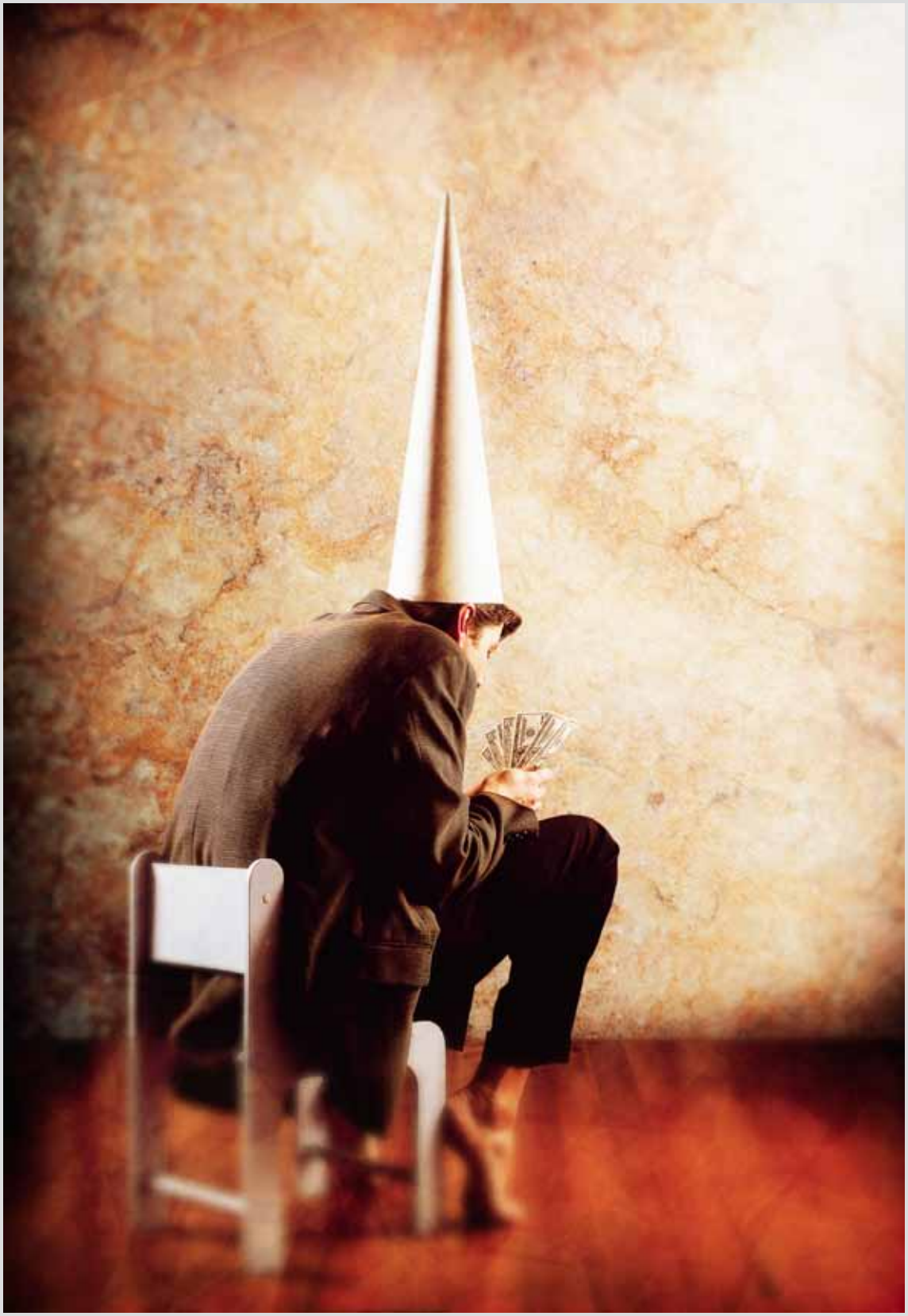
Datatilsynet: Så mange GDPR-henvendelser har vi modtaget på et år
https://www.cert.dk/da/news/2019-05-28/gdpr

Opgørelse: Der er rapporteret om 59.000 databrud siden GDPR-starten
https://www.cert.dk/da/news/2019-02-07/gdpr

Datatilsynet: Sådan sletter du bedst personoplysninger
https://www.cert.dk/da/news/2019-01-29/slet

En svaghed i et billetsystem berører 141 internationale flyselskaber
https://www.cert.dk/da/klumme/2019-01-17/booking

4. 2019 – året i ord



4. 2019 – året i ord

4.2.8. CMS-problemer i væsentligt omfang

Et indholdsstyringssystem, eller CMS, er grundstammen i rigtig mange websider, og blandt de store udgaver findes eksempelvis WordPress, Joomla og Drupal.

Men systemerne er ikke uden sikkerhedsrisiko, hvilket antallet af sikkerhedsopdateringer i 2019 også indikerer.

Problemet ligger ikke nødvendigvis i selve systemets kerne, men stammer i høj grad fra de plugins, der kan anvendes sammen med eksempelvis WordPress. Dem finders der tusindvis af. Ifølge en opgørelsen fra sikkerhedsfirmaet Imperva er 98 procent af CMS-sårbarhederne knyttet til plugins.

Når et CMS anvendes til millioner af installationer, kan en sårbarhed være kritisk for rigtig mange brugere.

I indlægget "Forhøjelse af sikkerheden i din webshop", der kan findes på Nets' blog, kan man læse om grelle eksempler på, at plugins med sårbarheder har været årsag til, at over 300.000 hjemmesider er blevet inficeret.

DKCERT MENER:

CMS er et vigtigt redskab til webformidling, men systemerne er ikke uden vedligeholdelse.

Anvend altid de nyeste versioner eller de versioner, som producenten anbefaler og vær omhyggelig, når du vælger dine plugins.

Det er vigtigt, at du opdaterer, når der er sikkerhedsrettelser og anvend sikkerhedssoftware til at scanne for sårbarheder.

Du skal altid anvende stærke adgangskoder og omdøbe standardkonti fra CMS'er. Anvend konti med så få brugerrettigheder, som det er muligt.

Udvalgte referencer fra cert.dk:

WordPress-relaterede sårbarheder stiger markant
https://www.cert.dk/da/news/2019-01-10/cms

Jetpack til WordPress skal opdateres
https://www.cert.dk/da/news/2019-11-21/jetpack

Drupal opdateres
https://www.cert.dk/da/news/2019-12-20/drupal

WordPress lukker seks sårbarheder
https://www.cert.dk/da/news/2019-09-09/wordpress

Drupal lukker kritisk sårbarhed
https://www.cert.dk/da/news/2019-07-18/drupal

Sårbarhed i WordPress-plugin
https://www.cert.dk/da/news/2019-03-25/wordpress

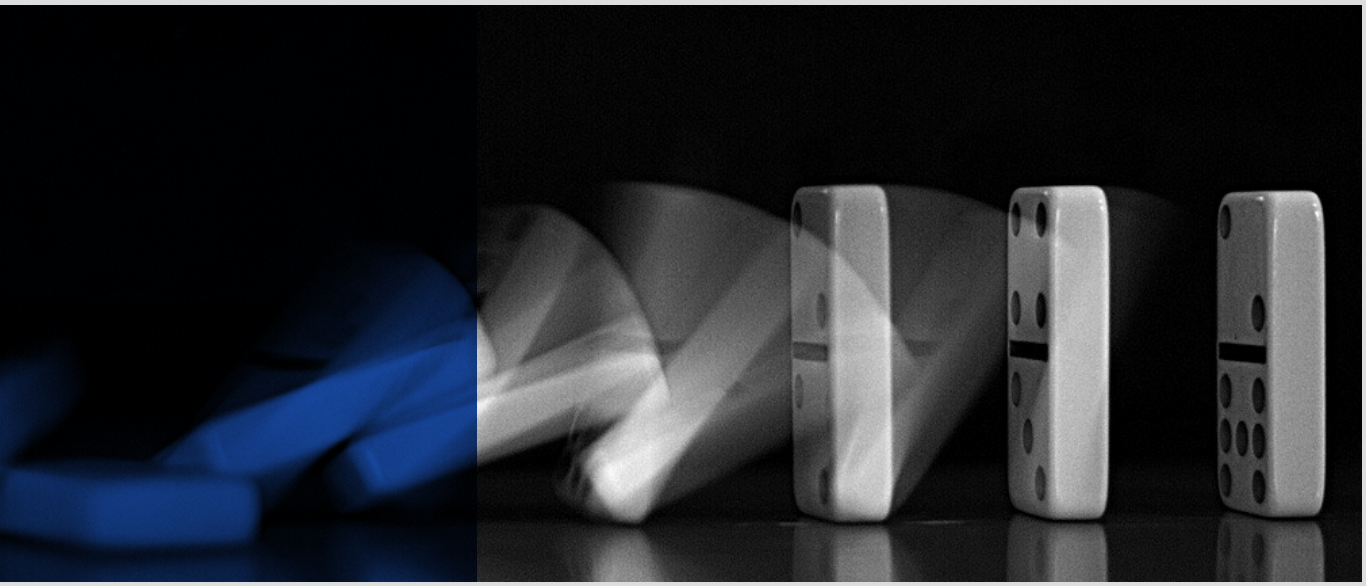
Ny version af Joomla
https://www.cert.dk/da/news/2019-03-14/joomla

5. Det eksterne perspektiv

Fem bidragydere giver her deres syn på, hvordan man bedst forbereder sig på at håndtere en krise. Vi har inviteret fem eksperter til at skrive hver deres indlæg, der fra forskellige vinkler belyser det vigtige arbejde med krisehåndtering.

Bidragsyderne er:

- Thomas Kristmar,
  Senior Manager KPMG og medlem af Fagrådet for informationssikkerhed i Dansk IT og regeringens cybersikkerhedsråd.
- Alf Moens,
  Corporate Security Officer, SURFnet
- Frederik Helweg-Larsen,
  Expert Director, Devoteam
- Simon Nexø Jensen,
  Sikkerhedsanalytiker, DKCERT
- Thomas Lund-Sørensen,
  Chef for Center for Cybersikkerhed



5. Det eksterne perspektiv

5.1. DET SKER NOK IKKE FOR MIG...

AF: THOMAS KRISTMAR,
SENIOR MANAGER KPMG OG MEDLEM AF FAGRÅDET FOR INFORMATIONSSIKKERHED I DANSK IT.

Det sker ikke for mig, synes at være en tilgang mange har til beredskabsplanlægning. "Hey, vi har en backup, og vores nyindkøbte next generation, AI-powered Intrusion Prevention System håndterer alle trusler, siger leverandøren.". Så enkelt er det ikke.

Vi læser dagligt om virksomheder og myndigheder i ind- og udland, som rammes af cyberangreb såsom fra ransomware. Når det alvorlige angreb rammer, viser det sig, at backuppen alligevel ikke er komplet eller tilgængelig, og at angreb ikke er blevet stoppet af magisk sikkerhedsteknologi. Hvordan kan det så gå galt? En væsentligt årsag er, med udgangspunkt i min erfaring, at der mangler en beredskabsplan, og nok så vigtigt, at beredskabsplanen ikke er trænet med alle relevante dele af organisationen.

5.1.1. Beredskab i teorien

En beredskabsplan bestemmer, hvordan en organisation styrer indsatsen og prioriterer ressourcer, når den daglige drift ikke slår til, hvordan organisationen skal samarbejde og samvirke på tværs af afdelinger og divisioner for at nå i mål. Operational Resilience er en term, som ofte anvendes til at favne elementerne i et effektivt beredskab. Kort fortalt består Operational Resilience af tre komponenter: IT Service Continuity Management (ITSCM), Business Continuity Management (BCM) og Crisis Management (CM). ITSCM handler om at sikre, at organisationen kan reetablere systemer og information inden for tidsrammer og i en rækkefølge fastsat af forretningen, herunder også sikre, at systemer kan reetableres fra bunden, hvis backuppen fejler. BCM handler om at identificere de kritiske processer og sammen med it-leverandøren mappe processer til systemer og fastlægge reetableringsstider – altså, hvor længe man kan opretholde sin forretningsproces, hvis systemer er helt eller delvis fraværende.

Som led heri også identificere nødprocedurer som beskytter processen mod kortvarige nedbrud. Helt lavpraktisk, hvis fx et ordresystem er nede, så have forberedt det at kunne skrive ordrer ned på papir og kunne ekspedere dem manuelt osv. Al erfaring tilsiger, at der i virksomheden er viden om disse "quick fixes", som blot skal identificeres og gøres tilgængelige for alle. CM handler om at udstikke den strategiske retning for virksomhedens reetablering, kommunikere omkring situationen internt og eksternt og – give it-leverandøren rum til at reetablere inden for de aftale rammer.

5.1.2. Beredskab i praksis

Det vigtigste at holde sig for øje er, at beredskab og operational resilience er en operativ disciplin og ikke en compliance-øvelse. Formålet med operational resilience er ikke at vise it-revisionen eller risikofunktionen, at der er "passende kontroller" for backup, men at sikre organisationens funktionsevne og fortsatte drift, når der er sket en alvorlig hændelse. Det betyder, at beredskabsplanen skal være kort og præcis, basere sig på den eksisterende organisering og kunne håndtere at hændelser ofte udvikler sig anderledes en forventet.

5.1.3. "Train as you Fight and Fight as you Train"

I praksis vil det sige, at den person eller enhed, der i dagligdagen har ansvaret for et område, også bør have ansvaret under krise. Det sikrer, at den viden, der i hverdagen er omkring drift og afhængigheder, også kan anvendes under krisen. Anbefalingen skyldes, at al erfaring tilsiger, at der ikke kommer noget godt ud af at ændre organisering eller beslutningsproces, når der opstår en krise.

Det medvirker til at skabe usikkerhed om prioriteringer, beslutningskompetence og øger kompleksiteten under krisen, hvilket netop skal undgås. Et vigtigt element i kriseledelse er også at kunne fokusere på den strategiske ledelse og afholde sig fra at overtage en operative ledelse i ren iver for at vise handlekraft.

Når man vurderer, hvor klar ens organisation er til at håndtere en uforudset cyberhændelse, skal man se på de tre elementer i operational resilience.

5. Det eksterne perspektiv

5.1.4. Krybe, kravle, gå

En beredskabsplan er intet værd uden træning og øvelse. Jo hyppigere man træner eget beredskab, jo bedre er man rustet, når hændelsen rammer. Første skridt bør være at verificere, at det tekniske beredskab har den kapacitet, organisationen forventer. Udvælg et kritisk system og reetabler dette fra bunden over en weekend og tjek at integrationerne stadigt virker. Der plejer altid at være læring her – der mangler noget dokumentation, noget integration kan kun konfigureres, hvis en bestemt nøglemedarbejder deltager, det vides ikke om funktionsevnen er opretholdt efter reetablering, da der ikke er testcases forberedt osv. Dernæst gennemfør en workshop med it og forretning og dokumentér nødprocedurer – jeres quick fixes – og bliv klar over, hvad muligheden er for at opretholde delvis funktionsevne, hvis reetablering trækker ud, herunder ikke mindst, hvor lang tid I kan opretholde funktionsevnen med nødprocedurer. Endelig bør der være en beredskabskuffert med laptops, skriveredskaber, kontakter eller prokura og beredskabsplanen i print, så man med kufferten kan igangsætte kriseledelsen uden afhængighed af centrale it-funktioner.

Når det basale er på plads, skal planen trænes. Begynd med skrivebordsøvelser af to-tre timers varighed omkring ét konkret scenarie. Først internt i IT og derefter med forretning og IT. Forbered strategisk og taktisk kommunikation til intern kommunikation, til kunder og samarbejdspartere og offentlighed og få dem godkendt internt. Kommunikation, som dækker hjemmesider, mails, intranet og sociale medier, hvis den foretrukne kommunikationsplatform ikke er tilgængelig. Man kan som organisation købe sig to-tre timers ro ved tidligt at melde ud, "ja, vi er ramt af en hændelse. Vi er ved at undersøge omfanget. Vi vender tilbage om tre timer med yderligere information". Der er ingen grund til at opfinde det, når man står i krisen.

Med det basale på plads er I klar til at afprøve og træne beredskab i større kontekst med den strategiske ledelse, forretning og it og til at træne flere scenarier.

Se på eksemplerne og vurder, hvordan I i egen organisation ville håndtere en tilsvarende hændelse.

