DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

Analyser, indsigt og anbefalinger til universiteterne om informationssikkerhed

DKCERT Trendrapport 2019

Redaktion: Henrik Larsen og Nicolai Devantier

Tak til vore øvrige bidragydere:

Thomas Lund-Sørensen, chef for Center for Cybersikkerhed.

Birgitte Hass, administrerende direktør, IT-branchen.

Rikke Hougaard Zeberg, direktør i Digitaliseringsstyrelsen.

Ole Kjeldsen, direktør for Teknologi og Sikkerhed, Microsoft og medlem af bestyrelsen i Rådet for Digital Sikkerhed.

Poul Halkjær Nielsen, informationssikkerhedschef, Københavns Universitet.

Jakob Willer, direktør, Teleindustrien.

Jan Kaastrup, chief technology officer, CSIS Security.

Simon Nexø Jensen, DKCERT.

Johnson Akpotor Scott, DKCERT.

DeiC-journalnummer: DeiC JS 2018-02

Design og layout: Kiberg & Gormsen

DKCERT - en del af DeiC

DTU, Asmussens Allé, Bygn. 305

2800 Kgs. Lyngby

Copyright © DeiC 2019

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 it-sikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen, samt internationale samarbejdspartnere.

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

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 hører organisatorisk under Styrelsen for Forskning og Uddannelse, Uddannelses- og Forskningsministeriet.

DKCERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om informationssikkerhed med inspiration fra 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 den globale organisation 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

2019 kommer til at stå i National strategi for cyber- og informationssikkerheds tegn. Derfor er det også naturligt, at vi har valgt dette emne som omdrejningspunkt for DKCERT Trendrapport 2019.

2018 var domineret af to milepæle, begge i maj. Det var nemlig her, at GDPR (som var emnet i sidste års rapport) trådte i kraft og den nye National strategi for cyber- og informationssikkerhed blev offentliggjort. En samlet national strategi har betydet et øget fokus på informationssikkerhed som helhed, men er også grundlaget for at beskytte Danmarks samfundskritiske infrastruktur mod angreb.

Strategien har allerede udmøntet sig i helt konkrete resultater og initiativer, og flere er godt på vej. Det handler eksempelvis om informationssikkerhedsportalen, Sikkerdigital.dk, der blandt er bygget på resultater fra rapporten Danskernes informationssikkerhed 2018, som er udarbejdet af DKCERT i samarbejde med Digitaliseringsstyrelsen, KL og Danske Regioner.

På Sikkerdigital.dk samles vigtig viden om informationssikkerhed til gavn for borgere, virksomheder og myndigheder. Det er altid nødvendigt at have adgang til information og hjælp - specielt i en tid, hvor antallet af borgere, der rammes at sikkerhedsproblemer, stiger ret kraftigt. Den tendens kan vi i DKCERT desværre også konstatere, bl.a. da vi analyserede data i forbindelse med rapporten om danskernes informationssikkerhed.

Et andet vigtigt element, der udspringer af den nationale strategi, er de seks sektorvise cyber- og informationssikkerhedsenheder, der skal sikre, at samfundets kritiske infrastruktur som sundhed, finans, sø- og landtransport, tele- og energiforsyning bliver beskyttet. Enhederne er etableret og bliver operative i løbet af første halvår 2019.

I DKCERT Trendrapport 2019 kan du naturligvis også finde statistikker fra DKCERTs sikkerhedsanalytikere om forskningsnettets sikkerhed, og samtidig har vi fornøjelsen af at kunne give et bredere perspektiv om den nationale strategi gennem indlæg fra seks eksterne skribenter.

God fornøjelse med læsningen!

Henrik Larsen
chef for DKCERT

2. Resumé

DKCERT foretog 121 sårbarhedsscanninger af institutionerne på forskningsnettet, behandlede 3.782 sikkerhedshændelser og udsendte blandt andet advarsler om sextortion, side channel-angreb og masser af datalæk.

DKCERT behandlede 3.782 sikkerhedshændelser i 2018. Det er cirka 1000 færre end i 2017. Forklaringerne kan være, at institutioner på forskningsnettet er blevet hurtigere til at løse sikkerhedsproblemer eller, at der er færre inficerede maskiner.

2018 blev et rekordår for antallet af registrerede sårbarheder i verden. Dette kan også ses i resultaterne fra DKCERTs sårbarhedsscanninger og –vurderinger. I 2018 udførte DKCERT 121 scanninger af institutioner på forskningsnettet, og samlet se viste scanningerne sårbarheder på 13.705 eksterne IP-adresser.

Risikovurderingerne i forbindelse med eksterne scanninger viste, at seks procent af sårbarhederne er kritiske, 13 procent høje, 61 procent middel og 21 procent lave.

DKCERT registrerede 61.400 advarsler fra tredjepart om sårbare systemer på forskningsnettet. Den mest hyppige var sårbarheden POODLE (Padding Oracle On Downgraded Legacy Encryption).

Antallet af modtagere af DKCERTs ugentlige nyhedsbreve var ved udgangen af 2018 på 1.577. Twitter bliver dog en stadig mere populær kanal, og antallet af DKCERTs følgere er steget fra 2.065 i 2017 til 2.439 i 2018.

2.1. TENDENSER FRA ÅRET DER GIK

I Danmark har seks procent af borgerne været ramt af ransomware på deres pc i 2018. 17 procent af de seks procent fik ikke data tilbage efter at være blevet ramt af ransomware. En anden angrebsmodel, der er dukket op flere gange i 2018, er de såkaldte sextortion-udsendelser. DKCERT udsendte flere advarsler om dette.

Året begyndte med et par alvorlige sårbarheder, Meltdown og Spectre, som i forskellige varianter har hærget hele 2018. Flere af disse såkaldte side channel-angreb er nemlig kommet til i løbet af året.

Adgangskoder har været et af fokusområderne i 2018, hvilket helt konkret har udmøntet sig i, at anbefalingerne til et godt password er blevet strammet op. 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.

2018 har - igen - været et år med enorme datalæk. Implementering af GDPR betyder, at der siden maj 2018 indberettes om mange nye danske dataproblemer til Datatilsynet. I perioden fra 25. maj til udgangen af 2018 kom der ifølge Datatilsynet i alt 2.780 af disse anmeldelser.

DeiC introducerede i 2017 en ny tjeneste, knyttet til DKCERT, der rådgiver institutioner om EU's databeskyttelsesforordning. Tjenesten har bidt sig godt fast på mange institutioner i 2018.

2.2. TENDENSER I 2019

En af de tendenser, vi har oplevet i 2018, er digital afpresning og i det kommende år, vil angrebene blive yderligere raffinerede og spille mere på brugernes frygt. Ved at skræmme ofrerene med områder som seksualitet, sundhed eller trusler i familiemæssig sammenhæng, kan der tjenes penge. GDPR-implementeringen betyder, at der er udsigt til store bøder, hvis man ikke passer godt på folks data. Dette kan udnyttes i forbindelse med afpresning. Det er alt sammen metoder, som kriminelle kan opfatte som gode forretningsmodeller for deres lyssky aktiviteter.

Et andet område DKCERT forventer at se aktivitet omkring i 2019, er hacktivisme i forbindelse med offentliggørelse af data. Stjålne data om fx politikere eller andre offentlige personer kan offentliggøres i forbindelse med politisk motiveret hacking - hacktivisme. Begrebet dækker over forfølgelse af politiske mål ved hjælp af midler som defacement, DDoS-angreb og altså informationstyveri.

Der skal både være Folketingsvalg og valg til EU-parlamentet i 2019. I den forbindelse forudser DKCERT påvirkningskampagner, hvor uvedkommende vil forsøge at påvirke interne politiske forhold gennem manipuleret indhold.

2019 bliver også året, hvor dataetik kommer i fokus i sammenhæng med sikkerhed. Og vi er allerede i gang.


password

3. 2018 – året i tal

DKCERT behandlede 3.782 sikkerhedshændelser i 2018.

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

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

3.1. ÅRETS SIKKERHEDSHÆNDELSER

DKCERT behandlede 3.782 sikkerhedshændelser i 2018 (se Figur 1). Det er cirka 1.000 mindre end i 2017, hvor antallet var på 4.736.

En mulig forklaring på faldet kan være, at der er færre inficerede computere på universiteterne, og at universiteterne er blevet hurtigere til at løse sikkerhedsproblemer.

En anden mulig forklaring er, at angreb i højere grad finder sted på andre niveauer end netværkslaget. Derfor er det ikke organisationer som DKCERT, der hører om dem. Det kan fx være sager, hvor en svindler udgiver sig for at være ledende medarbejder, der har brug for at få overført nogle penge til udlandet i en fart. Skønt henvendelsen kommer via e-mail, bliver den ikke nødvendigvis anmeldt som en it-sikkerhedshændelse til DKCERT. Heller ikke forsøg på ransomware-angreb bliver altid anmeldt til DKCERT.

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

3.782 er stadig et stort tal, og mange hændelser bliver da også filtreret fra i den interne proces. Det drejer sig eksempelvis om spam-mail, der ikke udgør en risiko i denne sammenhæng og derfor ikke bliver undersøgt i dybden.

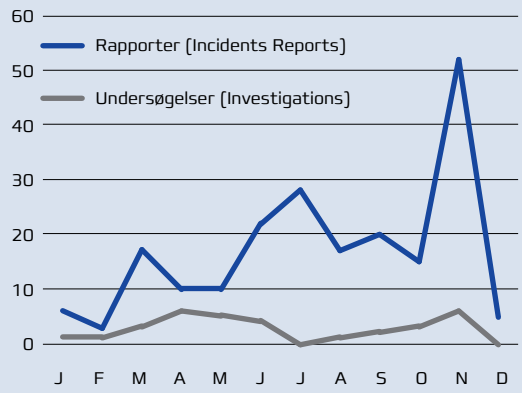
De alvorlige sager, hvor der skal foretages en indsamling af data fra eksempelvis angrebsramte institutioner og på baggrund af dette udarbejdes analyser, fordeler sig på følgende vis: DKCERT har modtaget 205 rapporteringer, som vi har analyseret og herudfra efterforsket 32 sager i 2018 (se Figur 2). Sagerne har blandt andet handlet om inficerede systemer på forskningsnettet og bedrageri med økonomiske tab til følge.

Figur 1: Sikkerhedshændelser pr. måned

Sikkerhedshændelser behandlet af DKCERT i løbet 2018.

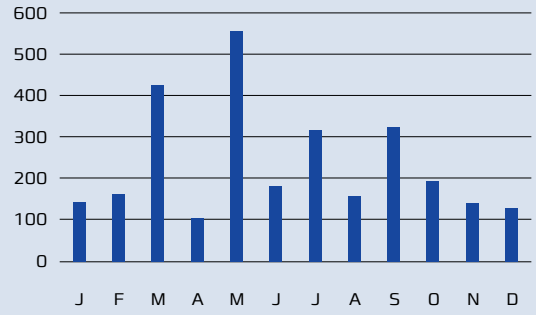
Figur 2: Rapporter og undersøgelser

Efter filtrering af de trivielle sikkerhedshændelser, som eksempelvis spam, har DKCERT udarbejdet følgende rapporter og undersøgelser i 2018.



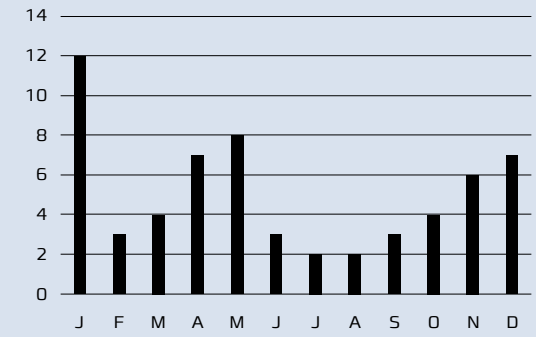
Figur 3: Portscanninger og rekognoscering

Portscanninger og andre forsøg på rekognoscering.



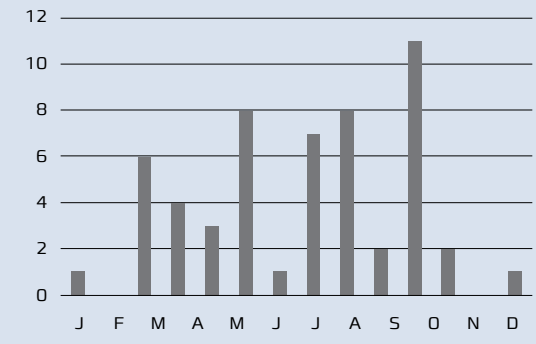
Figur 4: Spam-relaterede sager

Sager om udsendelse af spam pr. måned i 2018.



Figur 5: Uautoriseret adgang

Det samlede antal sager om uautoriseret adgang til it-systemer fordelte sig således.



3.2. SIKKERHEDSHÆNDELSER FORDELT PÅ TYPER

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

3.2.1. Portscanninger

Portscanninger var nummer et på listen over de hyppigste sagstyper i 2018. 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.

Mængden af registrerede portscanninger fordeler sig således (se Figur 3).

3.2.2. Spam

Sager om spam var nummer to på listen over de hyppigste sagstyper. DKCERT tager sig ikke af klager fra folk, der har modtaget spam. Sagerne handler i stedet om servere, der misbruges til udsendelse af spam.

Episoderne fordelte sig således pr. måned (se Figur 4).

3.2.3. Uautoriseret adgang

DKCERT opdeler hændelser om uautoriseret adgang til it-systemer 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 (se Figur 5).

3.2.4. Øvrige typer

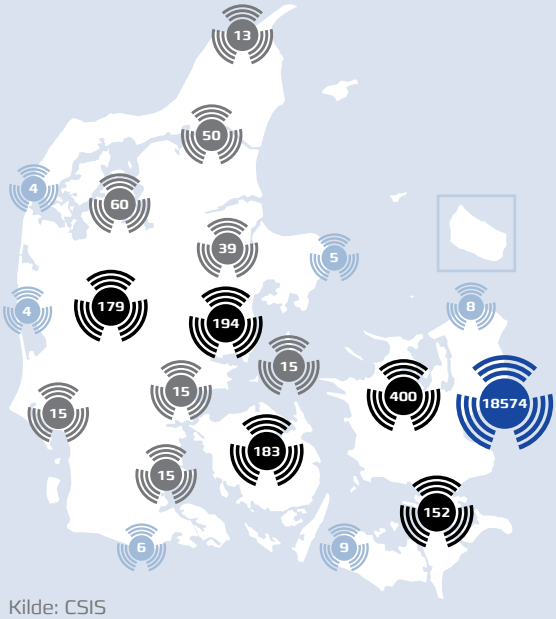
Piratkopiering har typisk været et område, med en betydelig hyppighed, indtil midten af 2017, hvor en bestemt IP-adresse, der modtog mange klager, blev lukket ned efter henvendelse fra DKCERT. Siden har der kun været få sager.

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

Figur 6: Phishing-sider, Command-and-Control-servere og drop-sider i Danmark

Kilde: CSIS

Figur 7: Inficerede IP-adresser i Danmark



Kilde: CSIS

3.3. MALWARE OG PHISHING I DANMARK

I Danmark har sikkerhedsfirmaet CSIS opgjort antallet af inficerede IP-adresser.

Hovedstadsområdet er hårdest ramt med 18.574 inficerede IP-adresser, efterfulgt af de øvrige større byer i landet. Infektionerne består eksempelvis af Sality malware-familien eller Conficker, der også er kendt under navnet Downadup. Det er en orm, der første gang blev set i 2008. Dengang inficerede den millioner af computere over hele verden. Den spreder sig via sikkerhedshuller i Windows, som for længst er lukket. At den stadig eksisterer, kan være tegn på, at nogle computere ikke er opdateret i mange år. Android malware, bank-trojanere m.m. falder også ind under dette område (se Figur 7).

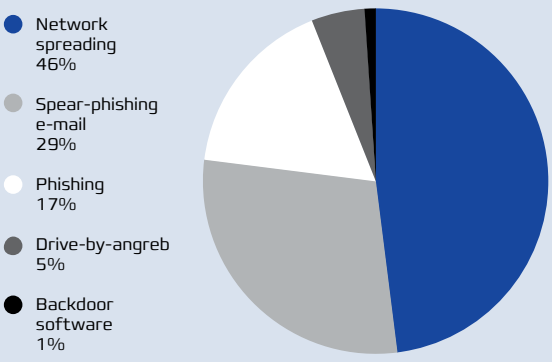
Phishing-sider, Command-and-Control-servere og dropsider er ligeledes mest udbredt i hovedstaden med 414 (se Figur 6). I resten af landet er antallet meget begrænset.