Område	Eksempel på spørgsmål til egen organisation	Eksempel på andres ulykker
IT Service Continuity Management	Et er, at I kan tage backup, men kan I reelt gennemføre restore i stor stil? Og er restore-rækkefølgen aftalt med forretningen?	https://www.computerworld.dk/fil/163243
Business Continuity Management	Kan I identificere de vigtigste data og systemer og opretholde kapacitet til at reetablere over flere dage?	https://www.maastrichtuniversity.nl/file/cyberattackresponseumfoxitmanagementsummary05-02-2020enpdf og https://ia.acs.org.au/article/2020/toll-group-recovers-after-ransomware-attack.html
Crisis Management	Har I et robust ledelsessetup for krisestyring, som giver plads til at operative teams kan reetablere, og til at kriseledelsen styrer den strategiske prioritering og kommunikation?	https://www.youtube.com/watch?v=C6MDz-AgQuE og https://www.youtube.com/watch?v=S-ZlVuM0we0 og https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

5. Det eksterne perspektiv

KRISØV – nationale krisestyringsøvelser

Hvert andet år deltager ministerier og styrelser med beredskabsansvar i en national krisestyringsøvelse (KRISØV).

Formålet med øvelsen er at træne myndighederne i de nationale stabs- og krisestyringsprocedurer. Hovedvægten lægges på tværgående koordination og samarbejde og på myndighedernes presse- og informationstjeneste.

Øvelsen tager udgangspunkt i en række hændelser, der kunne tænkes at finde sted eller har fundet sted i virkeligheden. Dette kunne for eksempel være terrorhandlinger eller miljøforureninger. Hændelsesforløbet er udstukket i en drejebog, der er udarbejdet af en tværministeriel øvelsesledelse.

Kilder:
https://brs.dk/beredskab/idk/krisestyringsoevelser/Pages/Krisestyringsoevelser.aspx og https://brs.dk/planlaegning/helhed/krisoev2019/Pages/default.aspx

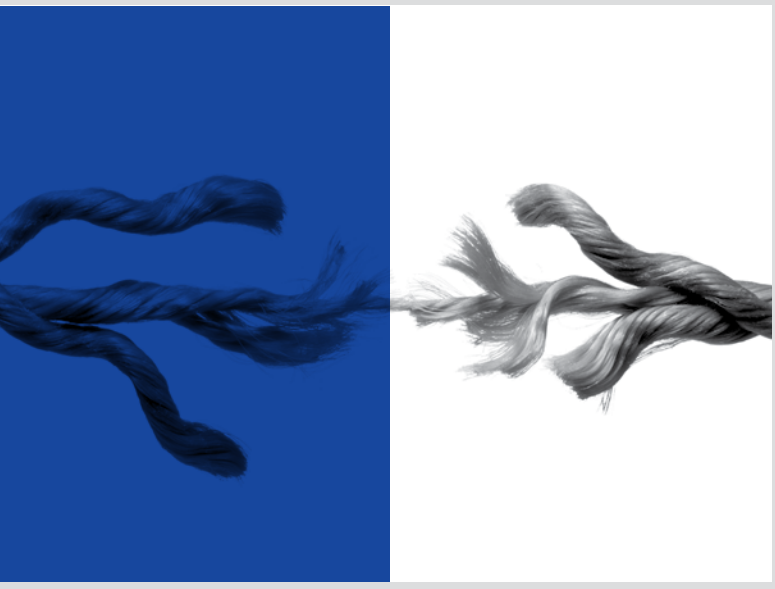
Internationale standarder inden for operational resilience.

- ISO22301 for Business Continuity Management
- BS11200 for Crisis Management
- ISO27031 for IT Service Continuity Management.

Kilder til yderligere information:
https://sikkerdigital.dk/myndighed/beredskabsstyring/

Beredskabsspillet:
https://sikkerdigital.dk/myndighed/beredskabsstyring/beredskabsspillet/

Pandora:
https://brs.dk/viden/publikationer/Documents/PANDORA%20-fremadskuende%20celle%20(BRS%20juni%202016).pdf



De mest modne organisationer supplerer deres beredskab med en såkaldt pandoracelle, som under krisehåndtering forsøger at forudse, hvordan hændelsen udvikler sig, og forbereder organisationen til at reagere hurtigere på hændelsen.

I takt med at flere organisationer bliver ramt af cyberhændelser, ofte som følge af komplekse it-miljøer, der ikke bliver patchet i tide, er det nødvendigt, at man som organisation tester og træner eget beredskab.

Start i det små, læg en plan for næste kvartal og få det basale på plads først. God træning.

5. Det eksterne perspektiv

5.2. EXERCISE OR THE REAL THING?

AF: ALF MOENS,
CORPORATE SECURITY OFFICER, SURFNET.

Just before Christmas 2019 Maastricht University was hit by a large ransomware attack. Hundreds of their Windows servers turned out to be encrypted, a number of their backups turned out to be useless.

The university quickly went into crisis mode and started analyzing and rebuilding. The Christmas period was both fortunate and unfortunate: No colleges but also no experts. It took the university 2 weeks to get the basic set of information systems running again, mid-January they were still struggling to get the last servers back online.

In 2016 the national research and education network for the Netherlands, SURFnet, launched a large cyber crisis exercise, called OZON, exactly to prepare universities for these kind of cyber crises. The aim of the exercise was to practice collaboration within and between universities with a 2-day life crisis simulation. The exercise included both technical challenges as well as board level dilemmas. As this exercise in 2016 was a great success SURFnet decided to make it a bi-annual recurring exercise with a far larger participation in 2018 and preparations underway for another large exercise in November 2020. The GEANT CLAW workshops are another spin off, of these exercises.

Next to the life exercises every other year SURFnet crafted less impacting exercises in the years in between, mostly table top and capture the flag exercises.

5.2.1. Knowledge is power, power to the people

OZON is a joined effort of SURFcert and SURFnet. In 2016 the main scenario focused on a hacking group that initially made propaganda for making all scientific research public available ("knowledge is power, power to the people"), for which a lot of participants were sympathetic. Soon the hacking group turned evil and started blackmailing universities for either making all research public or having all kind of personal data public, such as salary and private conversations of board members. All participating universities had made their own twist to the scenario as to which information was to be made public and what information systems proved to be hacked, just to make it more realistic for their own organization.

This scenario, as was the 2018 scenario, allowed for both technical challenges and board level dilemmas. At a large part of the participating universities the board also participated and they

5. Det eksterne perspektiv

were very serious about it. For some participating universities it was the first time a cyber crisis reached board level and both technical and managerial people worked on the same crisis.

The lessons learned from OZON 2016 turned out to be very useful when the Erasmus University Rotterdam was hit by a large cyber attack a month later. The attack was still serious but at least both IT staff and board level knew to find each other, were to start and what to do.

The most important lessons learned from OZON 2016 are for:

- The SURFcert team: They were stretched to the limits. As a part of the team was involved with organizing the exercise, part played a role (their own role) in the exercise and there still were normal security operations, things almost broke down in the team. CERT now learned in a pretty hard way that having just 1 person on call is not enough for handling crises. Shortly after they worked out an upscaling program where they can quickly scale up the team with both core team members and with other non-core security specialists when needed. With the cyber attack on Maastricht University Christmas 2019 the SURFcert team showed that they were well prepared and despite the holiday season were able quickly to scale up to crisis level. They stayed at crisis level for four weeks as the Maastricht crisis flowed into the Citrix crisis.
- For the universities: make friends in peace time. When there is a crisis you do not have time to figure out who you need to call.
- For SURFnet: Communication is serious business. The bottleneck in the crisis team at SURFnet proved to be a lack of communication resources. SURFnet needed to communicate to the universities, internal stakeholders, external stakeholders and at the same time stay friends with the press. Instead of the initial single communications officer in the crisis team, actually 3 were needed.
- For the education and research sector: Share information in an early stage and work together.

More information?
Read the whitepaper: OZON a gap-bridging exercise.
https://www.surf.nl/files/2019-02/whitepaper-cybercrisis-soefening-ozon-een-gap-bridging-exercise.pdf

Participants	OZON2016	OZON2018
Participating universities *	28	50
Players	200	1200
Preparation crew – core 8 months preparation	10	12
Preparation crew universities	30	60

* Universities, hospitals, regional teaching centers, research institutes

5. Det eksterne perspektiv

5.3. ET EFFEKTIVT OG OPERATIONELT BEREDSKAB SPARER TID

AF FREDERIK HELWEG-LARSEN,
EXPERT DIRECTOR, DEVOTEAM

Selv virksomheder, der har brugt mange ressourcer på cyber- og informationssikkerhed, bliver ramt af alvorlige hændelser, som kan standse alle aktiviteter. Det kan ramme os alle på trods af vores indsatser for at undgå det.

Vi kan blive ramt af udefrakommende cyberangreb og malware, vi kan blive udsat for strømsvigt eller oversvømmelser, eller måske er det simple fejl, som ender med at få alvorlige konsekvenser. Det er ikke muligt at beskrive alle scenarierne, og det bliver måske en hændelse, vi ikke havde forudset.

Hvis du har en beredskabsplan allerede, så brug denne artikel som en checkliste for, om du har husket det hele.

Lad dig inspirere af dem, som arbejder med beredskab i deres daglige arbejde, fordi det gælder liv og død: Politi, sundhedsvæsen, flytrafik og forsvar.

Her er omdrejningspunkterne i den gode beredskabsplan:

5.3.1. Struktur og agilitet med klart definerede roller

Grundelementet i ethvert effektivt beredskab er en klar fordeling af roller og ansvar. Brandmænd går ikke ind i en brændende bygning uden præcist at vide, hvem der gør hvad. Forsvarets effektivitet er baseret på klare principper for struktur og kommunikation, men med stor fleksibilitet i opgaveløsningen. Der er altså en vigtig balance imellem den faste struktur og den agilitet, vi skal udvise i en uforudsigelig krisesituation.

Ledelsen af en beredskabssituation er normalt mere håndfast og stringent end den daglige ledelse i virksomheden. Det kræver øvelse at styre et team igennem en struktureret mødeagenda i en situation, der er præget af uvished og stress. Derfor skal det trænes.

5.3.2. Beredskabsplanen skal være enkel

Når katastrofen sætter ind, og alt er kaos, skal du stå med alle nødvendige informationer i hånden, bogstaveligt talt, i papirform. Hvis det ikke er nødvendigt for organisationens arbejde, så bør man undgå teknologiske løsninger, når det gælder beredskab. Baseret på erfaringerne fra forsvar og sundhedsvæsen, så skal man forsøge at undgå kompleksitet, hvis det er muligt.

Til den analoge model hører også en tydelig verbal kommunikation, som er klar og præcis, så misforståelser minimeres. Denne form for kommunikation skal trænes, og det er ofte svært i starten. Husk at beredskab først og fremmest hviler på kommunikation mellem mennesker.

5.3.3. Klar og operationel opbygning

Beredskabsplaner bør altid starte med den operationelle del som det første. Alle forklaringer kan komme bagerst i planen som bilag. Det er der ikke brug for, når planen skal sættes i anvendelse.

Tydeliggør roller med farver, og angiv hvilke faser beredskabet er opdelt i. Dermed kan alle i beredskabsledelsen se, hvad de skal gøre på et givent tidspunkt, og alle checklister falder i hak med hinanden.

5.3.4. Træning, justering, træning

Den virkelige prøve finder sted i praksis, og derfor er træning, justering og atter træning det måske allervigtigste princip ved et beredskab. Hold hellere flere små scenarieøvelser, frem for nogle få store.

5.3.5. Det er planens anvendelse i praksis, der skal testes

Målet med øvelserne er ikke at opnå det bedst mulige resultat baseret på dagsformen, men at teste planens anvendelse i praksis. Hvis vi ikke tester planen, kan vi ikke gøre den bedre. Den skal virke hver gang, og ikke kun på en god dag. Du skal afprøve, om checklisterne kan sættes i praktisk anvendelse. Hvis noget virker ulogisk eller upraktisk, så er der behov for at justere. Det er på den måde planen forbedres og vi bliver bedre til at anvende den.

5. Det eksterne perspektiv

Hvad kan du selv gøre?

Hvis du er i tvivl om beredskabet i din virksomhed, er her nogle spørgsmål, du kan stille:

- Giver beredskabsplanen svaret på, hvad du konkret skal gøre i en krisesituation?
- Er ansvar og opgaver tydeligt fordelt?
- Er det tydeligt, hvad kriterierne er for at aktivere planen?
- Er planen opdelt i tid/faser?
- Er beredskabet kommunikeret internt, så det er klart, hvordan man alarmerer en hændelse?
- Er de forretningsmæssige prioriteringer afspejlet i planen?
- Er planen afprøvet inden for det sidste år med de personer, der er i beredskabsledelsen?

Anbefalet læsning: "The Checklist Manifesto", Atul Gawande.

5. Det eksterne perspektiv

5.4. MED PÅ CLAW-TRÆNINGSLEJR

AF: SIMON NEXØ JENSEN,
SIKKERHEDSANALYTIKER, DKCERT

En organisations krisehåndtering af cyber- og informationssikkerhed har visse paralleller til fodbold. Du er nødt til at have taktik, rolle- og ansvarsfordeling, strategi og masser af træning for at forøge din chance for at vinde.

På et fodboldhold skal man have en startopstilling, udpege en anfører, delegere ansvarsområde for hver kæde, lægge en taktik afhængig om modstanderen er FC Barcelona eller et hold fra 2. division. Du skal også have en plan, hvis du kommer bagud.

På samme måde har en organisationen en beredskabsplan. Organisationen har brug for at udpege en kriseleder, kende sine medarbejderressourcer og sørge for, at ansvar er delt fornuftigt, så organisationen kan reagere effektivt og hurtigt på alle fronter. Du kommer ikke langt med tre målmænd på banen.

Det næste er træning. Et hold skal kunne spille sammen. Roller skal indøves til de føles naturlige, og nye spillere skal finde deres plads i truppen. Øvelserne er ofte udformet af organisationen selv, eller med hjælp fra en ekstern leverandør. Det kan være alt fra gennemgang af procedure til fuldt simulerede kampøvelser. Det er ligesom med taktikken, en nødvendighed. Et godt sammenspillet og velfungerede hold kan ofte løfte sig langt over en håndfuld individuelle superstjerner.

5.4.1. Træning, øvelser, krise

I den erkendelse har GÉANT i de sidste tre år gennemført workshops – "træningslejre" - i krisestyring og beredskab for ansatte på de europæiske forskningsnet. DKCERT har deltaget i alle lejrene, der har fået navnet CLAW.

CLAW er tænkt som Europas træningslejr for beredskabsøvelser, hvor ansatte fra de nationale forskningsnet i hele Europa samles. Et sted, hvor forskningsnettene har mulighed for at tilmelde medarbejdere for at udvikle dem individuelt, i fællesskab og give dem erfaringer, de kan tage med hjem. Ambitionen er ikke, at alle skal arbejde efter deres egen beredskabsstrategi og -taktik hjemmefra, men at alle kommer på et hold fuld af forskellige kulturer og tilgange. Dét lærer man meget af.

Af flere årsager. Dels lærer deltagerne af hinanden, dels udvides ens forståelse i forhold til problematikkerne i krisehåndtering. Ydermere giver CLAW emnet et fokus, hvor det mange steder mangler starthjælp eller kørt fast i en ineffektiv rutine.

5.4.2. Hvad sker der i en CLAW?

CLAW er et to-dagesevent. Den første dag undervises der i forskellige temaer, som fx medarbejdernes håndtering af kriser og evne til at træffe beslutninger, som de ikke kan få clearet højere oppe, ekstern og intern kommunikation og håndtering af de stresselementer, der opstår under længere tids hårdt pres.

Den anden dag består af en interaktiv kriseøvelse. Den giver deltagerne mulighed for at tage første dags undervisning, samtaler og inspiration og se det komme i anvendelse under øvelsen.

Deltagerne bliver delt op i grupper. Grupperne består af medlemmer med erfaring for henholdsvis ledelse, PR, sikkerhed og netværk. Således har grupperne hver deres eget, lille forskningsnet. Hver gruppe skal så ved hjælp af kommunikation fra deres ledelse, PR og tekniske aktioner, valgt af deres sikkerheds- og netværksfolk, komme igennem en eventrig dag fuld af forhindringer, som hele tiden ændrer sig, ud fra hvordan gruppen agerer.

For at dette kan lade sig gøre har CLAW etableret sit eget land, Guilder Kingdom. Landet er kendt for sin stærke tradition inden for glaspusteri, det har sit eget sprog, en nationalsang, hovedstad og en række provinsbyer, hvis lokale, særegne universiteter med egen historie og traditioner er tilknyttet det nationale forskningsnet. Ministeren på området er en stærk personlighed, der sætter en ære i høj driftsstabilitet, og som fra tid til anden blander sig i sager, han ikke ved noget om.