Metoderne, hvorpå orme eller virus, ifølge CSIS, hyppigst spreder sig, fordeler sig på tre forskellige. Infektionsvektorerne, der netop fortæller, hvordan smitten spreder sig, er opgjort således: Smitten spredes hyppigst via netværket eller via generel phishing og spear phishing, som er digitale henvendelser, der retter sig mod udvalgte ofre eller målgrupper eksempelvis i en virksomhed. Drive-by-angreb er ligeledes udbredt (se Figur 8).

For at lokke godtroende brugere til at klikke på phishing-henvendelser anvendes store og kendte brands til at få de ondsindede mails til at se officielle ud. De firmanavne, der oftest benyttes som fluepapir, er virksomheder som Paypal, Microsoft, Google, Outlook og Apple (se Figur 9).

Figur 8: Top-5 infektionsvektorer

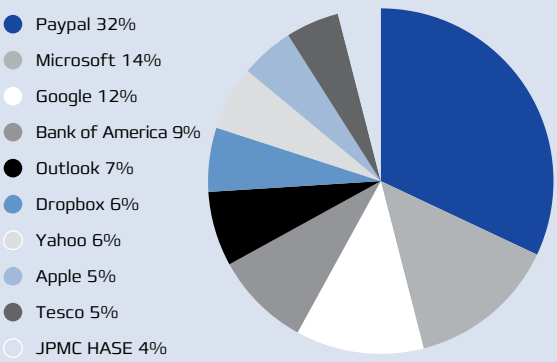
Fordelt på trusselstyper.



Kilde: CSIS

Figur 9: Top-10 phishing brands

De mest anvendte brands i forbindelse med phishing mails.



Kilde: CSIS

3.4. DANSKERNES INFORMATIONSSIKKERHED 2018

DKCERT har i flere år gennemført en statistisk undersøgelse af danskernes informationssikkerhed.

Den nyeste udgave blev udgivet i december 2018, og den afdækker, hvilke sikkerhedshændelser borgere og ansatte i det offentlige bliver udsat for, belyser deres viden om informationssikkerhed samt deres evne til at beskytte sig mod udbredte trusler.

Rapporten bygger på en undersøgelse, som Danmarks Statistik foretog for Digitaliseringsstyrelsen og DKCERT i foråret 2018.

Formålet med undersøgelsen er at afdække, dels hvilke trusler mod informationssikkerheden deltagerne oplever, dels hvad de ved om informationssikkerhed og deres mulighed for at beskytte sig.

Undersøgelsen stillede en række spørgsmål til et repræsentativt udvalg af den voksne danske befolkning om deres erfaringer med informationssikkerhed. Undersøgelsen bygger på svar fra 1.505 personer i alderen 18-74 år.

Nogle af konklusionerne i rapporten er, at én ud af tre borgere har enheder, der har været inficeret med virus eller lignende, og fem procent har fået misbrugt personoplysninger på nettet.

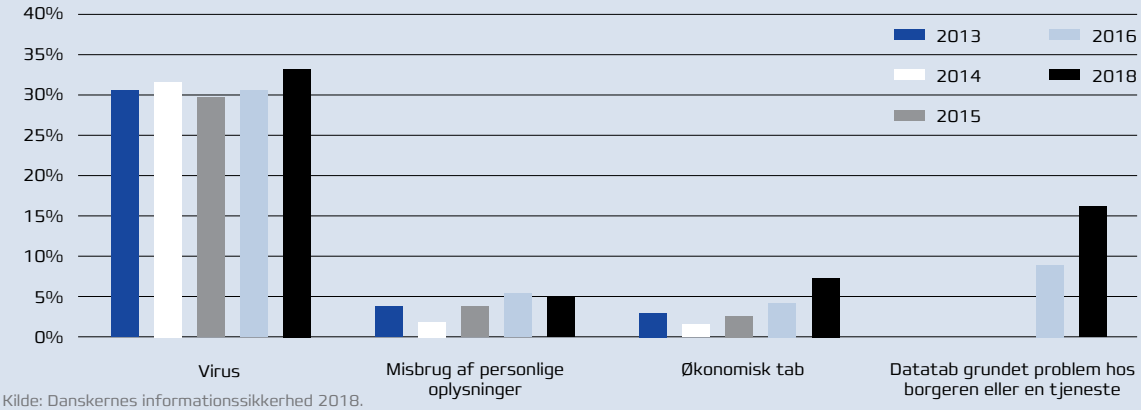
Otte procent af borgerne har desuden mistet penge som følge af onlinesvindel eller afpresning, og 17 procent har mistet data som følge af et computernedbrud eller softwarenedbrud – eller fx et ransomwareangreb.

Samlet har 44 procent af borgerne været udsat for mindst et af fire sikkerhedsproblemer: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data (se Figur 10).

Det er en stigning fra 34 procent i 2016.

Figur 10: Borgernes oplevede sikkerhedstrusler på computer

Flere borgere har oplevet virus-problemer, flere har oplevet økonomiske tab, og så er mængden af datatab vokset betydeligt. Her kan ransomware og/eller manglende sikkerhedskopiering være medvirkende årsager.



Kilde: Danskernes informationssikkerhed 2018.

Offentligt ansatte
I 2016 havde 16 procent af de offentligt ansatte været udsat for mindst én af fire trusler mod informationssikkerheden: Infektion med skadelig software, tab af data efter et angreb, tab af data grundet manglende backup, eller at uvedkommende fik adgang til data, vedkommende havde ansvaret for.

I denne undersøgelse er tallet steget til 18 procent. Der er således sket en lille stigning på to procentpoint.

Der er stadig områder, hvor der er plads til forbedringer. Det gælder eksempelvis disse frie punkter:

> De ansattes manglende efterlevelse af sikkerhedspolitikken.
> Manglende backup.
> Manglende kryptering af mails med følsomme oplysninger.
> Genbrug af adgangskoder.

Otte procent oplyser, at de har oplevet datatab som følge af manglende backup, mens en procent har oplevet, at uvedkommende har fået fat i de data, de har ansvaret for. En bedre sikkerhedskopiering vil give højere produktivitet.

Én ud af tre har sendt cpr-nummer eller andre personlige oplysninger via mail. 21 procent af dem i åbne mails uden kryptering.

Det tyder på, at reglerne i den nu ophævede sikkerhedsbekendtgørelse fra juni 2000 ikke har været implementeret korrekt, eller informationen omkring reglerne har været mangelfuld. Efter implementeringen af persondataforordningen burde myndighederne også være mere opmærksomme på reglerne.

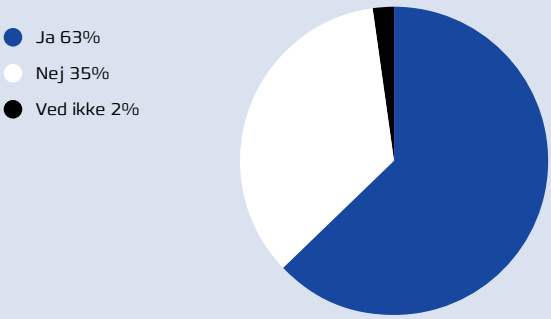
Information vedrørende sikkerhedspolitikker er ligeledes et område med plads til forbedring (se Figur 11).

Ud over analyser og tal, kan du finde anbefalinger til god informationssikkerhed i rapporten. Denne udgave er udarbejdet i et samarbejde mellem Digitaliseringsstyrelsen, KL, Danske Regioner og DKCERT, DeiC.

Du kan finde hele rapporten via DKCERTs webside: https://www.cert.dk/da/information/borgernes_informationssikkerhed

Figur 11: Er du blevet informeret om sikkerhedspolitikken?

Det er langt fra alle arbejdsgiverne i den offentlige sektor, der har informeret medarbejderne om deres informationssikkerhedspolitik.



Kilde: Danskernes informationssikkerhed 2018.

3.5. ÅRETS SÅRBARHEDER

2018 blev igen et rekordår med hensyn til det registrerede antal af sårbarheder. USA's National Vulnerability Database registrerede således 16.555 sårbarheder i 2018 (se Figur 12). I 2017 var tallet på 14.643. Der er således fundet lige knap 2.000 flere sårbarheder i år (se Figur 13).

1.465 sårbarheder fik i 2018 den højeste risikovurdering. Det vil sige, at de var udstyret med en CVSS-score (Common Vulnerability Scoring System) mellem 9 og 10. Det svarer til 8.9 procent (se Figur 14).