Alene dette scenarie motiverer deltagerne i en sådan grad, at de kaster sig ind i øvelsen med liv og sjæl.

I CLAW bliver der lagt stort vægt på, at øvelsen er interaktiv, og at historien ændrer sig, ud fra hvad deltagerne vælger at gøre under krisen. Øvelsen afsluttes med en såkaldt hotwash-evaluering, hvor der debriefes, stressniveauet sænkes og erfaringer delt.

5. Det eksterne perspektiv

5.4.3. Konceptet CLAW

CLAW er et koncept, hvor der bliver tilrettelagt teoriundervisning og beredskabsøvelser i et miljø, hvor man for det første ikke kan fejle. Eller rettere: Man kan naturligvis godt fejle, men det får ikke konsekvenser. Det giver deltagerne frihed til at udforske handlemulighederne og drøfte løsningsrum, som er anderledes i ens egne øvelser.

For det andet øges deltagernes forståelse for egen kommunikation til andre grene af deres organisation. En af udfordringerne i CLAW-øvelsen er, at deltagerne skal videreformidle kritiske informationer på tværs gennem deres holds undergrupper, netværk, sikkerhed, kommunikation og ledelse. Den udfordring er en øjenåbner for mange, for det tvinger deltagerne til at bringe nogle kompetencer i spil, de ikke almindeligvis anvender i deres normale driftsarbejde. Og det belyser også, hvor de måske har mangler i forhold til deres egen træning.

For det tredje er der det at komme væk fra dagligdagens opgaver og have fokus på områder, man ikke altid prioriterer. Selv om der er beredskabsplaner hjemme, både på print, USB og i skyen, mangler mange stadig fokus på øvelser i en travl hverdag. CLAW prøver at give deltagerne lyst til at adressere behovet for egne beredskabsøvelser hjemme. Alt for mange får først gjort sig erfaringerne, når det er for sent.

5.4.4. Kold eller varm afvaskning

En krise kan opstå når som helst og kan i omfang svare til, at du en mandag morgen uden forberedelse bliver sat ind i en Champions League-finale, hvor du hverken kender modstanderen eller længden af kampen, og modstanderne spiller efter regler, du almindeligvis ikke forbinder med fodbold. Det eneste, du ved er, at du skal rykke hurtigt og være klar til løse opgaver, du ikke plejer at løse. Og at du er under konstant bevågenhed fra tilskuere, presse, ejere, interessenter og familien derhjemme.

At stå i sådan en situation er ekstremt lærerigt. Derfor gælder det om at være så godt forberedt som muligt. Det kan CLAW være en hjælp til. Spørgsmålet er, om du og dit hold er klar til at komme bagud allerede i første minut, når I ikke havde regnet med overhovedet at skulle spille fodbold?

Hvad er GÉANT?

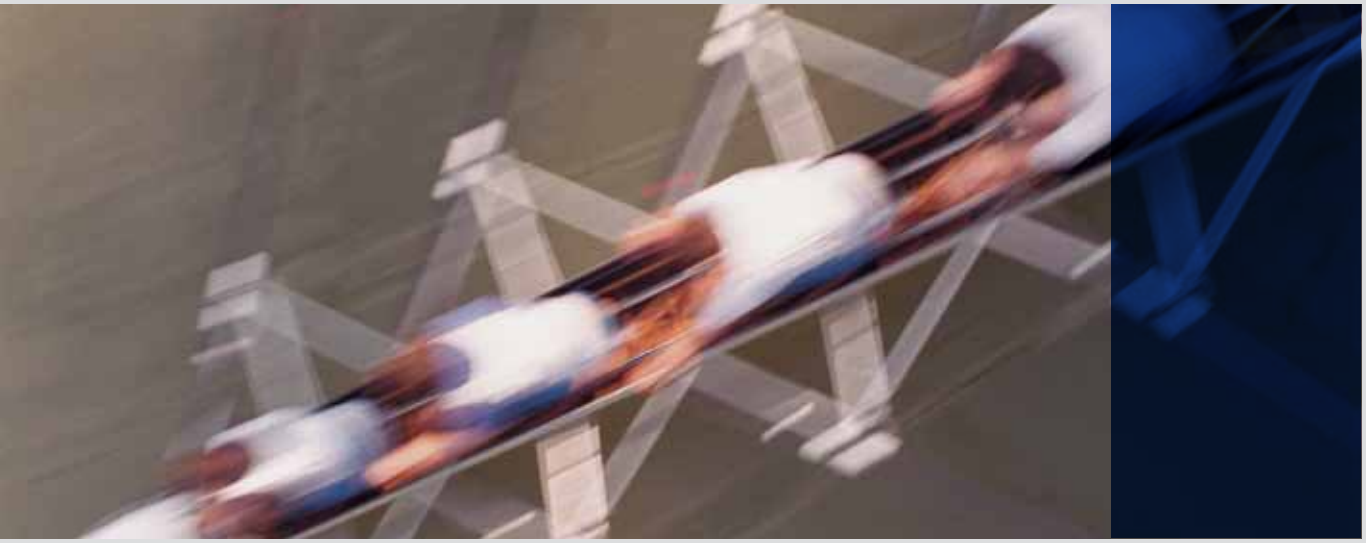
GÉANT er det fælleseuropæiske samarbejde om forsknings- og uddannelsesnet samt relateret infrastruktur og tjenester. GÉANT forbinder de nationale forskningsnet i Europa med hinanden, med forskningsnet i andre verdensdele og med det kommercielle Internet.

DeiC er medlem af GÉANT gennem NORDUnet, paraplyorganisationen for de fem nationale forskningsnet i Norden.
Se mere på https://www.geant.org/

DKCERT arrangerer en workshop i 2020

DKCERT har et ønske om at øge fokus på træning og undervisning. Derfor har vi arbejdet tæt med GÉANT og ydet bidrag til deres årlige CLAW workshop. Dette har givet DKCERT erfaringer og direkte overførbare værktøjer med hjem til at kunne tilbyde det i fremtiden til forskningsnettets tilsluttede institutioner. Vi håber derfor, at 2020 bliver året, hvor vi fra DKCERT side udfører de første øvelser og måske endda workshops for universiteter og andre institutioner på det danske forskningsnet.

5. Det eksterne perspektiv



5.5. SAMARBEJDE SKAL GØRE OS STÆRKERE, NÅR CYBERTRUSLEN RAMMER

AF: THOMAS LUND-SØRENSEN,
CHEF FOR CENTER FOR CYBERSIKKERHED

Danmark er ét af verdens mest digitaliserede samfund. Det er en af vores største styrker i den globaliserede verden, men det medfører også, at vi er afhængige af, at vores digitale tjenester fungerer. Det betyder, at datakommunikation er lige så vigtigt for Danmark, som at der er strøm i kontakten.

Når Danmark samtidig står over for en cybertrussel, som Center for Cybersikkerhed fortsat vurderer til at være meget høj, så er det overordentligt vigtigt, at vi kan reagere, hvis noget eller nogen gør alvor af truslen og forstyrrer vores digitale netværk.

Et vigtigt instrument i ethvert beredskab er overblik. Vi skal vide, hvad der sker og hvor, før vi kan prioritere vores indsats. I Center for Cybersikkerhed arbejder vi ihærdigt på at udbygge vores evne til at skabe overblik. Som led i den nationale strategi har Center for Cybersikkerhed fået til opgave at opbygge et nationalt cybersituationsbillede. Det skal hjælpe beslutningstagere, myndigheder og de dele af samfundet, som cybertruslerne rammer.

For at få overblik skal man kunne se, hvad der foregår. Derfor har et bredt politisk flertal med revisionen af lov om Center for Cybersikkerhed åbnet for, at virksomheder får lidt nemmere ved at bidrage med indblik i de aktuelle trusler. Konkret er betalingen for tilslutning til Center for Cybersikkerheds sensornetværk fjernet.

Samtidig er vi i færd med at indkøbe og implementere en ny enklere type sensor, som er egnet til at blive opstillet hos alle de myndigheder og virksomheder, der også er vigtige for vores samfund, men hvor det nuværende sensornetværk har været for specialiseret. Allerede nu mærker vi en god interesse for at deltage i netværket.

5.5.1. Bredere indblik

De nye sensorer giver ikke samme dybe indblik i de mest avancerede trusler, som vores egenudviklede sensorer. De placeres på ydersiden af netværket og lagrer ikke data i større omfang. Til gengæld vil de kunne give Center for Cybersikkerhed og de samfundskritiske sektorer (tele, energi, finans, sundhed, søfart, transport) og deres virksomheder overblik over det bredere spektrum af forsøg på angreb mod dem.

Herunder angreb fra cyberkriminelle, der også kan forvolde alvorlige afbrydelser i it-driften. Center for Cybersikkerheds situationscenter foretager teknisk monitorering af sensornetværket, holder øje med efterretningskilder og medier, modtager underretninger fra virksomheder og myndigheder og er desuden medlem af en række nationale og

5. Det eksterne perspektiv

internationale it-sikkerhedsnetværk for at få operative oplysninger om nye trusler og igangværende potentielt alvorlige cyberangreb med henblik på at skabe cybersituationsbilledet og varsle specifikt eller bredt om truslerne.

Data fra de nye sensorer bliver en vigtig brik i at skabe et nationalt overblik. En anden vigtig brik er samarbejdet med sektorerne selv. Her har oprettelsen af de decentrale cyber- og informationssikkerhedsenheder givet os et unikt redskab til at samarbejde og udveksle viden på et niveau, der allerede nu ser særdeles lovende ud. Samarbejdet udvikler sig hele tiden og bliver stadigt stærkere og operativt orienteret.

5.4.2. Løbende udvikling

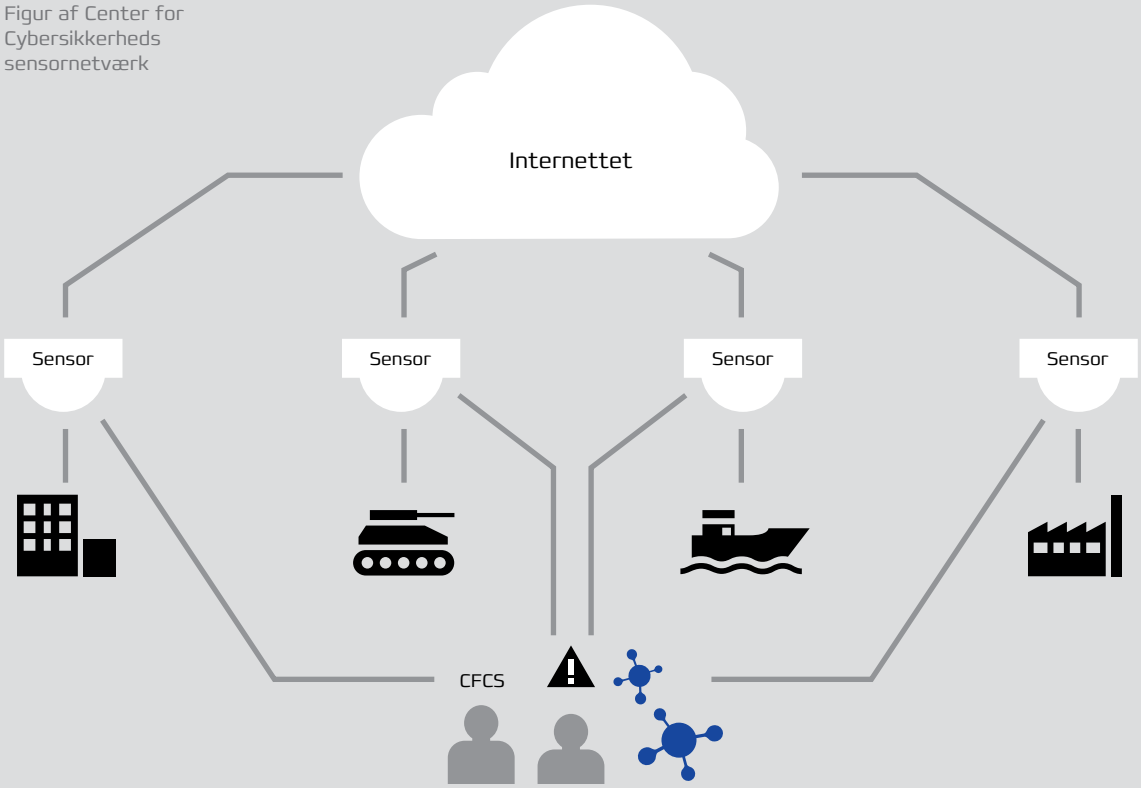
Vi ser, at cybertruslen løbende udvikler sig. I 2019 har vi set flere eksempler på målrettede ransomwareangreb, hvor virksomheder og myndigheder har været målet. Det er endnu en trussel, hvor det handler om at være forberedt, for det er vanskeligt helt at eliminere risikoen. Derfor skal man være parat til at håndtere, at netværket og de fleste enheder på netværket kan blive lammet. Har man en beredskabsplan, som alle kender, og har man øvet den, så har man en bedre chance for hurtigt at få organisationen på benene igen.

Det gælder især, hvordan man håndterer at være uden adgang til it-systemerne i en periode, mens der pågår reetablering af arbejdsstationer og netværk.

Truslen fra cyberspionage er også fortsat meget høj. Det er en trussel, der er kendetegnet ved, at angrebet kan stå ubemærket på gennem længere tid, og hvor deltagelse i Center for Cybersikkerheds eksisterende sensornetværk virkelig kan gøre en forskel.

Også her er det vigtigt at have beredskab for, hvordan man skal reagere, hvis man får mistanke om, at netværket er kompromitteret. I disse tilfælde skal man både kunne håndtere sin egen undersøgelse af, hvilke data der kan være tilgået og få undersøgt, hvordan angrebet er sket, så man kan lukke hullerne i de digitale forsvarsværker. Det kræver et køligt overblik, og derfor er det vigtigt at have en plan, før det går galt.

Figur af Center for Cybersikkerheds sensornetværk



6. Klummer af Henrik Larsen

6. Klummer af Henrik Larsen

Hver måned kommenterer Henrik Larsen, chef for DKCERT, aktuelle problemstillinger inden for informationssikkerhed.

Her bringer vi et udvalg af de klummer, som Henrik Larsen har skrevet til Computerworld i 2019.

6.1. TELESEKTORENS DCIS SKAL PLACERES HOS DKCERT

De 11 teleselskaber har valgt DKCERT som medspiller i deres kommende DCIS. Det samarbejde vil være til gavn for både telesektoren, universitetsverdenen og samfundet.

Den 15. maj 2018 blev National strategi for cyber- og informationssikkerhed en realitet, og derved kom der en samlet plan for Danmarks cyberforsvar. Den skal sørge for, at vores kongerige kan forblive trygt på trods af eksterne trusler mod den digitale infrastruktur.

Strategien indeholder blandt andet krav om sektorstrategier for samfundskritisk infrastruktur inden for sundhed, finans, tele, søfart, transport og energi.

Hver især skal disse områder opbygge Decentrale Cyber- og Informationssikkerhedsenheder (DCIS'er), der skal sikre informationsudveksling mellem sektorerne og Center for Cybersikkerhed samt forestå vedligeholdelsen af risiko- og sårbarhedsvurderinger.

Opgaven gribes an på forskellig vis, men i telesektoren har de 11 udpegede selskaber besluttet, at DKCERT skal bistå i udviklingen og driften af en Tele-DCIS.

6.1.1. Den gode danske forening

Teleselskaberne har, efter det gode danske princip, valgt at oprette en forening, hvor den stiftende generalforsamling blev afholdt den 15. marts. Her besluttede medlemmerne, at den kommende DCIS skal placeres hos DKCERT på DTU Campus i Lyngby.

Den beslutning blev vi selvfølgelig meget glade for og stolte over, samtidig med at dette faglige samarbejde kan blive til gavn for både telesektoren, samfundet og universitetsverdenen, som jo er vores hjemmebane.

DCIS-enheden bliver en decentral organisation under DKCERT, og ideen er at bruge det faglige miljø, der eksisterer hos os, til at udvikle og sparre med de nye folk, som skal drive telesektorens enhed. Vi har rigtig mange års erfaring med informationssikkerhed på forskningsnettet og ikke mindst et meget solidt netværk af sikkerhedsorganisationer i hele verden, som kan bibringe værdi.

Ligeledes er begrundelsen fra telebranchens valg, at DKCERT er neutral i forhold til politiske - og konkurrencemæssige interesser, hvor specielt det sidste kendetegner denne branche.

Arbejdet med at bygge sikkerhedsenheden er allerede godt i gang, og stillingsopslaget efter en leder af tele-DCIS'en udløber i dag fredag den 29. marts – så hvis du vil søge, har du travlt. Når fundamentet er på plads, vil der dog være behov for yderligere kræfter til enheden. Indtil da har telebranchen, CFCS og DKCERT et midlertidigt samarbejde om opgaven.

6.1.2. Sammen er vi stærkest

Som chef for DKCERT glæder jeg mig naturligvis, sammen med mine medarbejdere, til at være med til at løfte denne opgave, som vi er meget ydmyg overfor.

Men set i helikopterperspektivet så mener jeg også, at det er en meget stor ting, at sektorerne går sammen på tværs af selskaber og interesser for at styrke den nationale informationssikkerhed. I et digitalt samfund er det nemlig en forudsætning, at de kritiske tjenester kan levere varen – selv i kriser.

Ved at rykke tæt sammen kan vi langt bedre modstå de trusler, der hele tiden er mod vores nation.

Oprindelig bragt på Computerworld Online den 29. marts 2019.

6. Klummer af Henrik Larsen

6.2. KRIMINELLE ER KONSTANT PÅ JAGT EFTER HØJTSPECIALISERET VIDEN

Beskyttelse af forskningsdata er en vigtig opgave på universiteterne. Her er et eksempel på en konkret trussel og de redskaber, vi anbefaler for at undgå de kriminelles fiskeri efter oplysninger.

På forskningsnettet, hvor DKCERT holder øje med sikkerhedshændelser, oplever vi med jævne mellemrum, at ondsindede personer eller organisationer forsøger at kompromittere intellektuel ejendomsret og derved erhverve sig specialviden gennem tyveri.

Det samme gør sig naturligvis også gældende for mange af de vidensvirksomheder, som vi er så berømte for i Danmark.

Et helt konkret eksempel, som vi har observeret ad flere omgange, forekommer i forbindelse med en gruppe, der blandt andet er kendt under betegnelsen Silent Librarian. Gruppen jager oplysninger på universiteter og andre forskningsinstitutioner gennem phishing.

6.2.1. Den stille bibliotekar

I sikkerhedskredse har der været stor enighed om, at Silent Librarian har forbindelse til den iranske regering, og at dens formål er at stjæle værdier i form af viden fra universiteter over hele kloden.

Det er en aktiv gruppe, og det vurderes, at den har sendt bunkevis af phishing-beskeder til mindst 380 universiteter i mere end 30 lande gennem flere år. Gruppen arbejder i perioder og i alene i juli og august i år er der rapporteret angreb mod 60 universiteter.

Phishing er altså stadig roden til rigtig mange sikkerhedsudfordringer, når det handler om den intellektuelle ejendomsret.

6.2.2. Høje klikrater

Gruppens metoder er, som mange andre phishing-kampagner, ikke specielt sofistikerede, men ganske effektive. Maddingen i beskeden, der består af en engelsksproget mail, beder ofret om at logge ind på sin bibliotekskonto for fortsat at have adgang til ressourcen. Herefter sendes vedkommende til en falsk login-side og tappes for oplysninger.

Simpelt, men det virker. Vores egne tal fra de praktiske awareness-kampagner, som vi afvikler for institutionerne, viser, at det i nogle tilfælde er op mod en tredjedel, som åbner en phishing-besked, og en stor andel af dem går videre og klikker sig frem til en ofte tilforladeligt udseende indlogningsside. Det er naturligvis også derfor, at denne angrebsmetode stadig bliver benyttet i stort omfang: Den er simpel og den giver resultater.

I forbindelse med direktørsvindel og andre specialdesignede phishing-beskeder, der bruger endnu mere sofistikeret "social engineering", vil min antagelse være, at klikraterne er mindst lige så høje.

Beskyttelsen mod disse angreb er på den anden side også simpel – i hvert fald i teorien.

6.2.3. Awareness og kritisk sans

Vidensdeling blandt kollegaer og awareness blandt brugerne er et meget vigtigt punkt.

Gennem hele oktober har der eksempelvis været fokus på informationssikkerheden i form af national cybersikkerhedsmåned og disse oplysende tiltag, skal vi selvfølgelig fortsætte og følge op på hele tiden. Hvis der er mulighed for det, er interne phishing-kampagner også et godt værktøj til at teste effekten af awareness-indsatsen.

Desuden vil jeg gerne slå et slag for password-manageren. Et effektivt værktøj, der både gør det nemt og sikkert for brugeren, der kan få genereret lange og komplekse adgangskoder, som er unikke for hver enkelt tjeneste. Samtidig skal brugeren kun huske en adgangskode, som så til gengæld skal være lang.

Ydermere binder de fleste password-managere kodeordet sammen med sidens adresse for at kunne automatisere dit login. Dette styrker også sikkerheden, for hvis du møder en falsk side, vil den have en anden unik adresse og derfor ikke automatisk logge dig ind. Altså en lille alarmklokke om at dette ikke er det kendte domæne.

De lange og unikke adgangskoder gør livet virkelig surt for kriminelle, der i stor stil udnytter, at vi anvender de samme (nemme) adgangskoder på tværs af tjenester.

6. Klummer af Henrik Larsen

Sidst, men ikke mindst, er der de fem grundregler for, hvordan man undgår at blive fanget i phishing-fælden:

> Vær altid kritisk over for mails, hvor du ikke kender afsenderen.
> Kontroller altid den faktiske afsender-mailadresse. Passer mailadressens domæne med det navn, afsenderen giver sig ud for at have? Du kan stadig blive snydt, men har dog sorteret en hel del fra.
> Lad være med at klikke på links eller vedhæftede filer, selvom du er nysgerrig. Skriv i stedet selv adressen ind i adressefeltet og se efter, at den ser sandsynlig ud.
> Vær opmærksom på, at banker og myndigheder ikke beder om følsomme oplysninger via mail eller over telefon.
> Er du det mindste i tvivl, så slet beskeden, eller kontakt den formodede afsender for at få bekræftet, at de har sendt den pågældende e-mail, før du åbner den.

I forbindelse med beskyttelse af den intellektuelle ejendomsret er der naturligvis også en række andre foranstaltninger, der skal hjælpe med at holde nysgerrige væk. Eksempelvis forholdsregler om hvor data opbevares, hvordan data krypteres og andre sikkerhedspolitikker – mere om det en anden gang.

Men har du fået bugt med phishing, så er du nået langt.

Oprindelig bragt på Computerworld Online den 25. oktober 2019.

6.3. SÅDAN HAR VI SELV BYGGET EN SIKKER LOGIN-LØSNING

På de højere uddannelsesinstitutioner i Danmark kan man med ét enkelt password logge på 4.000 danske og globale tjenester. Her er forklaringen på, hvordan det virker.

En solid og sikker adgangskontrol er fundamentet for smidig kommunikation mellem mennesker, systemer og tjenester. Identifikation og autentifikation er de to grundlæggende elementer i informationssikkerhed, der skal håndteres på en både sikker og brugervenlig måde.

På de højere uddannelsesinstitutioner har vi løst den udfordring gennem en såkaldt føderation, som vi selv udvikler.

Hvis man slår "føderation" op i den Den Danske Ordbog, så lyder forklaringen, at det er "en sammenslutning af delstater med fælles regering og statsoverhoved". Men det kan også betyde et "partnerskab mellem to eller flere sikkerhedsdomæner, hvor man godkender hinandens brugere og giver dem adgang til de udvalgte systemer, der via føderationen stilles til rådighed". Og det er sagen her.

Helt skåret ind til benet er det en sammenslutning mellem tjenester og institutioner, hvor brugerne har adgang til alle (registrerede) tjenester med ét login, der kontrolleres af én instans.

De to store fordele ved denne model er, at (person-data)sikkerheden er høj, og at man kun skal logge på én gang, uanset hvor mange tjenester man tilgår. De ansatte og studerende slipper altså for at huske særskilte login¬oplysninger for hver webtjeneste, som de anvender uden for deres institution.

6.3.1. Godt for både it- og personsikkerheden

Vi kalder løsningen for Where Are You From (WAYF), hvilket samtidig er en ret præcis beskrivelse af, hvordan vi definerer brugeren i forbindelse med login.

Overordnet kan det sammenlignes med NemLog-in, som vi alle kender og anvender, dog med en afgørende forskel.

Hvor NemLog-in kan identificere dig som borger i det danske samfund, så er WAYF bygget til at benytte

6. Klummer af Henrik Larsen

arbejdspladsen eller studiestedet som udgangspunkt for autentificeringen (Where Are You From).

Vi opbevarer således ingen personoplysninger i løsningen. Det foregår på den enkelte uddannelsesinstitution, der så selv bestemmer kriterier og rettigheder. Det er ligeledes her, at brugeren forsynes med den login-profil, som WAYF forbinder med tjenesterne.

Er du eksempelvis studerende eller ansat på Københavns Universitet er det altså her, dine informationer opbevares, og din konto udstedes.

Når du har behov for at logge på en ekstern tjeneste, så overføres derfor også kun de data, der er strengt nødvendige. Det kan vi gøre, fordi universitetet indgår i føderationen, WAYF.

Det er et minimum af information, der udveksles, hvilket er godt for persondatasikkerheden. Kommunikationen sker samtidig via hardware-signering, hvilket giver en teknisk sikker løsning.

Samtidig slipper brugeren for at skulle oprette og huske forskellige passwords til hver webtjeneste, som ellers er vores anbefaling. Passwordet overføres slet ikke til tjenesten, så også her styrkes sikkerheden betydeligt.

6.3.2. En registrering giver adgang til 27 mio. brugere

Føderationen kræver naturligvis, at de eksterne tjenester registrerer sig i WAYF. Men når det er gjort, så er der adgang til tjenesten for alle de personer, som har et login – i hele verden. I runde tal svarer det til 27 millioner brugere heraf mere end 500.000 er i Danmark. Det skyldes at WAYF, der er en dansk føderation, også er medlem af den globale føderation for universitetssektoren, kaldet eduGAIN.

Brugerne på de danske uddannelsesinstitutioner kan, via WAYF, benytte omkring 275 danske tjenester og yderligere 3.500 globale tjenester. Hvis du har fået tildelt adgang til tjenesterne af dit studiested eller din arbejdsplads, kan de alle tilgås med ét enkelt password og login.

Omvendt er det også en meget enkel måde for en tjeneste at komme i kontakt med rigtig mange brugere i en arbejdsgang. For udbydere, der vil forbinde til forsknings- og undervisningsverdenen, har selvfølgelig de samme fordele ved at melde sig ind under føderationens fane.

Det er enkelt, sikkert og effektivt.

Oprindelig bragt på Computerworld Online den 26. april 2019.

6. Klummer af Henrik Larsen

6.4. LÆK, LÆK, LÆK. DATA DE ER VÆK

En af de største udfordringer for informationssikkerheden er data, der er kommet ud af kontrol. Datalæk rammer milliarder af mennesker, og den enkelte bruger må oftest bare stå og se på, at det sker. Her er, hvad du selv kan gøre.

Den 25. marts 2018 blev der med GDPR sat bødetakster og handlingskonsekvenser på fejlagtig håndtering af følsomme persondata. EU har sat fokus på, at borgerens data skal håndteres på en sober og sikker måde. Det er et skridt i den rigtige retning for at minimere sikkerhedsbrud, der afslører brugernavn og kodeord eller kontokortoplysninger.

Problemet med data, der falder i forkerte hænder, er nemlig et af tidens helt store informationssikkerhedsproblemer. Der er selvfølgelig flere niveauer af datalæk, hvor de værste kan medføre, et din digitale identitet bliver misbrugt af kriminelle til eksempelvis økonomisk kriminalitet.

Og som bruger er du både dårligt - og godt stillet, når dine data er sluppet ud.

6.4.1. Brugeren må bare se på

I forhold til datalæk så opstår bruddet oftest hos en tjeneste eller e-butik, der opbevarer informationerne. Sikkerheden omkring opbevaringen er således tjenestens ansvar. Her er brugerens eneste mulighed at have tillid til de tjenester, der anvendes, hvilket dog kan være ualmindelig svært at vurdere, da sikkerhedsbrud rammer bredt. Her er et par eksempler:

I 2018 var nogle af de største datalæk fra hotelkæden Starwood, der er en del af Marriot-kæden, fitness-appen, Fitness Pal, der ejes af sportsvirksomheden Under Armor, samt sociale medier som Facebook, der havde problemer med 147 millioner konti i forbindelse med tre forskellige episoder. Den mest omtalte var nok den, der ramte analysefirmaet Cambridge Analytica, der er sat i forbindelse med det amerikanske valg.

Inden for vores grænser blev terapi-portalen GoMentor trukket frem i lyset for problemer med sikkerheden i forbindelse med brugernes data, og butikskæden Bahne måtte informere kunderne om, at et sikkerhedshul i online-butikken potentielt kunne føre til misbrug af betalingsoplysninger og kreditkort.

Datalæk kan også fremkomme ved stjålne eller tabte enheder og behøver ikke nødvendigvis være i form af indbrud i it-systemer. Det har vi set flere gange.

Det er således nærmest umuligt at give gode råd om hvilke tjenester, man skal holde sig fra og hvilke, der er sikre. Datalæk kan ramme alle, og hyppige datalæk må også forventes fremover.

6. Klummer af Henrik Larsen

6.4.2. Et par gode råd til dig

Ifølge Datatilsynet er der indberettet mere end 3.000 danske sager om sikkerhedsbrud fra GDPR-starten til slutningen af januar 2019. Det er positivt, at vi på grund af GDPR-implementeringen hører mere om de lækager, der finder sted, hvilket giver bedre mulighed for at reagere og samtidig sætter nødvendigheden af sikker opbevaring af data på dagsordenen.

Noget af det du, som almindelig bruger, kan være opmærksom på, er gode password-vaner. Separate passwords til hver tjeneste er et nøglepunkt i forhold til datalæk. Husk også at skifte din adgangskode, hvis den tjeneste du anvender, er blevet kompromitteret, og hav omtanke for hvilke data du afgiver og til hvem.

Sidst men ikke mindst skal du holde øje med dine bankkonti, og anvend gerne de muligheder som banken giver eksempelvis i form af en besked, hvis der sker større transaktioner på dine konti.

6.4.3. Og nu til det gode

Alt er dog ikke slemt. Hvis lækkede oplysninger anvendes til økonomisk kriminalitet, så er du nemlig udmærket dækket i forhold til økonomiske tab.

Hvis du oplever, at dit betalingskort bliver misbrugt af andre, er det som regel banken, der dækker tabet. Nogle gange er der dog en selvrisiko, afhængig af omstændighederne. Men husk, at banken hæfter for misbrug, der er foretaget, efter du har givet besked om, at kortet er blevet væk, at en uvedkommende har fået adgang til koden, eller du af andre grunde har ønsket at få kortet spærret.

Vi slipper nok aldrig af med datalæk, men hvis vi forbereder os godt, er opmærksomme og holder fokus på udfordringerne, kan vi langt hen ad vejen håndtere problemet.

Men det er en fælles indsats, hvor alle skal bidrage.

Oprindelig bragt på Computerworld Online den 22. februar 2019.

6.5. OVER 200.000 DANSKERE HAR MISTET PENGE PÅ NETTET I 2018

Overskriften er bare et enkelt eksempel fra rapporten med navnet Danskernes informationssikkerhed 2018, hvor vi har spurgt danskerne om it-sikkerheden. Her er tendenserne.

DKCERT har i flere år gennemført en statistisk undersøgelse af danskernes informationssikkerhed. I 2018 har vi gjort det i et samarbejde med Digitaliseringsstyrelsen, KL og Danske Regioner.

Formålet med at spørge danskerne om sikkerhed og samle besvarelserne i en rapport er at afdække, hvilke sikkerhedshændelser borgere og ansatte i det offentlige bliver udsat for, samt belyse deres viden om informationssikkerhed og deres evne til at beskytte sig mod udbredte trusler.

Eller kort: At tage temperaturen på informationssikkerheden.

6.5.1. Her er et par af tendenserne

Vi har ladet Danmarks Statistik stille mere end 100 spørgsmål til borgere og offentligt ansatte, så der er rigtig mange tal i rapporten, der i mange tilfælde kan sammenlignes med de tidligere år. I denne klumme har jeg udvalgt et par stykker, der handler om borgernes svar, så du kan få en fornemmelse af, hvordan sikkerhedshverdagen ser ud blandt almindelige danskere.