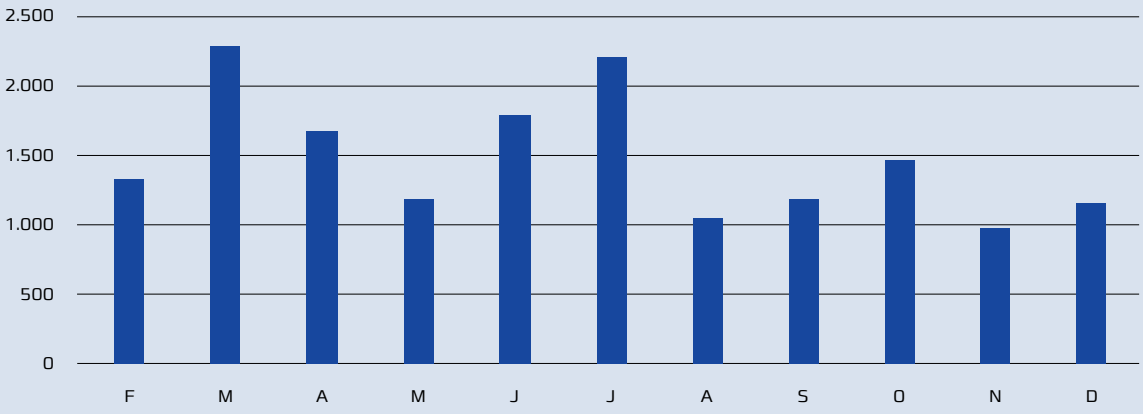
CVSS er en åben standard, der anvendes til at beskrive, hvor alvorlig en sårbarhed er. Skalaen går fra 0 til 10, hvor 10 er mest alvorlig.

I 2017 var antallet af sårbarheder med en risikovurdering på 9 eller derover på 10,4 procent.

De forskellige typer sårbarheder kan ses i Figur 15. Listen over leverandørernes sårbarheder kan du finde i Figur 16. Vær dog opmærksom på, at en leverandør kan have mange forskellige produkter.

Figur 12: Indberetninger om sårbarheder i 2018 fra National Vulnerability Database

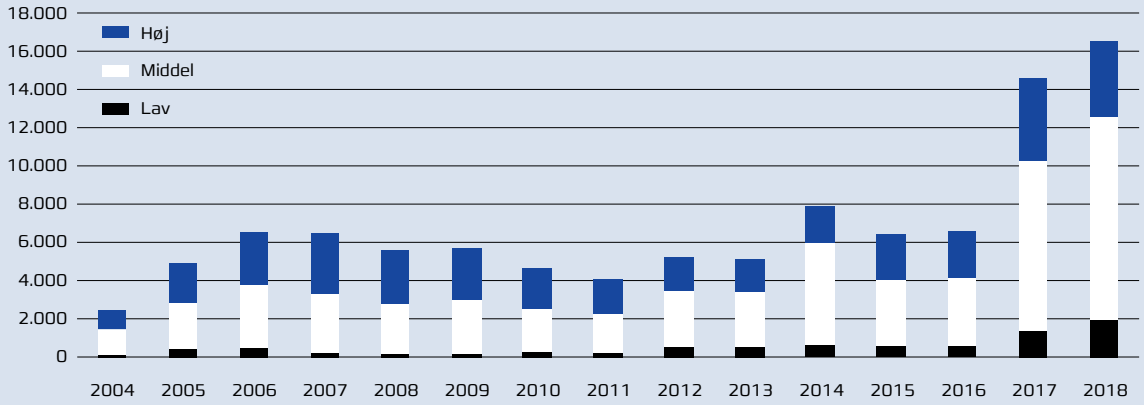
Opgørelse over sårbarheder pr. måned i 2018 fra National Vulnerability Database.



Kilde: National Vulnerability Database og CVE Details

Figur 13: Indberetninger om sårbarheder til NVD mellem 2004 og 2018

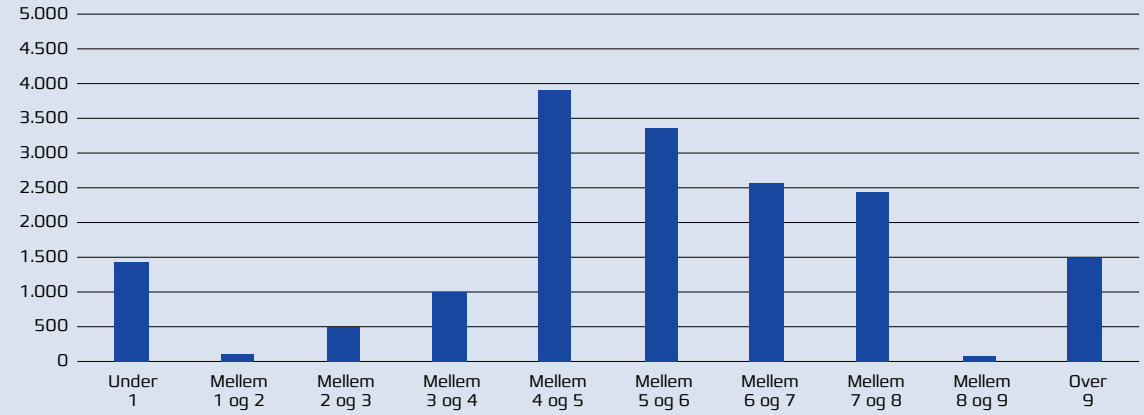
Sårbarheder registreret i USA's National Vulnerability Database 2004-2018.



Kilde: National Vulnerability Database og CVE Details

Figur 14: Sårbarheders CVSS i perioden 1. januar til 31. december

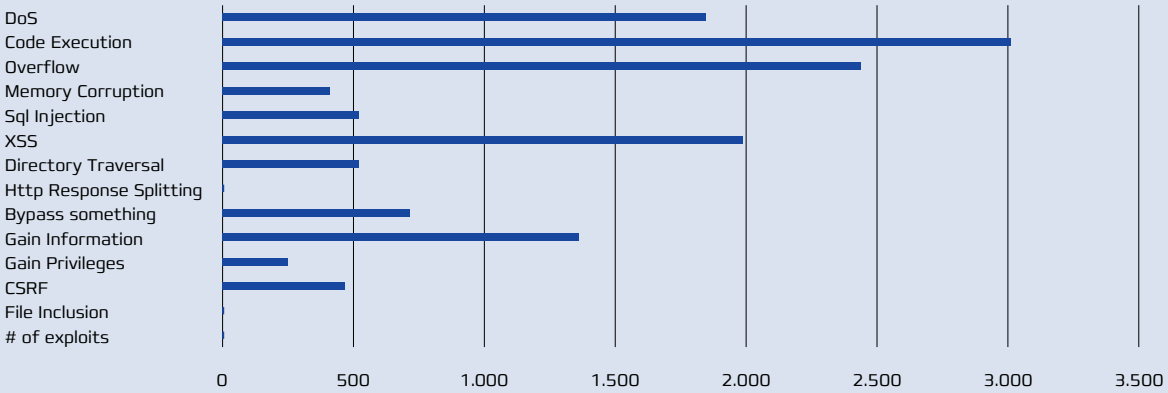
Risikovurdering af sårbarheder fra National Vulnerability Database gennem 2018.



Kilde: National Vulnerability Database og CVE Details

Figur 15: Antal sårbarheder efter type i 2018

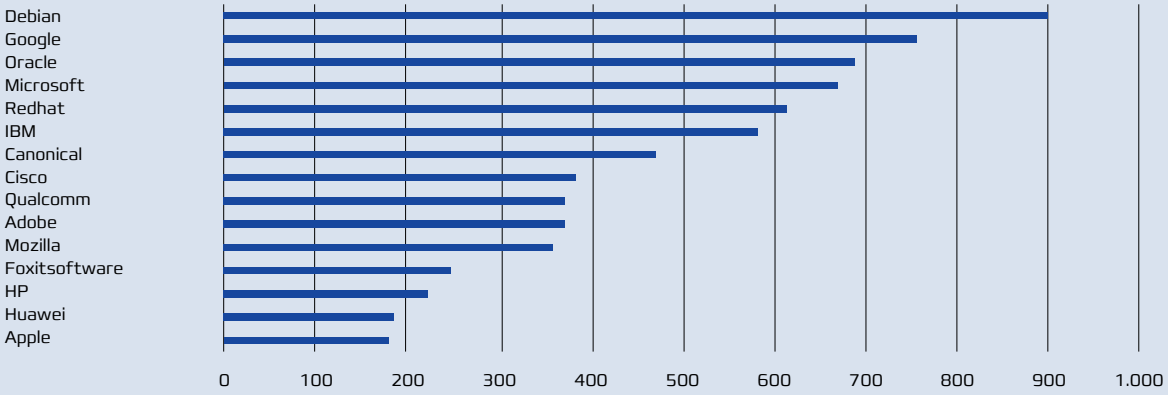
Sårbarheder fordelt på type.



Kilde: National Vulnerability Database og CVE Details

Figur 16: Top-15 over unikke sårbarheder i 2018 fordelt på leverandører

Top-15 listen over de leverandører med flest sårbarheder i 2018. Vær opmærksom på at en leverandør kan have mange forskellige produkter.



Kilde: National Vulnerability Database og CVE Details

3.6. 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, der bør foretages for at højne sikkerheden på den enkelte institution.

Scanningstjenesten har gennem 2018 således udviklet sig fra at være traditionelle sårbarhedsscanninger til at blive meget mere grundige rapporter, der indeholder en egentlig vurdering af de fundne sårbarheder og anbefalinger til institutionens prioritering og håndtering af disse. Ud over en mere grundig analyse er antallet af udførte scanninger ligeledes steget betydeligt. I 2017 udførte DKCERT 94 scanninger, i 2018 var tallet på 121 (se Figur 17).

I 2018 scannede DKCERT 184.698 eksterne IP-adresser. I 2017 var tallet på 204.638 scannede IP-adresser, men dette tal indeholder både eksterne og interne scanninger. Fraregnes de interne scanninger i 2017-tallet, bliver det sammenlignelige tal på 163.235 eksterne scanninger. Der er således sket en stigning på 21.461 i antallet af eksterne scanninger fra 2017 til 2018 (se Figur 18).

18.847 IP-adresser svarede på vores forsøg på scanning, og vi fandt sårbarheder på 13.705 af dem. Det høje tal kan hænge sammen med, at antallet af sårbarheder generelt er i stigning.

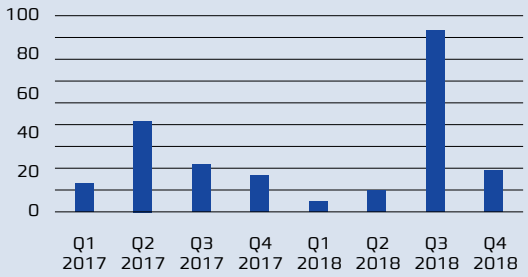
I 2018 viste scanningerne 38.701 sårbarheder. I 2017 var tallet på 29.299, hvilket betyder en stigning på cirka 9.400.

En anden del af forklaringen på denne stigning i antallet af fundne sårbarheder er, at institutionerne har øget frekvensen af scanninger: Hvor de før blev scannet en-to gange om året, scannes flere af dem nu hvert kvartal eller mere. Vær dog opmærksom på, at hvis institutionen samtidig er længe om at opdatere software, tæller den samme sårbarhed med i flere scanninger.

Risikovurderingerne i forbindelse med de eksterne scanninger fortæller, at seks procent af sårbarhederne er kritiske, 13 procent er høj, 61 procent er middel og 21 procent er lav (se Figur 19).

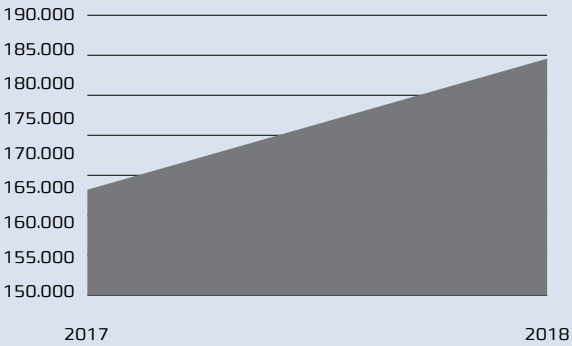
Figur 17: Antal sårbarhedsscanninger i 2017 og 2018

I 2017 udførte DKCERT 94 scanninger. I 2018 var tallet på 121.



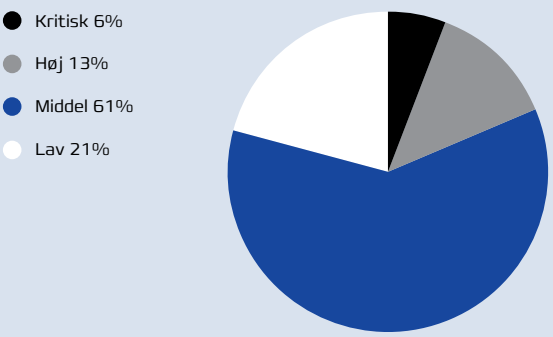
Figur 18: Eksterne scanninger af IP-adresser

Der er sket en stigning på 21.461 i scannede IP-adresser.



Figur 19: Risikovurdering 2018

Langt hovedparten af sårbarhederne, der blev fundet i de eksterne scanninger i 2018, fik risikovurderingen middel.



Kilden til sårbarheder opstår i services, applikationer, operativsystemer og konfigurationer. Nedenfor har vi kategoriseret de sårbarheder, der optræder oftest i vores eksterne scanninger af institutionernes IP-adresser.

Sårbarhedernes opdeling er baseret på OWASP TOP 10 web-applikationer 2018 og er markeret med en de tre mest anvendte sårbarheds-identifikationsmærker:

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

INJECTION

SQL Injections

- CGI Generic SQL Injection (blind)
- CGI Generic SQL Injection
- CGI Generic SQL Injection (Parameters Names)
  [CWE: 20, 77, 801, 810, 89, 91, 203, 643, 713, 722, 727, 751, 928, 929]
- CGI Generic SQL Injection (2nd pass)
  [CWE: 20, 77, 89, 713, 722, 727, 751, 801, 810, 928, 929]
- CGI Generic 2nd Order SQL Injection Detection (potential)
- CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass)
- CGI Generic Header Injection
  [CWE: 113, 93]
- Bash Remote Code Execution
  [CVE-2014-6277 / CVE-2014-6278] (Shellshock)
- PHP 7.1.x < 7.1.25 Arbitrary Command Injection Vulnerability
  [CVE-2018-19158]
- PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
  [CVE-2012-1823, BID: 53388]

Cross-Site Scripting (XSS)

- Web Server Generic XSS
  [CVE-2002-1060, CVE-2002-1700, CVE-2003-1543, CVE-2005-2453, CVE-2006-1681, CVE-2012-3382]
- MediaWiki API XSS
  [CVE-2011-1587]
- CGI Generic XSS (quick test)
- CGI Generic XSS (extended patterns)
- CGI Generic XSS (comprehensive test)
  [CWE: 20, 74, 79, 80, 81, 83, 84, 85, 86, 87, 116, 442, 692, 712, 722, 725, 751, 801, 811, 928, 931]

Sensitive data exposure

- SSL Medium Strength Cipher Suites Supported
  [CVE-2013-4508]
- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
  [CVE-2014-3566]
- SSL Version 2 and 3 Protocol Detection
  [CVE-2014-3566]
- TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
  [CVE-2014-8730]
- SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
  [CVE-2016-0800]
- SSLv2 Cross-Protocol Session Decryption Vulnerability (DROWN)
  [CVE-2016-0800]
- OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities (DROWN)
  [CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800]
- SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
  [CVE-2011-3389]
- SSL Weak Cipher Suites Supported
  [CWE: 326, 327, 720, 753, 803, 928, 934]
- SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
  [CVE-2015-0204]
- SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
  [CVE-2016-2183, CVE-2016-6329]
- Transport Layer Security (TLS) Protocol CRIME Vulnerability
  [CVE-2012-4929, CVE-2012-4930]
- SSL Certificate with Wrong Hostname
  [CVE-2013-2037]
- SSL Self-Signed Certificate
  [CVE-2017-14582]
- SSL Certificate Signed Using Weak Hashing Algorithm
  [CVE-2004-2761]
- SSH Protocol Version 1 Session Key Retrieval
  [CVE-2001-0361, CVE-2001-0572, CVE-2001-1473]
- Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
  [CVE-2002-1623]
- Cisco ASA / IOS IKE Fragmentation Vulnerability
  [CVE-2016-1287]
- Internet Key Exchange (IKE) v 1 Authentication implementation
  [CVE-2005-3732]
- WordPress User Enumeration
  [2017-5487]
- Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure
  [CVE-2017-6168, CVE-2017-17382]