Det første er allerede præsenteret i overskriften og spørgsmålet er: Har du mistet penge, eksempelvis ved online-svindel eller afpresning?

Det svarede otte procent ja til.

Selv om procenttallet ikke er stort, så bliver det faktisk til en hel del danskere. Når man ganger tallet op på hele befolkningen (i aldersgruppen mellem 18 og 74 år), er det nemlig mere end 200.000 borgere, som har mistet penge ved online-svindel.

Fem procent af borgerne kunne desuden berette, at de havde fået misbrugt personlige oplysninger.

Tilbøjeligheden går desværre også i retning af, at flere bliver ramt af it-sikkerhedsproblemer. 34 procent - eller cirka en million borgere - oplyste

6. Klummer af Henrik Larsen

således, at deres computer havde været inficeret med virus eller andre typer skadelige programmer.

Samlet set har 44 procent, eller cirka 1.200.000 borgere i alderen 18 til 74 år, været udsat for mindst et af fire sikkerhedsproblemer: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data.

Det er en stigning fra 34 procent i forhold til den sidste rapport fra 2016.

Det er tankevækkende og fortæller, at der er behov for, at vi bliver bedre til informationssikkerhed. Det skal eksempelvis Digitaliseringsstyrelsens Sikkerdigital.dk-projekt være med til at rette op på, og i DKCERT gør vi selvfølgelig også vores bedste for at oplyse om informationssikkerheden.

6.5.2. (Lidt) bedre til adgangskoder

Vi har også spurgt om, hvor lange adgangskoder danskerne har, og her svarer 75 procent, at deres koder er mellem seks og ti tegn. 18 procent har over 11 tegn, mens tre procent anvender mellem et og fem tegn.

Det er i underkanten af, hvad de nye anbefalinger til et godt password er. De siger nemlig, at lange passwords, på mindst 12 karakterer, giver højere sikkerhed. Det betyder mindre om de indeholder specialtegn, store bogstaver og lign.

Et andet vigtigt element i forhold til adgangskoder er, at de ikke anvendes på tværs af tjenester, og her er der sket en markant forbedring blandt borgerne. En positiv tendens.

37 procent anvender samme adgangskode til flere online-tjenester. 24 procent af dem svarer dog, at det kun er til tjenester, der ikke håndterer følsomme data.

De 37 er stadig et højt tal, men det er en klar forbedring i forhold til rapporten fra 2016, hvor 66 procent anvendte samme password til flere tjenester, der er altså sket et markant fald, hvilket er positivt. Det skal vi arbejde på at få mere af.

6.5.3. Læs mere og bliv klogere

Informationssikkerhed er bestemt af mange faktorer, og som eksemplerne viser, er der både frem- og tilbagegang. Hvis du vil vide mere, så dyk ned i rapportens tal. Der er mange spændende data om informationssikkerheden i Danmark direkte fra dem det handler om, nemlig brugerne af it.

Du kan finde Danskernes informationssikkerhed her: https://www.cert.dk/da/information/borgernes_informationssikkerhed

Oprindelig bragt på Computerworld Online den 29. januar 2019.

7. Fremtidens trusler og trends

Kriminelle er på evig jagt efter nye angrebsplatforme, og den kritiske infrastruktur står i orkanens øje i 2020. Et år hvor DKCERT også forventer fokus på Business Continuity-planer og flere tiltag i forbindelse med uddannelse af brugerne.

7.1. TRUSLER MOD INFORMATIONSSIKKERHEDEN I 2020

7.1.1. Angreb mod kritisk infrastruktur

Forsyningsselskaber og anden kritisk infrastruktur er fortsat et oplagt mål for cyberangreb. I 2019 har eksempelvis amerikanske forsyningsselskaber været ramt af udfordringer.

Tendensen underbygges af trusselsvurderingerne fra de samfundskritiske sektorer og Center for Cybersikkerheds samlede trusselsvurdering. DKCERT har i 2019 udarbejdet en trusselsvurdering for universitetssektoren, der ligeledes bekræfter dette billede i universitetsverdenen.

Udfordringerne kan eksempelvis være i form af gammel teknologi, som kriminelle nemt kan kompromittere, og som kan være svær at opgradere til nye og sikre udgaver på grund af specialtilpasning.

Cybersikkerheden i forbindelse med den kritiske infrastruktur er derfor et højprioritetsområde for 2020.

7.1.2. Ransomware, phishing og malware

Phishing, ransomware og malware udnyttes med ønske om økonomisk vinding, ud fra politiske motiver og i forbindelse med destruktive angreb – eller i en kombination af disse elementer. Angrebsmetoderne er ikke nye, men de er fortsat et af de øverste punkter på dagsordenen i 2020.

Ransomware:
I 2019 kunne vi erfare, at ransomware i stigende grad blev målrettet mod udvalgte virksomheder, myndigheder og sundhedsorganisationer. Angriberne anvender ofte social engineering - indsamling af oplysninger om mål/personer - for at forsage maksimal skade i forbindelse med et angreb. Bekymringen er, at de organisationer, der rammes, fristes til at betale løsepenge for at undgå nedetid. Hvis denne situation opstår, vil det give en selvforstærkende effekt og derved flere ransomware-angreb.

Phishing:
E-mail var i 2019 den foretrukne platform til at udføre phishing-angreb, men de kriminelle forsøger sig i stigende grad med nye åbninger til at snyde sine ofre. I 2020 kan vi således forvente en stigning i antallet af sms-baseret phishing via telefonen også kaldet smishing, angreb via sociale medier eller eksempelvis spilplatforme.

Malware:
Også på dette område kan vi se en tendens til, at computeren ikke nødvendigvis er den primære angrebsflade. Ifølge sikkerhedsvirksomheden Check Point bød det første halvår af 2019 på en stigning på 50 procent i antallet af angreb, i forhold til samme periode 2018, fra mobile banking malware. Det vidner om, at der er stor interesse fra kriminelle for at finde nye angrebsplatforme til at stjæle betalingsdata, legitimationsoplysninger og penge fra ofrene.

7.1.3. Sikkerheden i 5G netværket

Vi står på tærsklen til udrulningen af 5G i Danmark, og sikkerheden i den kommende teknologi er et yderst vigtigt område.

Truslerne fra ondsindede personer, organisationer eller stater kan blive høj da angrebsfladen vil blive mange gange større, når 5G kan anvendes til at forsyne 'alt' med internet.

Det betyder eksempelvis at nye IoT-enheder, som en termostat på kontoret eller i hjemmet, kan være angrebsfladen for en kriminel, der kan misbruge den til eksempelvis et DDoS-angreb.

Udfordringerne ligger i at skabe et sikkert økosystem med end-to-end-sikkerhed og i den forbindelse bliver automatisering en vigtig faktor. Her vil kunstig intelligens og maskinlæring spille en ny rolle for informationssikkerhed.

Begejstringen for høj hastighed, nye forretningsområder og nemt adgang til netværk må ikke stå i vejen for informationssikkerheden. Det vil få alvorlige konsekvenser.

7. Fremtidens trusler og trends

7.2. SIKKERHEDSTRENDS I 2020

7.2.1. Awareness, fejl 40 og GDPR

I 2019 blev der sat rigtig mange gode awareness-programmer i gang (læs mere om det under punktet: Tendenser og trusler i 2019). De vil følge os ind i 2020 og forhåbentlig bære frugt i form af bedre uddannede brugere.

Der har eksempelvis været afholdt den første nationale cybersikkerhedsmåned samt udgivet undervisningsmateriale til både unge og uddannelsesinstitutioner, til bestyrelser og til offentligt ansatte.

Ligeledes er der sat fokus på konkrete områder som dataetik, industrielle kontrolsystemer og Internet of Things (IoT), hvilket er en meget positiv tendens.

Men en af de største trusler finder vi stadig bag firmaets egne fire vægge i form af medarbejdere, der ikke overholder/kender sikkerhedspolitiker eller måske agerer på egen hånd, fordi det kan lettet arbejdsopgaven, hvis sikkerheden springes over.

I 2020 vil der derfor igen blive sat fokus på uddannelse af brugere - ikke mindst på grund af GDPR og de konsekvenser, disse regler kan medføre.

7.2.2. Forretningen skal køre - Business Continuity

Temaet for årets Trendrapport er krisehåndtering, og når angrebet eller nedbruddet kommer, er det vigtigste punkt på dagsorden at få forretningsdriften op at køre hurtigst muligt, så de negative konsekvenser holdes på et minimum.

Nedetid koster nemlig både på bundlinjen og på goodwill-kontoen, hvilket der er flere eksempler på fra 2019. Og de erfaringer vil stadig være på dagsordenen i 2020.

Det er derfor helt vitalt at have en beredskabsplan, som straks kan iværksættes, når uheldet er ude. Der skal tages højde for mange ting, og den kræver således, at du har styr på dine data, dit data flow og dine processer så alle ved, hvad de skal gøre.

Forretningskontinuitetsplanlægning er processen med at skabe systemer til forebyggelse og gendannelse for at håndtere potentielle trusler mod en organisation. Ud over forebyggelse er målet at muliggøre løbende operationer før og under udførelse af katastrofegendannelse.

7.2.3. Fake news og "beskidte data"

Selv om det amerikanske præsidentvalg foregår på et helt andet kontinent, kan det – set i lyset af sidste valg – komme til at betyde, at nettet vil blive ramt af bølger af falske informationer og uægte/beskidte data.

Der er i denne forbindelse risiko for, at datasæt og nyhedshistorier er unøjagtige, partiske eller direkte forkerte. Da datadreven beslutningstagning fra kunstig intelligens og algoritmer bliver mere udbredt, vil der i 2020 komme et øget behov for (offentlig) kontrol af udgivelsesplatformene.

8. Anbefalinger

I dette kapitel kommer DKCERT med anbefalinger, der har til formål at øge informationssikkerheden i den akademiske verden. DKCERT har udarbejdet to sæt anbefalinger til uddannelses- og forskningsinstitutioner. Det første er rettet til de it-ansvarlige, det andet til ledelsen.

8.1. 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. Forlang ledelsens aktive involvering 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.
4. Hav fokus på sikkerheden ved udvikling af applikationer og tjenester samt tilretninger af eksisterende systemer.
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, når de anvender dem til arbejds- eller studieformål.
7. Effektiviser 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. Indfør whitelisting af de applikationer, brugerne må køre.
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. 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 password manager til brugerne.
17. Undervis brugerne i sikkerhedsrisici og forholdsregler.

8.2. 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.
2. Tænk risiko og sikkerhed ind fra starten i udviklingen af produkter og tjenester.
3. Gør det tydeligt, at ledelsen er aktivt involveret i arbejdet med informationssikkerhed.
4. Før tilsyn med overholdelse af databeskyttelsesforordningen.
5. Hold de ansatte, studerende og gæster informeret om informationssikkerhedspolitikken og aktuelle problemer.
6. Etabler et beredskab, udarbejd en beredskabsplan for kritiske hændelser og hold øvelser.
7. Prioriter og synliggør risikostyring.
8. Foretag løbende risikovurderinger af forretningskritiske systemer.
9. Afsæt ressourcer til uddannelse og kompetenceudvikling for alle medarbejdere i informationssikkerhed.
10. Arbejd sammen med andre institutioner om informationssikkerhed, del viden og erfaringer.
11. Afsæt tid, penge og personale til håndtering af informationssikkerhed.

9. Trusselsvurdering

Cybertruslen mod den danske uddannelses- og forskningssektor 2019.

En trusselsvurdering har til formål at hjælpe organisationer med at kende og forstå deres modstandere i cyberspace, så de bedre kan vurdere den risiko, som aktørerne udgør, og så de bedre kan forsvare sig mod dem.

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 DKCERT's 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.

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 muligt, 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 awareness vedrørende truslen og konsekvenserne heraf, hvilket øger sandsynligheden for menneskelige fejl, uanset om disse er bevidste eller ubevidste.

Det er dog samtidig vigtigt at være opmærksom på forskellen mellem de tre trusler, der alle klassificeres som meget høj. Alle tre opfylder kravene til klassificeringen, men der er stor forskel på de tre trusler. Cyberspionage er normalt lange operationer, der går efter et begrænset mål. Angriberne forsøger at undgå at blive opdaget og konsekvensen er oftest ikke en, organisationerne oplever med det samme. Truslen fra cyberkriminelle og fra insidere er derimod hændelser, der ofte kan påvirke den daglige drift, og derfor kan have til umiddelbare konsekvenser for organisationerne.

9. Trusselsvurdering

INDLEDNING

Hvad er cybertrusler?

DKCERT har hentet data fra The Verizon 2019 & 2020 Data Breach Investigations Report (DBIR) som baggrundsinformation til denne trusselsvurdering.

DBIR er en årlig rapport, hvor Verizon har analyseret mere end 40.000 sikkerhedshændelser og fordelt på både trusselstype, sektor og motivation for angrebet.

Denne trusselsvurderingen 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 forskningssektor har en samfundsvigtig rolle i Danmark, men er ikke defineret som samfundskritisk i den Nationale Strategi for Cyber og Informationssikkerhed[1]. Cyberangreb mod den danske uddannelsessektor kan få betydning for samfundets funktion, stabilitet og velfærd. Det er derfor vigtigt, at denne trussel håndteres, 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 enkelt forskere.

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.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede og har en varslingshorisont på op til et år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Der er ingen tvivl om, at cybertruslerne er et stadigt stigende problem for den danske uddannelses- og forskningssektor. I 2019 steg det samlede antal ondsindede digitale "objekter", som Kaspersky registrerede med mere end 13% til over 24 millioner[2]. Samtidig med at uddannelsessektoren på verdensplan var en af de to sektorer, der blev udsat for flest cyberangreb i 2018[3].

Hackere kan både være statsstøttede APT'er, som ofte har et meget smalt og veldefineret fokus, og som i udgangspunktet ikke ønsker at gøre opmærksom på deres tilstedeværelse. Det kan være kriminelle, der ønsker at skabe så meget opmærksomhed som mulig, således at organisationerne bliver presset til at betale for at komme af med de kriminelle. Det kan også være en kombination af de to, som det muligvis var hos en dansk virksomhed, der ifølge CFCS blev hacket fem gange på to år via en sårbarhed, som havde været mulig at opdatere og dermed sikre sig mod i mere end seks år. I det konkrete tilfælde har Center for Cybersikkerhed udarbejdet et undersøgelsesrapport, hvor det vurderes, at virksomheden blev kompromitteret af fem hackere, der handlede uafhængigt af hinanden. Alle udnyttede samme sårbarhed, men havde forskellige formål med kompromitteringen[4].

9. Trusselsvurdering

Sårbarhedsscanninger

I 2019 viste DKCERT's sårbarhedsscanninger 3.431 unikke sårbarheder. Risikovurderingerne i forbindelse med de eksterne scanninger fortæller, at syv procent af sårbarhederne er kritiske, 29 procent er høj, 55 procent er middel og ni procent er lav.

Advarsler fra tredjeparter

I 2019 udsendte DKCERT 37.308 advarsler fra tredjeparter. Denne service, som blev introduceret i slutningen af 2014, giver institutionerne på forskningsnettet advarsler om potentielt sårbare systemer på deres netværk. Advarslerne kommer fra tredjeparter, der løbende scanner internettet for kendte sårbarheder, som angribere kan udnytte.

Hverken tallene for sårbarhedsscanninger eller for advarsler fra tredjeparter siger dog noget om, hvorvidt angribere har forsøgt at udnytte sårbarhederne.

CYBERSPIONAGE

Danske myndigheder og virksomheder er løbende 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 den danske uddannelsessektor. Det er sandsynligt, at fremmede stater særligt har interesse i de dele af uddannelsessektoren, der har adgang til forskningsdata eller intellektuel ejendom.

Et grelt eksempel fra 2019 på omfattende cyberspionage er historien om en højstående medarbejder i Department of Homeland Security, der havde fremskaffet en kopi af kildekoden til et internt Enforcement Database System. Denne kode havde medarbejderen solgt videre sammen med en kopi af de 150.000 interne undersøgelser som Department of Homeland Security var i gang med samt personoplysninger på 250.000 ansatte.

Cyberkriminelle er ligeledes ude efter uddannelsessektorens data, da sektoren rummer en stor mængde data, som kriminelle kan udnytte til afpresning eller sælge. Disse data er fx forskningsdata eller informationer om udstyr eller produkter anvendt i sektoren. Nogle cyberkriminelle forsøger at afpresse organisationer ved at true med at frigive data, de har fået adgang sig til.