F5 BIG-IP Cookie Remote Information Disclosure

- SSH Weak Algorithms Supported
- SSL Certificate Cannot Be Trusted

Security Misconfiguration and Non-Compliance

> HTTP TRACE / TRACK Methods Allowed
[CVE-2003-1567, CVE-2004-2320, CVE-2010-0386]
> Web Application Potentially Vulnerable to Clickjacking
[CWE: 693]
> SSL Certificate with Wrong Hostname
[CVE-2013-2037]
> SSL Self-Signed Certificate
[CVE-2017-14582]
> SSL Certificate Expiry
> SSL Certificate Cannot Be Trusted
> IIS Detailed Error Information Disclosure

Using Components with known vulnerabilities

> PHP Unsupported Version Detection (PHP 5.6.x < 5.6.32 & PHP 7.2.x < 7.2.5)
[CVE-2016-3074, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544]
> Apache Unsupported Version Detection (Apache 2.4.x < 2.4.35)
[CVE-2017-15710, CVE-2017-15715, CVE-2018-1283, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-2018-1312]
> SSL Version 2 and 3 Protocol Detection
[CVE-2014-3566]
> Joomla! Unsupported Version Detection
[CWE: 16]
> Atlassian JIRA Unsupported Version Detection

Microsoft Operating System/Servers Unsupported Version Detection

> Microsoft Exchange Server Unsupported Version Detection
> Microsoft Windows Server 2003 Unsupported Installation Detection
> Microsoft IIS 6.0 Unsupported Version Detection
> Microsoft-IIS/7.5 2010 SP1-version: 14.1.438.0

Unix/Linux Operating System Unsupported Version Detection

> Fedora Linux Operating System - Fedora release 13
> Debian Linux Operating System - Debian 6.0 & 7.0
> Red Hat Enterprise Linux 3 support ended on 2010-10-31.
> Debian 7.0 support ended on 2016-04-26 end of regular support
> / 2018-05-01 (end of long-term support for Wheezy-LTS).
> Unix FreeBSD 8.3 support ended on 2014-
> CentOS release 5
> Ubuntu 10.04




Broken Authentication

> WordPress User Enumeration
[CVE-2017-5487]

Broken Access control

> Microsoft Exchange Client Access Server Information Disclosure
[BID: 69018]
> Web Server Directory Enumeration
[OWASP-CM-006]
> CGI Generic Local File Inclusion
[CWE: 73, 78, 98, 473, 632, 714, 727, 928, 929]
> Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing
[CVE-2001-1446]
> Web Server info.php / phpinfo.php Detection
[CWE: 200]
> Microsoft Exchange Client Access Server Information Disclosure
[BID: 69018]
> Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check)
[CVE-2012-2532]
> Apache Tomcat Default Files
[CWE: 20, 74, 79, 442, 629, 711, 712, 722, 725, 750, 751, 800, 801, 809, 811, 864, 900, 928, 931, 990]
> Backup Files Disclosure
> F5 BIG-IP Cookie Remote Information Disclosure
> Web Application SQL Backend Identification

3.7. ADVARSLER FRA TREDJEPARTER

I 2018 udsendte DKCERT 61.500 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.

DKCERT udsender automatisk disse advarsler hver dag, mandag til fredag. Derfor kan det samme sårbare system 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 5210 advarsler i 2018 (Se Figur 20).

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.

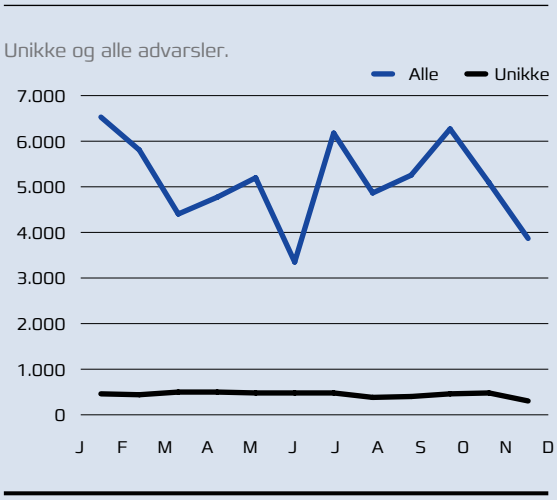
Institutionerne har ligeledes mulighed for at fravælge advarsler. Det kan fx skyldes, at man er klar over, at en IP-adresse er sårbar, men at man først kan fjerne sårbarheden om nogen tid. I mellemtiden kan institutionen slippe for at få advarsler om den. Herunder kan du se de tre mest almindelige advarsler.

3.7.1. POODLE-sårbarheden

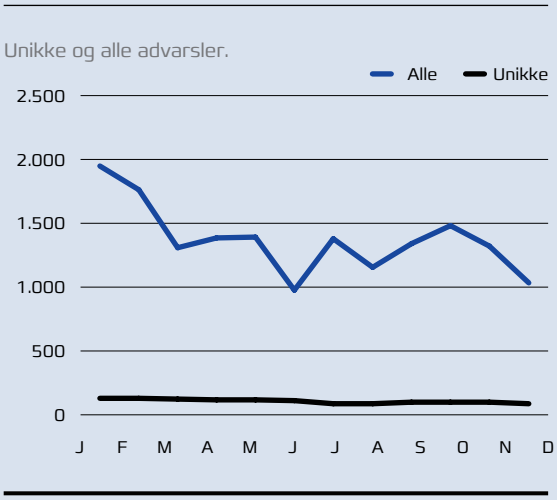
Med en hyppighed på 16.424 handlede hovedparten af advarslerne om sårbarheden POODLE (Padding Oracle On Downgraded Legacy Encryption) (Se Figur 21).

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.

Figur 20: Advarsler fra tredjepart modtaget i 2018



Figur 21: Advarsler om POODLE



3.7.2. Åbne RDP-computere

Advarsler om åbne RDP-computere (Remote Desktop Protocol) tegnede sig for 12.190 af årets advarsler. 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 22).

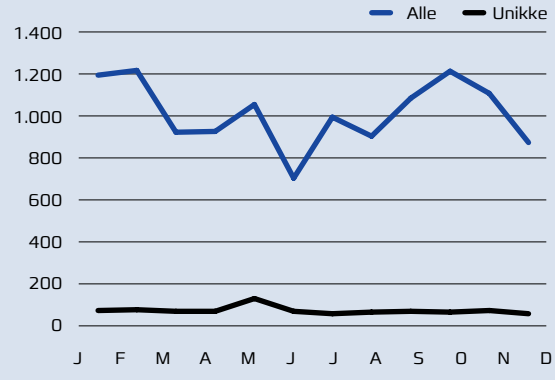
3.7.3. Åbne tidsservere

Nummer tre på listen over de hyppigst forekommende advarsler, med 4668 forekomster, var NTP (Network Time Protocol). NTP-servere bruges til at stille uret på computere via netværk.

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 23).

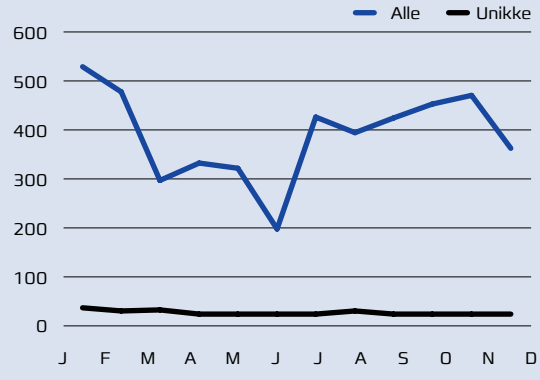
Figur 22: Advarsler om åbne RDP-systemer (Remote Desktop Protocol)

Advarsler om RDP, der giver mulighed for fjernstyring.
Unikke og alle advarsler.



Figur 23: Advarsler om åbne NTP-servere (Network Time Protocol)

Advarsler om åbne NTP-servere.
Unikke og alle advarsler.



4. 2018 – året i ord

DKCERT introducerede awareness-tjenesten Phish, der kan oplyse brugeren om trusler fra phishing i et trygt miljø, og DPO-tjenesten bed sig godt fast på institutionerne.

4.1. DKCERTS AKTIVITETER I ÅRETS LØB

4.1.1. Information om sikkerhed

DKCERT informerede løbende om aktuelle trusler, sårbarheder og sikkerhedshændelser på web, via fire ugentlige nyhedsbreve og Twitter. Ved udgangen af 2018 abonnerede 1.577 personer på et eller flere af DKCERTs nyhedsbreve. Ved udgangen af 2017 var tallet på 1.586 (se Figur 24).

Twitter bliver dog en stadig mere populær kanal til information om informationssikkerhed, hvilket også kan læses i antallet af følgere. 2439 fulgte således DKCERT på Twitter ved udgangen af 2018. I 2017 var tallet på 2065 (se Figur 25).

Cert.dk fik 51.408 besøg på cert.dk i 2018. I 2017 var tallet på 42.214.

Henrik Larsen optrådte jævnligt som ekspertkilde og klummeskribent i medierne i årets løb. Siden maj 2018 har vi samlet information om hvilke medier, der anvender DKCERT som kilde. Det samlede antal medieklip i perioden er på 51 (se Figur 26).

Chefen for DKCERT er desuden medlem af en række danske og europæiske netværk, udvalg og paneler på it- og informationssikkerhedsområdet – blandt andet er han medlem af bestyrelsen for Rådet for Digital Sikkerhed og af National strategi for cyber- og Informationssikkerheds Advisory Board.

4.1.2. DKCERT-CAB

DKCERT-CAB (Change Advisory Board) er et rådgivende organ med repræsentanter for brugerne af DKCERTs tjenester. Gruppen består af en repræsentant for Danske Universiteters CIO-gruppe, to for CISO-forum, en for NetTekRef og en for øvrige institutioner, p.t. Kulturministeriets koncern¬sikkerheds¬koordinator. Formand var informationssikkerhedschef Ole Boulund Knudsen, Aarhus Universitet, indtil november 2018, derefter informationssikkerhedschef Poul Halkjær Nielsen, Københavns Universitet. Man mødtes fire gange i 2018.

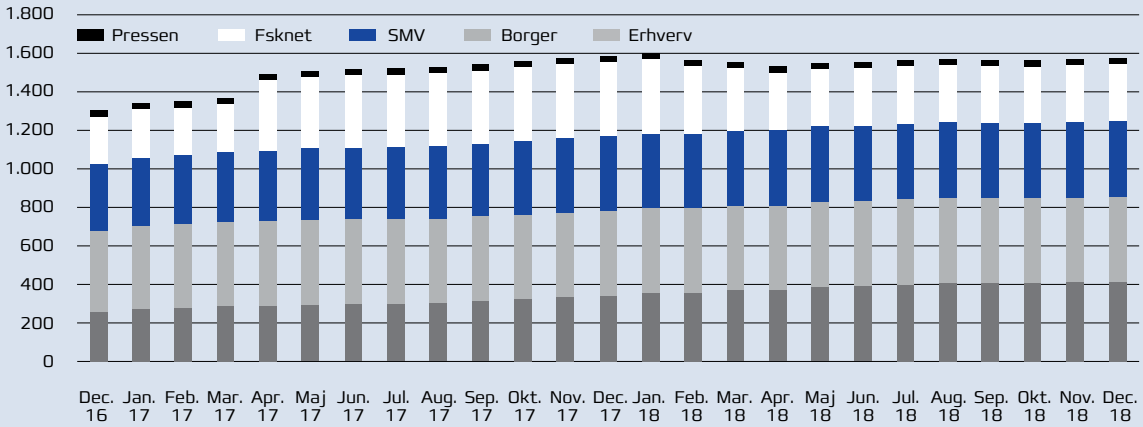
4.1.3. Dataanalyse

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 24: Abonnenter på DKCERTs nyhedsbreve

Antallet af brugere på DKCERTs nyhedsbreve december 2016 - december 2018.



4.1.4. Rådgivning om databeskyttelses-forordningen (DPO-tjeneste)

Universiteter og andre institutioner på forskningsnettet skal som alle andre overholde EU's databeskyttelsesforordning, der trådte i kraft i maj 2018. Til at hjælpe dem med opgaven, introducerede DeiC i 2017 DPO-tjenesten, der er rettet mod databeskyttelsesrådgivere (DPO, Data Protection Officer). Tjenesten er knyttet til DKCERT.

DPO-tjenesten er blevet godt modtaget, og der blev i 2018 indgået aftaler med en række uddannelsesinstitutioner både om fast regelmæssig rådgivning eller mere ad hoc-hjælp. I 2018 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.

I forlængelse af tjenestens opgave med at varetage DPO-funktionen hos en række forsknings- og uddannelses¬institutioner, har tjenesten også oprettet og drifter et netværk for uddannelsesinstitutionernes DPO'er, hvor der i 2018 blev afholdt fire møder og nedsat tre arbejdsgrupper. Samtlige universiteter og professionshøjskoler deltager i netværket sammen med repræsentanter fra KADK, AARCH og Designskolen. Også mellem møderne udveksler og deler netværket løbende informationer om den nyeste praksis og fortolkning i implementeringen på forsknings- og uddannelses¬institutionerne.

Tjenestens medarbejdere deltager i et større netværk af danske DPO'er og i forskellige kompetenceudviklingsaktiviteter.

4.1.5. Internationalt samarbejde

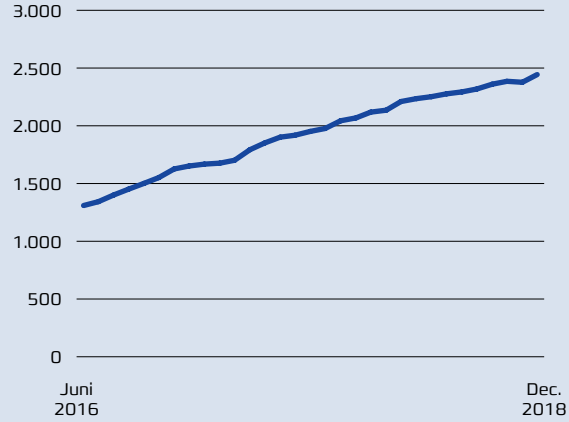
CERT'erne (Computer Emergency Response Team) for de nordiske forskningsnet holder videomøder sammen med NORDUnet-CERT en gang om måneden. På møderne diskuterer deltagerne aktuelle sikkerhedshændelser og erfaringer med værktøjer og metoder.

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 har været repræsenteret ved de tre møder, dette store netværk har afholdt i 2018.

DKCERT er også medlem af FIRST.org (Forum of Incident Response and Security Teams), som er en organisation for mere end 460 CERT/CSIRT-teams

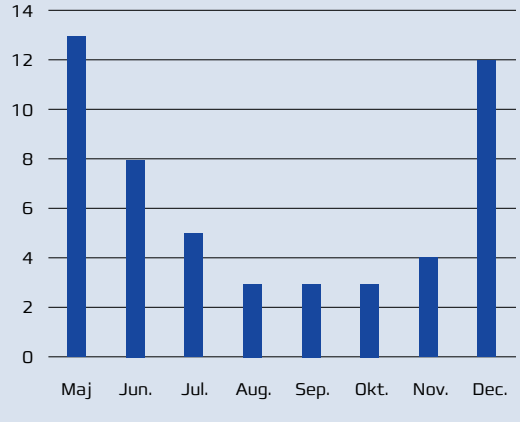
Figur 25: DKCERT på Twitter

Antallet af følgere på Twitter juni 2016 - December 2018.



Figur 26: DKCERT-presseklip/interviews

Presseomtale i perioden maj til december 2018.



i 91 lande. Tre DKCERT-medarbejdere deltog i FIRSTs regionale seminar i Hamburg i februar. To deltog i årskonferencen og generalforsamlingen, der fandt sted i Malaysia.

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 han 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.

Fem medarbejdere fra DKCERT deltog i en workshop om krisehåndtering arrangeret af GÉANT i regi af SIG-ISM og SIG-MARCOMMS (GÉANTS special interest group for markedsføring og kommunikation), i Malaga i november.

Projektleder Morten Eeg Ejrnæs Nielsen var i august 2017 med til at etablere en ny arbejdsgruppe under GÉANT, TF-DPR (Task Force Data Protection Regulation). Han blev valgt til formand for styregruppen i taskforcen og indtager stadig denne rolle.

4.1.6. Ny tjeneste: Phishing-test

DKCERT har afsluttet arbejdet med at udvikle en 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.