I sommeren 2019 og igen i starten af 2020 var der indikationer på et iransk-baseret angrebsforsøg mod biblioteksressourcer hos flere universiteter, herunder også danske universiteter. Det er den iranske gruppe Silent Librarian, der mistænkes for at stå bag. Efterfølgende oplysninger har dog tydet på, at der muligvis er tale om russiske aktører, der alene bruger Iran som et dække for deres aktiviteter [5], eller en kombination af begge. Dette skete samtidig med et andet angreb, hvor mere end 60 universiteter på verdensplan var omfattet af angrebet [6].

Mens det omtalte cyberangreb har været rettet mod forskningsinstitutioner i flere lande, kan det danske forskningsmiljø i sig selv være interessant for fremmede stater. Dansk forskning er i skarp international konkurrence om at komme først med

9. Trusselsvurdering

forskningsresultater, sikre finansiering og rekruttere de bedste forskere og studerende. Danske forskere leverer også viden, som udgør en del af grundlaget for de politiske valg, regering og Folketing træffer. Fremmede stater kan også have interesse i at få adgang til eksempelvis it-infrastrukturer eller følsomme person data, som forskningsinstitutionerne administrerer.

Et nyere tilfælde drejer sig om et Password Spray Attack (Brute Force), der stod på i ca. seks måneder i løbet af 2018 og 2019 og var rettet mod danske uddannelsesinstitutioner. Dette angreb kan både være cyberkriminalitet og cyberspionage, men vedholdenheden i angreb kan tyde på, at en statslig aktør har stået bag.

Et af 2019's mest interessante sikkerhedsbrud inden for uddannelsessektoren var sandsynligvis da Australian National University i juni offentliggjorde opdagelsen af en avanceret ekstern operator i universitets systemer, hvis første adgang kunne spores tilbage til slutningen af 2018. Der har i angrebet været adgang til alle ansatte, studerende og gæsters personoplysninger fra de seneste 19 år [7]. Ligeledes afsluttede FBI i 2018 en undersøgelse af et angreb målrettet uddannelsessektoren i USA og en lang række andre lande. Det var et angreb, hvor forskere på 144 amerikanske universiteter og 176 universiteter i andre lande, herunder Norge og Danmark, modtog en mail fra tysk kollega, der efterspurgte nogle publikationer. I den mail var der et link til en hjemmeside, der var præcis kopi af deres eget universitets log-on side. Ved indlogning på denne kopiside kunne forskernes brugernavn og adgangskode blive stjålet, hvilket også skete.

Yderligere oplever danske universiteter ofte kompromitterede studenter- eller ansattes konti, der efterfølgende anvendes til udsendelse af phishing af typen "Your mailbox is set to expire..." internt i mailsystemet og derfor på indersiden af spamfilteret. Her er det antagelsen, at den initiale kompromittering sker ved hjælp af phishing-mails, hvor særligt udvekslingsstuderende er ramt. Dette kan skyldes de kulturelle forskelle og sproglige barrierer, der gør, at udenlandske studerende og ansatte kan have svært ved at skelne mellem phishing-mails og legitime mails.

Cyberspionage mod uddannelsessektoren vil højst sandsynligt være økonomisk motiveret, men kan også være politisk motiveret. Spionagen kan bl.a. skaffe viden, der kan bruges til at komme i besiddelse af nye teknologier til at styrke og udvikle egen industrier og sektorer, eksempelvis inden for udvikling af grøn teknologi, sundhedsviden eller innovation inden for andre områder, der kan have interesse fra fremmede magter.

Selvom det oftest vil være stater, der står bag reel cyberspionage, så er der en tydelig udvikling, hvor de kriminelle bliver mere og mere sofistikerede i deres angreb, og i hvordan de får en finansiel gevinst ud af deres angreb. CFCS advarer netop mod, at de kriminelles angreb bliver mere avancerede og forårsager større skade, når de lykkes med at kompromittere en person eller et system[8].

Cyberspionage mod fx intellektuel ejendom fra uddannelsessektoren udgør en samfundsøkonomisk trussel mod Danmark og kan skade danske interesser. Tyveri af følsomme personoplysninger om danskerne fra forskningsprojekter kan skade danskernes tillid til, at sektoren kan håndtere deres data på en sikker og forsvarlig måde. Tab af tillid kan udfordre sektorens mulighed for at drive forskning på de hidtidige, kendte vilkår, som i kraft af en høj grad af digitalisering af det danske samfund har skabt en styrkeposition for danske universiteter i konkurrence med andre lande.

Truslen fra cyberspionage mod enkeltdele af den danske uddannelses- og forskningssektor afhænger af, hvilken og hvor meget data myndigheden eller virksomheden har adgang til. Det danske uddannelsesvæsen er dog meget digitaliseret og forbundet, så en aktør kan angribe en sårbar del af sektoren i forsøget på at få adgang til andre mål.

Ud over angreb, der oftest sker via phishing, er der også registreret brute force angreb. DKCERT's sårbarhedsscanninger har også vist, at mange uddannelsesinstitutioner stadig bruger standardkonfigurationen, som udstyr kommer med fra leverandøren. Dette øger sårbarheden for udstyret betydeligt, da disse konfigurationer ofte er kendte, og derfor nemmere at komme udenom i forbindelse med forsøg på kompromittering udefra.

9. Trusselsvurdering

Nogle af de mest udbredte sårbarheder, der er fundet blandt danske uddannelsesinstitutioner, som er baseret på manglende eller forkert konfiguration er:

- Standard ID og password (eks. SNMP Community String)
- Ingen input validering (eks. SQL injection og cross-site scripting)
- Tillader ikke valideret adgang (eks. Directory traversel)
- Tillader forældet krypterings standarder (eks. sweet32)

Leverandørvinklen

Cyberspionage mod uddannelsessektoren kan også foregå ved angreb på en leverandør. Hackerne kan enten udnytte leverandøren til at opnå adgang til det egentlige mål, eller de kan stjæle data, som leverandøren behandler for sin kunde. Ofte har leverandører eller producenter fjernadgang til deres produkter på eksempelvis danske universiteter. Det kan muliggøre, at hackere kan få adgang til et system eller udstyr, hvorfra de kan sprede sig videre ud i de øvrige systemer. Leverandører af fællesoffentlige systemer kan også være det egentlige mål. Hackere kan i sådanne tilfælde forsøge at kompromittere uddannelsessteder, der benytter de fællesoffentlige systemer, for gennem dem at få adgang til leverandører eller producenter.

Leverandørvinklen understreger nødvendigheden af både et due diligence-tjek af leverandøren, inden der indgås en aftale, samt løbende opfølgning og tilsyn hos leverandører. Det er noget, som Digitaliseringsstyrelsen har anbefalet kraftigt siden 2013 på grund af CSC-sagen. Senest har CFCS udgivet en trusselsvurdering i forhold til cyberangreb via leverandører[9].

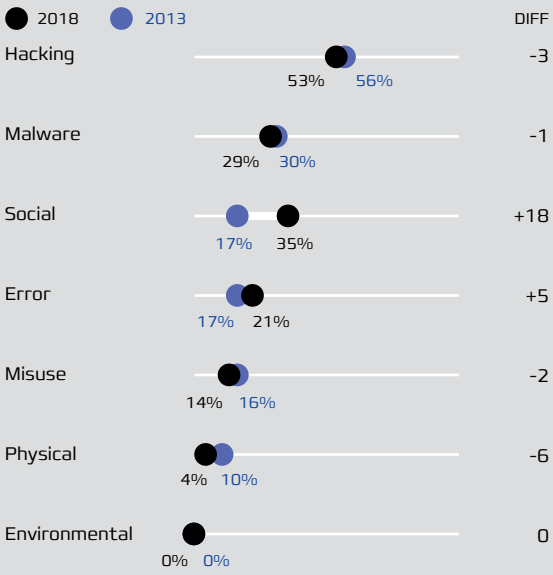
Ifølge Sophos og Europol er der blandt de kriminelle et stigende fokus på at angribe organisationer via leverandøren. Især leverandører af cloud eller andre online løsninger er eftertragtede angrebsmål, da man de ved en kompromittering, sandsynligvis vil kunne ramme en større del af leverandørens kunder[10]. Et af de mest kendte leverandørhacks er Target, der i 2014 angrebet hacket gennem deres leverandør af aircondition-enheder[11].

2019 var også året, hvor iranske hackere målrettet er gået efter VPN-leverandører. I den anden fase af angrebet var fokus på at lateral bevægelse i de penetrerede organisationer i forsøg på at udnytte flere sårbarheder og implementere bagdøre i systemerne[12].

9. Trusselsvurdering

Figur 22: Threat actions in data breaches

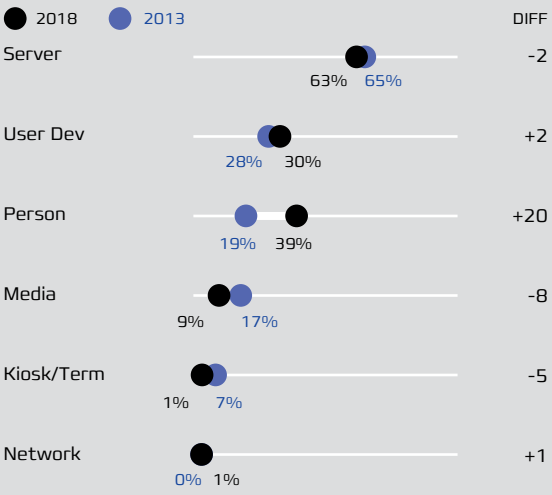
Over time n=2,501 (2013), n=1,638 (2018).



Kilde: DBIR

Figur 23: Asset categories in data breaches

Over time n=2,294 (2013), n=1,513 (2018).



Kilde: DBIR

CYBERKRIMINALITET

Truslen fra cyberkriminalitet mod den danske uddannelsessektor er MEGET HØJ.

Cyberkriminelle angriber uddannelsessektoren for at tjene penge på bl.a. afpresning og datatyveri. Dele af sektoren har været præget af ældre og sårbare systemer, og tidligere har der 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.

Den høje trussel understøttes af data fra DBIR[13], der viser, at motivationen for angreb på uddannelsessektoren for 80% af hændelserne er motiveret af finansiel vinding. Dette overstiger den næstmest udbredte kategori, som er spionage med 11%.

Cyberkriminelle er opfindsomme i deres forsøg på at berige sig og anvender mange forskellige typer cyberangreb, hvoraf en del er avancerede og komplekse. Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra virksomheder og myndigheder. Denne trussel kommer især til udtryk i form af ransomwareangreb, men cyberkriminelle afpresser også deres ofre på andre måder, fx ved hjælp af DDoS-angreb eller ved at true med at offentliggøre data, som de har stjålet ved hjælp af hacking.

Cyberkriminelle er rigtig gode til at udnytte forskellige situationer til at fremme deres mål. Eksempelvis bruger de gerne store begivenheder eller kriser til det, og ved epidemier er det især sundhedsorganisationer, de forsøger at udgive sig som. Alle ønsker informationer om epidemien, og er derfor ikke så eftertænksomme, som de normalt ville være, når de modtager mails.

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 medarbejdernes loginoplysninger. Dette understreger vigtigheden af awareness-aktiviteter blandt medarbejderne om denne trussel.

9. Trusselsvurdering

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 tre store angrebsteknikker er således phishing, malware og via sårbarheder.

DKCERT's sårbarhedsscanninger af uddannelsesinstitutionerne viser, at en af de mest udbredte sårbarheder, som nemt kan udnyttes til at installere cryptomining-software, er forældet software, både i form af styresystemer og i form af forældede versioner af eksisterende software. Når software har nået sin end-of-life, så bliver den ikke længere supporteret fra leverandøren. Nye sårbarheder bliver derfor ikke patchet, hvilket øger systermerne og servernes sårbarhed over for angreb betydeligt.

Nogle af de mest udbredte sårbarheder, der er fundet blandt danske uddannelsesinstitutioner, som er baseret på forældet software og operativsystemer er:

- Apache Unsupported Version Detection
- SSL Version 2 and 3 Protocol Detection
- CMS - Wordpress & Joomla! Unsupported Version Detection
- Microsoft Operating System/Servers Unsupported Version Detection
- Unix /Linux Operating System Unsupported Version Detection
- OpenSSL (DROWN)
- Variuos Cross Site Scripting vulnerabilities due to CGI
- PHP Unsupported Version Detection

Ransomware kan forstyrre driften og ødelægge forskning

Ransomware er en form for skadelig software, der spærrer for adgangen til offerets computer eller data. For at få genoprettet adgangen skal offeret betale en løsesum til bagmændene. Der er dog mange eksempler på, offeret ikke har fået data tilbage på trods af betaling af løsesummen Ransomware er Europols toptrussel i den seneste IOCTA rapport[14]. Her forklares det, at selvom den samlede volumen er faldet en smule, så er angrebene blevet mere specifikke og forårsager større skade på ofrene, noget som EU's egen CERT er enig i[15]. Der er især sket et forskydning fra spray-angreb til meget målrettede angreb, hvor de kriminelle har brugt flere ressourcer til at identificere, hvilke personer de skal forsøge at kompromittere, og hvordan de skal gøre det.

Uddannelsessektoren i både Danmark og i udlandet, har ligesom en lang række andre sektorer været ramt af ransomware. Dette kan være problematisk for uddannelses- og forskningssektoren, fordi især forskeres arbejde både kan være tidskritisk, og fordi mange års pludselig ikke længere er tilgængeligt.

Lige før jul blev tre universiteter i Tyskland, Belgien og Holland ramt af Clop ransomware, og dette angreb tvang to af universiteterne til at tage næsten alle deres systemer offline. University of Antwerpen havde tilsyneladende held til at begrænse skaden, både fordi angrebet blev opdaget tidligt, men også fordi der var en god netværkssegmentering og offline backup. University of Maastricht[16] og Justus-Leibig University Giessen blev tilsyneladende ramt betydelig hårdere, hvorfor det tog længere tid at genoprette driften[17].

Nogle af nyeste eksempler fra omverdenen er den amerikanske kystvagt, der fik et af operationscentrene inficeret med Ryuk og efterfølgende måtte lukke ned for centeret og tilhørende operationer[18]. Et andet eksempel er den globale virksomhed Travelex, der blev ramt kort efter nytår. Tre uger senere var organisationen stadig ikke tilbage på samme niveau som før angrebet[19]. Travelex er nu i den situation, at angriberne er begyndt at offentliggøre fortrolige data i et forsøg på at få Travelex til at betale løsesummen.

I Danmark har, iflg. DKCERT's undersøgelse for Digitaliseringsstyrelsen, seks procent af borgerne været ramt af ransomware på deres pc i 2018. Det

9. Trusselsvurdering

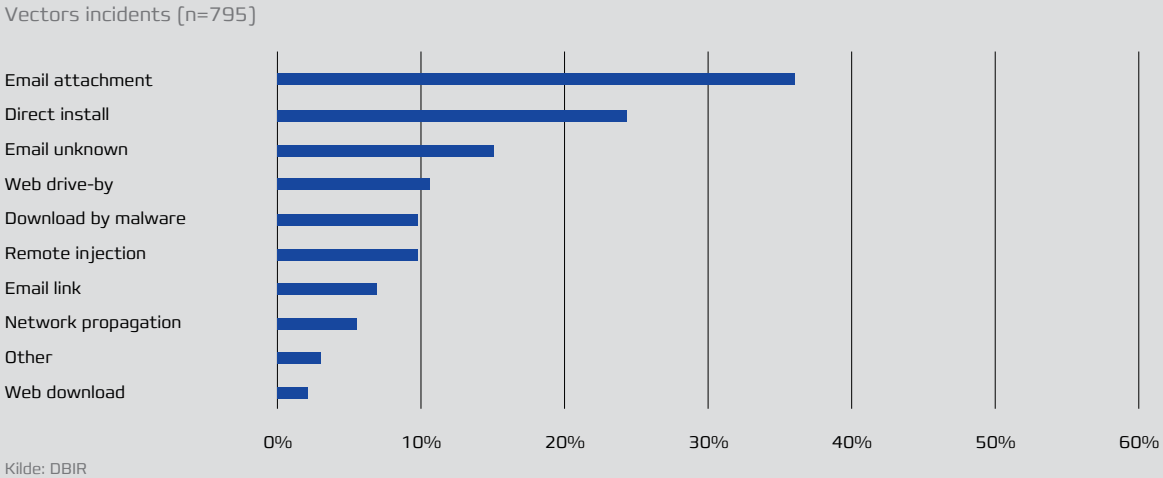
er en smule lavere end i 2016, hvor otte procent oplyste, at have været udsat for ransomware[20].

Email er den primære angrebsvektor, hvilket også tydeligt ses af figur 24. Mere end 90 % af den malware, der opdages, modtages i en gennemsnitlig organisation via mail. Vedhæftninger i mail, kode der afvikles fra mailen, eller andre angreb, der initieres via en mail, udgør de tre største angrebsvektorer blandt de virksomheder Verizon har indsamlet data fra til deres DBIR.

Den bedste måde at forsvare sig mod ransomware angreb er patch-management. Derudover er netværkssegmentering, backup og offline backup vigtige mitigerende tiltag, der kan mindske problemets omfang. DKCERT må konstatere, at selvom de danske uddannelsesinstitutioner er gode til at lave backup, så halter det hos flere uddannelsesinstitutioner med at implementere netværkssegmentering og tilstrækkelig patch-management, hvilket gør, at ransomware er en større trussel, end det behøver være.

Det er svært at understrege, hvor skadelig ransomwareangreb kan være. I løbet af sidste halvdel af 2019 blev adskillige amerikanske counties ramt af ransomware, der forstyrrede driften, og flere steder var man nødt til at gå tilbage til at udføreopgaver på papir. New Orleans blev i sommeren 2019 ramt så hårdt, at byen var nødt til at erklære undtagelsestilstand, da man var ude af stand til at levere basale ydelser til borgerne grundet angrebet[21]. I Danmark har både Maersk, Demant og senest ISS oplevet at deres forretning blev forstyrret betydeligt, eller fuldstændigt stoppet af ransomware angreb, med tab i flere hundrede millioner af kroner til følge[22].

Figur 24: Topmalware action



Kilde: DBIR

9. Trusselsvurdering

Malware, der udvinder kryptovaluta, stiger i omfang

Ud over de for tiden mest almindelige former for malware, så som Ruyk og Sodinokibi og payload leveringsmalware som Emotet og Trickbot, så er der også en type malware, som misbruger ofrets processorkraft (og dermed elforbrug) til at udvinde kryptovaluta, fx BitCoin eller Monero[23]. 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 krypto-valuta. Et sådant angreb er set mod mindst et dansk universitet inden for det seneste år. 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, der altid skal garderes mod.

HPC-anlæg kan være særligt eftertragtede for de kriminelle at få adgang til, men også uddannelsesinstitutionernes og især forskernes it-udstyr og software 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.

Overbelastningsangreb er en mindre alvorlig trussel

Der findes fortsat cyberkriminelle, der benytter Distributed Denial of Service (DDoS) angreb som et værktøj til afpresning. Et overbelastningsangreb foregår ved at kriminelle truer med at udføre angreb mod offerets it-systemer. Et større overbelastningsangreb kan gøre en hjemmeside til en uddannelsesinstitution - eller hjemmesider der bruges til at samarbejde og koordinere via – utilgængelig.

Den type angreb er blevet mere tilgængelig med udbredelsen af usikre IoT-enheder[24], som har vist sig som en effektiv platform for overbelastningsangreb. Ligeledes er lyssky online-tjenester, der udbyder overbelastningsangreb, lettilgængelige og billige at benytte.

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

Organisationer i uddannelsessektoren i Danmark har været udsat for forsøg på Business E-mail Compromise (BEC), hvor kriminelle har forsøgt at snyde organisationerne til at overføre penge til de kriminelles egne konti ved at udgive sig for at være en ledende medarbejder.

De såkaldte BEC-scams har til formål at franarre virksomheder og myndigheder 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. Hvis en ondsindet aktør er lykkedes med at kompromittere medarbejderes konti, øger dette risikoen for et succesfuldt bedrageriforsøg. DKCERT har en forventning om, at uddannelsessektoren, 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 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.

9. Trusselsvurdering

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 truslen mod den danske uddannelsessektor til at være LAV. Trusselsniveauet kan dog stige uden eller med kort varsel, hvis enkeltsager fanger aktivisternes opmærksomhed.

Der er dog eksempler på cyberaktivisme eller hærværk, om man vil. I sommeren 2017 blev 150.000 printere hacket af en ung mand, der fik alle printere til at udskrive store mængde af sider indeholdende mandens budskab[25]. Selv om konsekvenserne ikke var store i dette tilfælde, så viser eksemplet at denne type angreb kan bruges på mange forskellige måder, hvoraf nogle kan forårsage større skade end andre.

Ligeledes gik hackerkollektivet LulzSecITA i starten af 2020 ud på twitter og annoncerede et hack af tre italienske universiteter i et forsøg på at påvise universiteternes dårlige sikkerhed. Dette er et klart eksempel på en ideologisk begrundet hacktivism[26]. Angrebet var et simpelt SQL-injection, hvormed hackerne skaffede sig adgang til forskellige databaser hos universiteterne, og derfra kunne bevæge sig videre.

Senest har vi i Danmark oplevet, at UniLogin blev lagt ned af et større DDoS-angreb i starten af Corona-epidemien i Danmark, hvilket grundet situationen havde en betydelig større konsekvens end et sådan angreb ville have haft, hvis ikke skolerne var lukket på grund af Covid-19 og derfor afhængige af fjernundervisning[27].

Destruktive cyberangreb
En række lande har cyberkapaciteter, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur. Baseret på den offentlige tilgængelig 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 nogen konkrete hændelse rettet mod den danske uddannelsessektor. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

Et af de største destruktive cyberangreb var NotPetya, som også Maersk blev ramt af. Selvom truslen for destruktive cyberangreb hidtil ikke har været stor, er denne trend ifølge Europol ved at brede sig. I sommeren 2019 kom der en ny malware (GermanWiper), der overskriver de inficerede filer og dermed permanent ødelægger organisationens data[28]. Udbredelsen af destruktive cyberangreb kan muligvis forklares med, at de bruges til at ødelægge beviserne for cyberspionage.

9. Trusselsvurdering

Insidertruslen
En insider er en person med legitim adgang, som bevidst eller ubevidst påvirker uddannelsesinstitutionens virke gennem at sprede, skade eller ændre de informationer og processer, der udgør uddannelsesinstitutionens fundament. DKCERT vurderer at insidertruslen mod uddannelsessektoren er MEGET HØJ.

DBIR-data[29] viser, at 45% af alle trusselsaktører i uddannelsessektoren i 2019 var interne. Dette kombineret med, at "diverse fejl" – som primært dækker over menneskelige fejl – var en af de største kilder til sikkerhedshændelser. Det viser, at insidertruslen er meget vigtig for organisationerne at holde øje med og træffe foranstaltninger mod.

Insidertruslen er fra et samfundsperspektiv særlig skadelig for organisationer, som driver samfundsvigtig infrastruktur eller tjenester, håndterer følsomme data eller besidder værdifuld intellektuel ejendom.

Insidere kan inddeles i ubevidste og bevidste insidere. De ubevidste insidere er medarbejdere, der ikke er klar over, at deres adfærd kan være skadelig for organisationen. Bevidste insidere er medarbejdere, som bevidst overtræder organisationens sikkerhedspolitikker for egen vindings skyld eller med det formål at skade organisationen.

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.

I gruppen af ubevidste insidere finder man blandt andet de medarbejdere, 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.

Så sent som i starten af 2020 oplevede universiteterne et mindre phishingangreb gennem en kompromitteret bruger fra et dansk universitet. Brugeren var sandsynligvis selv kompromitteret via phishing, og da de kriminelle havde fået kontrollen over vedkommendes konto, kunne denne bruges til at udsende tusinder af phishingmails til ansat-

9. Trusselsvurdering

te på alle landets universiteter, og dermed omgå mange af de sikkerhedsforanstaltninger, som universiteterne har implementeret. Nogle gange lykkes sådan en fremgangsmåde, men DKCERT har også mange rapporteringer om forsøg, men hvor universiteterne har stoppet angrebet, inden de er kommet i gang.

Uagtsomme medarbejdere

En særlig gruppe ubevidste insidere er de uagtsomme medarbejdere, som undlader at følge gældende sikkerhedsprocedurer, fordi de føles besværlige eller unødvendige. En anden årsag kan være, at organisationen slet ikke har defineret nogen sikkerhedsprocedure, eller at procedurerne er utilstrækkelige. Medarbejdere kan eksempelvis vælge at dele sit password med kolleger, undlade at følge organisationens regler for udformning af sikre passwords, eller overføre følsomme data via private mailkonti eller usikre medier, fx for at kunne arbejde hjemmefra. Medarbejdere under arbejdspres kan tilsidesætte sikkerhedsprocedurer, som forsinker løsningen af en opgave.

Mangel på brugbare interne it-værktøjer kan få medarbejdere til at benytte usikre og uautoriserede løsninger. Det kan eksempelvis komme til udtryk ved download af ikke godkendt software eller deling af intern dokumentation via internetbaserede fildelings-løsninger uden for organisationens kontrol. Uagtsomheden kan også medføre, at it-systemer ikke installeres af it-afdelingen og dermed ikke driftes i forhold til organisationens sikkerhedspolitikker eller best practice.

Den stadig større udbredelse af mobile enheder som en del af arbejdspladsen, udgør også en stigende trussel for uddannelsesinstitutionerne. Mobile enheder giver sjældent de samme muligheder for at kontrollere indhold, som en computer gør, da designet har et andet fokus. Samtidig benyttes disse enheder oftest på farten, hvor brugernes opmærksomhed også er optaget af andre opgaver, hvilket øger chancen for at medarbejderne er uagtsomme[30].

Samtlige brud på persondatasikkerheden, som DKCERT's DPO-tjeneste har kendskab til, udspringer af medarbejdere, der enten ikke var klar over, at deres handlinger udgjorde et brud på persondatasikkerheden, eller medarbejdere, der har lavet basale fejl. Der er både tale om medarbejdere, der sender oplysninger, de ikke burde have sendt, og medarbejdere, der ikke kender reglerne godt nok, eller medarbejdere, der laver simple tastefejl. De har dog alle været ubevidste insiders, idet deres handlinger har medført brud på persondatasikkerheden, som har måtte rapporteres til Datatilsynet.

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 lavet af Carnegie Mellon University i USA[31] viser imidlertid, at op til 80% 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.

Af nyere eksempler på bevidste insidere er fx medarbejdere hos AT&T, der tog imod penge for at sælge kundernes oplysninger til andre virksomheder, eller bruddet hos Capitol One, hvor en tidligere ansat hos deres leverandør Amazon Web Services mistænkes for at have skaffet sig adgang til mere end 106 million af Capitol Ones kunders personoplysninger på en Amazon Simple Storage Servers (S3)[32].

9. Trusselsvurdering

Awareness
Manglende awareness blandt administrativt ansatte, blandt de studerende og blandt forskerne er et af de grundlæggende problemer i forhold til insidertruslen. Denne kan dog afhjælpes gennem træning og viden, fx i forhold til passwords, hvor mange brugere har for korte passwords, genbruger passwords eller laver for lette passwords.

Kravet om komplekse passwords, regelmæssig udskiftning og sikring har faktisk vist sig ikke at have den ønskede effekt, hvilket har krævet de nye anbefalinger, der gør op med den nuværende best practice. Længden af dit password betyder mere end store bogstaver, tal eller specialtegn, som hidtil har været prioriteret højt. Et godt password bør derfor være på mere end 12 tegn.

I rapporten Danskernes informationssikkerhed fra 2018[33], har vi blandt andet spurgt om, hvor lange adgangskoder danskerne har. 75 procent har en adgangskode på mellem seks og ti tegn. 18 procent har over 11 tegn, mens tre procent anvender mellem et og fem tegn.

Det andet vigtige element i forhold til sund password-håndtering er, at man ikke anvender den samme adgangskode til flere tjenester. Her fortalte danskerne, at 37 procent anvender samme adgangskode til flere online-tjenester. 24 procent svarer dog, at det kun er til tjenester, der ikke håndterer følsomme data[34]. Genbrug af password er en af de største risici i forhold til at få konti til andre tjenester kompromitteret.

Flere og flere organisationer er begyndt at teste deres medarbejderes kendskab til phishing-angreb, noget som DKCERT understøtter med en phishing-tjeneste.

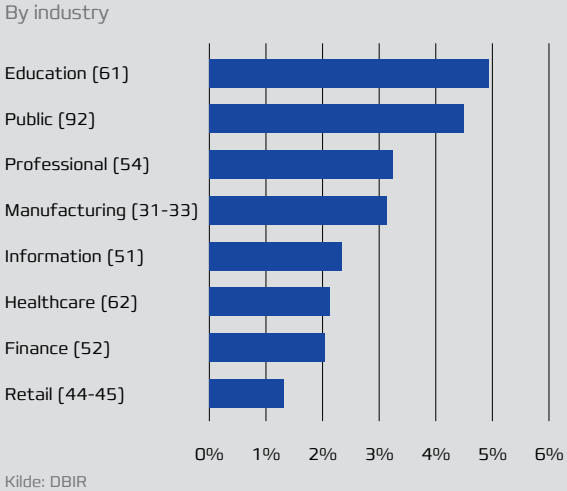
Tal fra Verizons DBIR viser, at uddannelsessektoren er det område, der klarer sig dårligst, når organisationer selv tester deres medarbejderes awareness vedrørende phishing.

Yderligere er uddannelsesinstitutionerne mere sårbare end mange andre typer organisationer, da de studerende også kan være en angrebsvektor ind i organisationerne.

Samtidig viser rapporten også en stor diskrepans mellem medarbejdere, der klikker på phishinglinks, og de medarbejdere der indberetter, at de har klikket på phishinglinks.

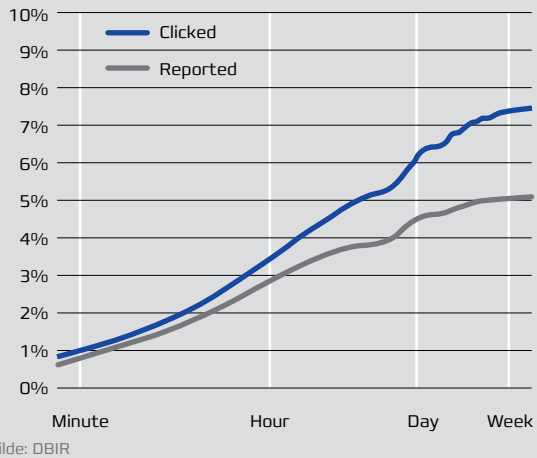
Awareness vil også kunne hjælpe uddannelsesinstitutionerne med at beskytte sig mod, at medarbejdere installerer apps på deres mobile enheder, som kan have sårbarheder, eller bagdøre i sig. Google har fx for nyligt fortalt, at der i løbet af de sidste to år er blevet fjernet mere end 1.700 apps, der alle var inficeret med den samme type malware (Bread/Joker)[35].

Figur 25: Click rate in phishing



Kilde: DBIR

Figur 26: Simulated Phishes



Kilde: DBIR

9. Trusselsvurdering

Tendenser i uddannelsessektoren med betydning for cybertruslen

Der er en række forhold i uddannelsessektoren, som kan have betydning for cybertruslen. Blandt andet er sektoren sårbar over for, at cyberangreb faciliteres af medarbejdere, der mere eller mindre bevidst nedprioriterer cybersikkerhed. Både forskning og den generelle drift i uddannelsessektoren er også i stigende grad afhængig af (netopkoblet) teknisk udstyr og it-systemer, og disse er i stadig udvikling (se Figur 27).

Internet of Things på universiteter og andre uddannelsesinstitutioner

Begrebet "Internet of Things" (IoT) beskriver en tendens, hvor flere og flere elektroniske apparater bliver koblet til internettet. Denne tendens gør sig også gældende for laboratorier og hospitaler, men her forbindes apparaterne dog ofte til hospitalernes interne net. Apparaterne er ofte udstyret med sensorer, som automatisk indsamler data. IoT-apparaterne har mange fordele, da de eksempelvis kan give forskere mere data om deres forskningssubjekter eller gøre det nemmere at udveksle data.

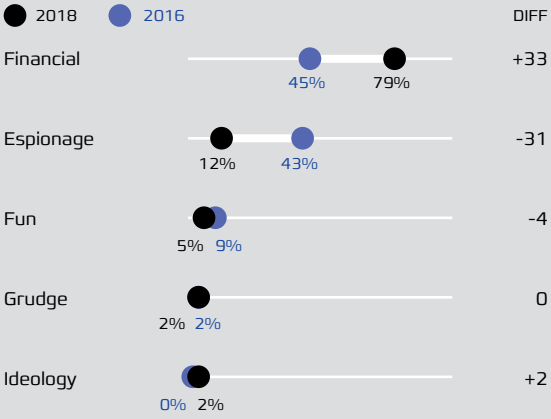
Der er dog mange af disse IoT-apparater, hvor cybersikkerhed ikke er tænkt ind fra producentens side. Det kan fx skyldes, at producenten har fokus på at mindske apparatets størrelse, øge dets batterilevetid eller på at gøre det nemmere for leverandøren at supportere. IoT-apparaternes dårlige sikkerhed kan i sig selv være en adgang for hackere, men den trådløse deling af data imellem apparaterne kan også gøre det nemmere for hackere at opsnappe data, hvis disse ikke er krypterede i forsendelsen.

Sikkerhedsforskere har i flere tilfælde illustreret, hvordan forskelligt udstyr under visse omstændigheder kan hackes med alvorlige konsekvenser for sikkerheden. Eksempelvis blev en termostat i et akvarium hos et kasino i Las Vegas brugt som indgang til kasinoets netværk. Dette resulterede i, at hackerne fik kopieret kasinoets kundedatabase indeholdende mange forskellige personoplysninger[36]. Også i legetøj, el-kedler, køleskabe, web-kameraer og en række andre IoT-enheder er der fundet alvorlige sårbarheder, som på forskellig måde har kunnet anvendes til direkte eller indirekte angreb.

Om den manglende sikkerhed i IoT-enheder skyldes et ønske om at få produkterne på markedet hurtigst muligt, at gøre enhederne så billige som muligt, eller at sikkerhed aldrig har været prioriteret i netop den branche er uklart. Faktum er, at IoT-enheder sjældent har nogen former for sikkerhed indbygget.

Figur 27: Breaches

Grafen viser tydeligt udviklingen for sektoren, hvor den finansielle motivation stiger kraftigt, samtidig med at der over de to år tilsyneladende er sket et betydeligt fald inden for spionage.



Kilde: DBIR

9. Trusselsvurdering

Anbefalinger
Alle forsknings- og uddannelsesinstitutioner anbefales at orientere sig om truslen fra insidere og inddrage den trussel i deres løbende risikovurdering.

Selvom ubevidste insidere kan findes i alle organisationer, så er det vigtigt også at se medarbejderne som et væsentligt værn mod cybertruslen. Dette værn fungerer imidlertid kun, hvis organisationen løbende motiverer medarbejderne til at følge veldefinerede og forståelige sikkerhedsprocedurer. Organisationer bør desuden holde medarbejderne opdateret om de metoder, som trusselsaktørerne benytter samt træne dem i at se faresignalerne i fx uventede kontakter, telefonopkald, e-mails og lignende.

Organisationer kan med fordel undersøge, hvor stor potentiel skade en bevidst insider i organisationen eller hos en underleverandør kan gøre blot ved at udnytte gældende processer og legitime adgange til forretningskritiske it-systemer og data. Resultatet kan måske give anledning til at indføre eller ændre sikkerhedspolitikker, processer, tekniske sikkerhedsmekanismer eller medarbejderes adgange til og roller på kritiske it-systemer.

Mange af de sikkerhedshændelser, der forekommer i uddannelsessektoren, er et resultat af dårlig sikkerhedshygiejne. 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 2-faktor autorisation.

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.

Endeligt er det vigtigt at være opmærksom på, at konflikter med medarbejdere opdages og håndteres hensigtsmæssigt, samt om der er forhold, som potentielt kan føre til en konflikt.

9. Trusselsvurdering

Konkrete emner

- Det er DKCERT's vurdering, at flere danske uddannelsesinstitutioner allerede har implementeret god patch management. Dog er det ikke alle steder, at der er den nødvendige opfølgning på den udførte patch management eller de nødvendige kontroller, der sikrer, at den nødvendige patch management altid udføres.
- Det er DKCERT's vurdering, at insidertruslen i mange tilfælde forstørres af bruges af social engineering fra de kriminelles side, og derfor anbefales det, at uddannelsesinstitutionerne implementerer DMARC og DNSSEC som værn mod at domæner misbruges til phishing og andet, således at der er tekniske sikkerhedsforanstaltninger, der sammen med nedskrevne og implementerede procedurer kan understøtte medarbejdernes awareness inden for området.
- Med den stigende udbredelse af ransomware, er det DKCERT's anbefaling, at alle uddannelsesinstitutioner implementerer forebyggende tiltag som offline backup, test af offline backup, beredskabsplaner og test af beredskabsplanerne med henblik på hurtigt at kunne komme tilbage fra et ransomwareangreb.

Anbefalingen om implementering af DMARC understøttes også af, at det fra 1. januar 2020 er blevet et krav til statslige organisationer[37].

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

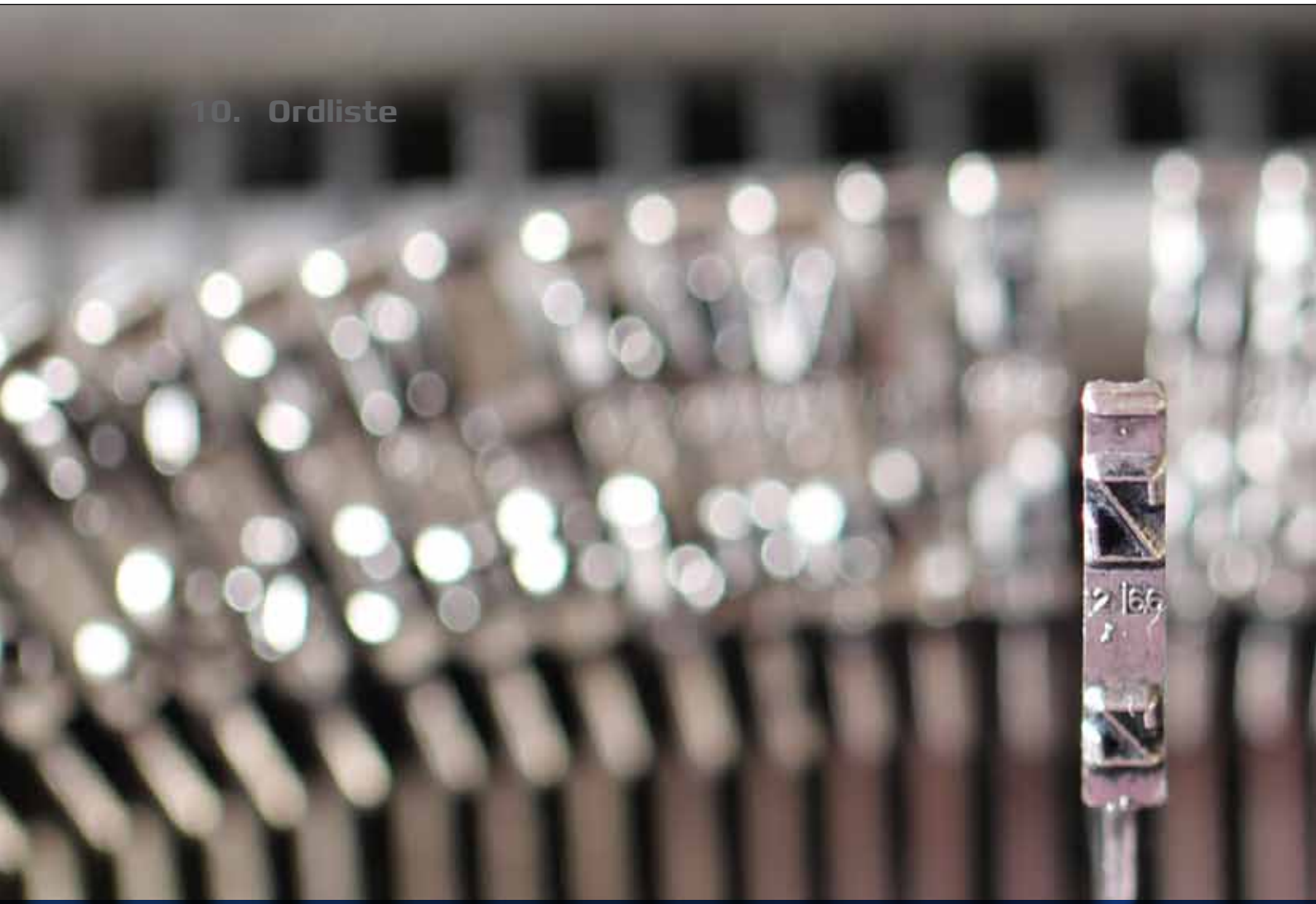
Der konkrete trusler. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

9. Trusselsvurdering

Notehenvisninger til trusselsvurderingen

1 https://www.fm.dk/publikationer/2018/national-strategi-for-cyber-og-informationssikkerhed
2 https://www.marketscreener.com/news/Malware-Variety-Grew-by-13-7-In-2019--29719304/
3 https://www.fortinet.com/blog/industry-trends/threat-landscape-trends-education.html
4 https://fe-ddis.dk/cfcs/nyheder/arkiv/2020/Pages/Undersoegelsesrapport-Glemmer-du-saa-husker-hackerne.aspx
5 https://www.version2.dk/artikel/vestlige-efterretningstjenester-trusselsaktoer-camouflerede-sig-iran-1089230
6 https://www.cert.dk/da/news/2019-09-16/phishing
7 https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/
8 https://www.dr.dk/nyheder/penge/digital-afpresning-vokser-det-maa-naermest-betegnes-som-en-kampagne-mod-forskellige
9 https://fe-ddis.dk/cfcs/publikationer/Documents/Trusselsvurdering-Cybertruslen-mod-leverandoerer.pdf
10 https://news.sophos.com/en-us/2019/12/09/ransomware-the-cyberthreat-that-just-wont-die/
11 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
12 https://www.zdnet.com/article/iranian-hackers-have-been-hacking-vpn-servers-to-plant-backdoors-in-companies-around-the-world/
13 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
14 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
15 https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-Executive-Summary-TLR2019Q4-v1.0.pdf
16 https://www.observantonline.nl/English/Home/Articles/articleType/ArticleView/articleId/17790/Cyberhack-Maastricht-University-pays-ransom
17 https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt
18 https://www.silicon.co.uk/security/cyberwar/ransomware-us-coast-guard-326285
19 https://fossbytes.com/sodinokibi-ransomware-makes-stolen-data-public-ransom-isnt-paid/
20 https://digst.dk/media/18755/danskernes_informationssikkerhed_december_2018_191218.pdf
21 https://www.engadget.com/2019/12/14/new-orleans-cyberattack/
22 https://www.computerworld.dk/art/251215/iss-har-gjort-kaemperegningen-op-for-hacker-angreb-kommer-til-at-koste-minimum-en-halv-milliard-kroner
23 Monero er en kryptovaluta, der lige som den mere kendte Bitcoin bygger på blockchain-teknologi.
24 Internet of Things – samlebetegnelse for internetopkoblede tekniske enheder, der ikke er egentlige computere. Fx laboratorieudstyr, køle- og fryseskabe, overvågnings- og alarmudstyr, varme- og ventilationsstyring o.m.a.
25 Bruce Schneiers bog, Click Here to Kill Everybody, side 2
26 https://securityaffairs.co/wordpress/97802/breaking-news/lulzsec-ita-hacked-italian-universities.html
27 https://www.computerworld.dk/art/251204/unilogin-lagt-ned-af-stort-cyber-angreb-staten-kaemper-for-at-afvaerge-angrebet
28 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
29 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
30 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
31 https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21232
32 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
33 https://digst.dk/media/18755/danskernes_informationssikkerhed_december_2018_191218.pdf
34 Et nyt site med awarenesstræning er sikkerkollega.dk, som Industriens Fond står bag
35 https://www.zdnet.com/article/google-details-its-fight-against-the-bread-joker-malware-operation/
37 https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/
38 https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/

10. Ordliste



10. Ordliste

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 informationssikkerhed 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. Centeret har i dag cirka 100 medarbejdere og består af seks afdelinger (Rådgivning og standarder, Forsvar og akkreditering, Cyber policy, Situationscenter, Cyberanalyse samt Defensive cyberoperationer). Organisatorisk er Center for Cybersikkerhed en af seks sektorer i Forsvarets Efterretningstjeneste.

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.

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 eller BEC, Business E-mail Compromise. Falske e-mails eller sms'er ofte sendt til regnskabsafdelingen. Angiver at komme fra en ledende medarbejder, der beder modtageren hurtigt gennemføre en pengeoverførsel til udlandet.

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.

10. Ordliste

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.

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.

M

Malware
Skadelig software. Ordet er en sammentrækning af "malicious software". Malware er en samlebetegnelse for virus, orme, trojanske heste, keyloggere, spyware, adware, botnet-programmer 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.

10. 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.

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.

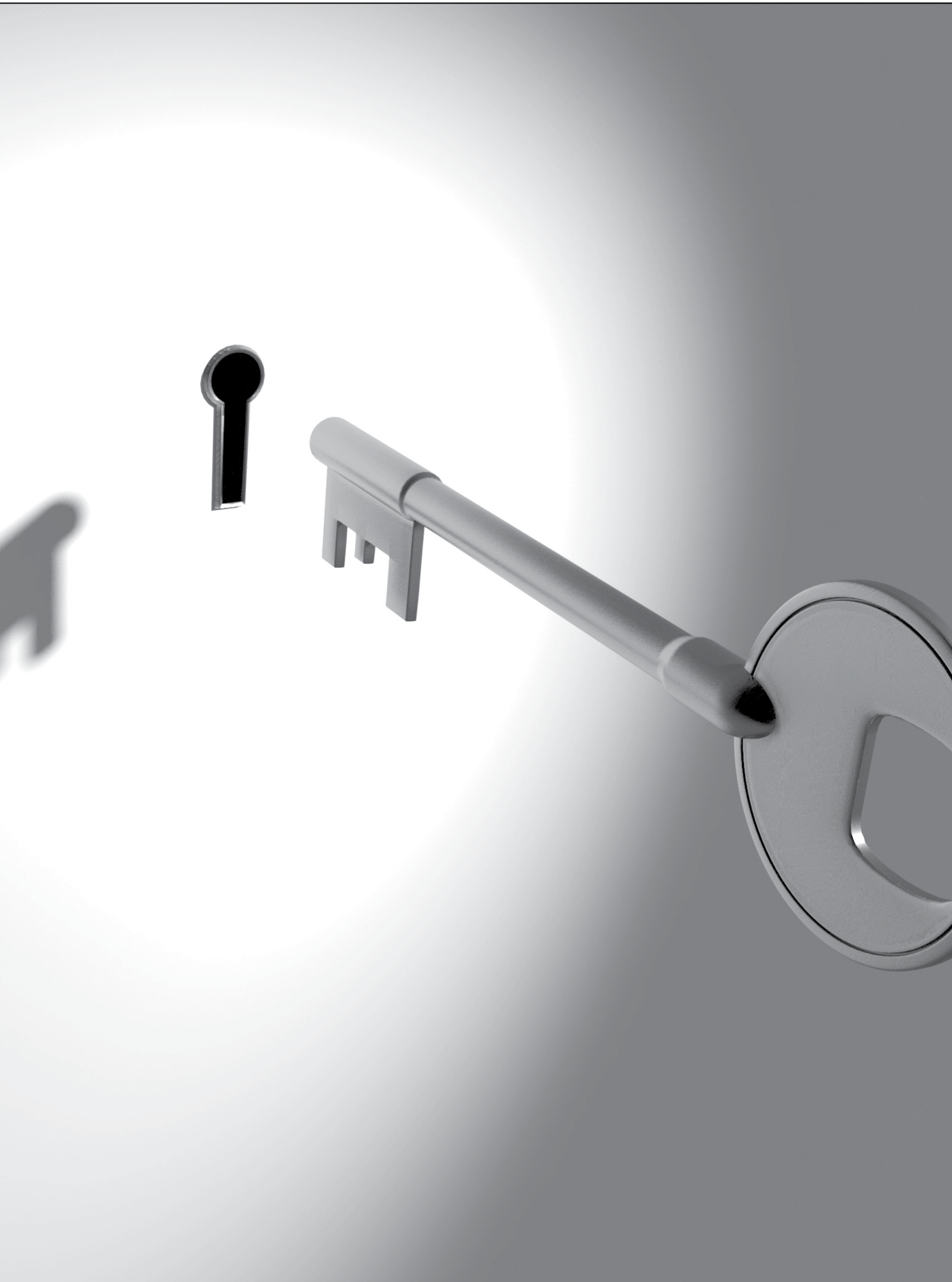
V

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.

11. Figurliste



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