Tjeneste blev meldt klar til brug ultimo 2018, og der er derfor ingen data for 2018.

4.2. TENDENSER OG TRUSLER I 2018

4.2.1. Afpresning på flere måder

En tendens fortsatte uændret i 2018: It-kriminelle går i høj grad efter økonomisk gevinst, og forskellige former for afpresning er en populær metode.

Ransomware

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.

I Danmark har seks procent været ramt af ransomware på deres pc i 2018. Det er en smule lavere end i 2016, hvor ransomware ramte otte procent. 17 procent af de ramte fik ikke data tilbage efter at være blevet ramt af ransomware. Det er mere end en fordobling i forhold til 2016, hvor det tal var godt otte procent. Der er således en relativ stor risiko for, at man ikke ser sine data igen, hvis man bliver ramt af ransomware. Kilden til disse oplysninger er Danskernes informationssikkerhed 2018.

Problemet rammer ikke mange, men for den enkelte kan det være et alvorligt problem at miste adgang til sine data.

Sextortion

En anden angrebsmodel, der er dukket op flere gange i 2018, er de såkaldte sextortion-kampagner.

De kriminelles arbejdsgang er, at de udsender en mail, som påstår, at afsenderen har intime 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 penge for at ofret kan undgå, at materialet bliver offentliggjort til eksempelvis Facebook-venner.

Overbelastning

En tredje form for afpresning går ud på, at de kriminelle truer med at udføre angreb mod offerets it-systemer. Et større overbelastningsangreb kan sætte systemer ud af drift, så kunder fx ikke kan købe ind i webshoppen eller lægge en spiltjeneste ned.

Den type angreb har vi også set i 2018, og usikre IoT-enheder har vist sig som en effektiv platform for denne type overbelastningsangreb. Ligeledes er lyssky online-tjenester, der udbyder overbelastningsangreb, lettilgængelige og billige at benytte.

DKCERT MENER

Udbredte afpresnings- og ransomware-angreb understreger behovet for sikkerhedskopiering. Med en sikkerhedskopi kan man 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.

Begrænsning af lokaladministrative rettigheder nedsætter også sandsynligheden for infektion med ransomware og andet malware.

Udvalgte referencer fra cert.dk:

Ny ransomware-kampagne går efter virksomheder og kræver store beløb
https://www.cert.dk/da/news/2018-08-23/ryuk

Vær opmærksom på en bølge af sexafpresningsbeskeder
https://www.cert.dk/da/news/2018-07-17/sextortion

Antallet af ransomware-familier er faldende
https://www.cert.dk/da/news/2018-05-09/ransomware

Ransomware lægger informationsskærme ned
https://www.cert.dk/da/news/2018-09-18/ransomware

4.2.2. CPU'erne blev ramt

Året begyndte med et par alvorlige sårbarheder, Meltdown og Spectre, som i forskellige varianter har hærget hele 2018. Flere af disse, såkaldte side channel-angreb, er nemlig kommet til i løbet af året eksempelvis Foreshadow, der også omtales som L1 Terminal Fault, fordi den henvender sig til processorens L1 data-cache.

Det drejer sig om sårbarheder i de processorer, der indgår i computere, smartphones og andet udstyr omkring os. Dele af sårbarhederne kan rettes i software, andre kræver hardwareopdateringer, der er mere avanceret.

I et side channel-angreb tilgås fortrolige data ikke direkte, men ved at observere andre arbejdsdata i CPU'en, kan angriberen slutte sig til, hvad de fortrolige data er. CPU-producenterne har arbejdet hårdt på at få løst problemerne gennem hele året, men er stadig ikke i mål.

DKCERT MENER

Producenterne af processorer og styresystemer bør udvirke sikre tilstande omkring CPU'erne. Der bør stilles krav til producenterne om sikkerhedsrettelser.

I virtualiserede løsninger er side channel-problemet ekstra stort, da CPU'erne fordeler databehandlingen mellem forskellige brugerløsninger. Derved kan én sårbarhed i én processor ramme mange forskellige kunder af en virtuel løsning.

Udvalgte referencer fra cert.dk:

Intel fortæller nu om en ny sårbarhed i familie med Spectre og Meltdown
https://www.cert.dk/da/news/2018-08-16/Foreshadow

Google og Microsoft beretter om to nye Spectre-varianter
https://www.cert.dk/da/news/2018-05-22/Spectre

Intel udsender flere firmware-opdateringer mod Spectre
https://www.cert.dk/da/news/2018-02-23/Intel

4.2.3. Krypto-valutaer ramte himlen - men faldt ned igen

En af begrundelserne for, at it-kriminelle har fået massiv fokus på området er, ifølge sikkerhedsfirmaet McAfee, at krypto-valutaer er steget så eksplosivt i de seneste år. Der er med andre ord opstået en ny guldfeber.

Pengene i en krypto-valuta dannes som regel ved såkaldt mining. Det går ud på, at et program foretager en række beregninger. Kriminelle tager i hemmelighed andres computere i brug med henblik på at udvinde krypto-valutaer ved mining. Angrebene på andre computere gennemføres ofte, uden at computerejerne selv er opmærksomme på det, ved at installere små programmer til beregning af krypto-valuta.

Sikkerhedsfirmaet McAfee noterer også, at malware-udviklerne gennem 2018 skifter fokus fra ransomware til kryptovaluta, og der er ingen tvivl om, at kryptovaluta har haft stigende interesse blandt it-kriminelle i året der gik.

DKCERT MENER

Krypto-valutaer giver kriminelle mulighed for at skabe sig adgang til anonyme betalinger for deres afpresning og andre ulovlige aktiviteter, hvilket er bagsiden af medaljen med hensyn til de digitale valutaer.

Samtidig sker der et ikke uvæsentligt strøm/ressource-tyveri i forbindelse med ulovligt installerede mining-programmer på uvidende brugers computere. Produktionen af krypto-valuta er meget el-forbrugende.

Udvalgte referencer fra cert.dk:

Ny rapport: Angreb mod krypto-valutaer er det nye sort blandt it-kriminelle
https://www.cert.dk/da/news/2018-07-03/kryptovaluta

4.2.4. Adgangskoder/password

Adgangskoder har været et af fokusområderne i 2018, hvilket helt konkret har udmøntet sig i, at anbefalingerne til et godt password er blevet strammet op.

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 i dag mere end kompleksitet med store bogstaver, tal eller specialtegn, som hidtil har været prioriteret højt. Et godt password skal derfor være på mere end 12 tegn – men kompleksitivitet hjælper stadig. Vigtigst er dog, at brugeren kan huske sine passwords, så fristelsen til at genbruge ikke bliver for stor.

Med den computerkraft, der er til rådighed eksempelvis gennem de kriminelles botnet, kan de korte adgangskoder nemlig hurtigt knækkes, uanset om der er brugt store eller små bogstaver. Men i takt med at længden på din adgangskode øges, øges de kriminelles regne-tider også markant, hvilket giver bedre sikkerhed. Ligeledes er anbefalingen om, at en adgangskode ikke må genbruges på tværs af tjenester naturligvis stadig gældende.

I rapporten Danskernes informationssikkerhed 2018, 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 er således i underkanten af, hvad anbefalingerne til et godt password er (se Figur 27).

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.

De 37 procent er en klar forbedring i forhold til tal fra 2016, hvor 66 procent anvendte samme password til flere tjenester, der er altså sket et markant fald, hvilket er positivt

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 sørge for, at der er forskellige og stærke adgangskoder til alle. Slet eventuelt de konti, du ikke benytter mere.

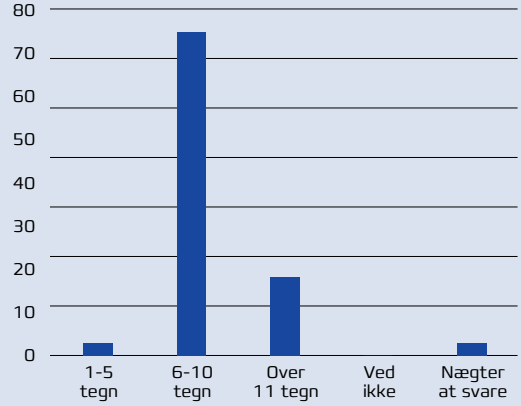
Udvalgte referencer fra cert.dk:

CFCS: Halvdelen af danskerne genbruger passwords
https://www.cert.dk/da/news/2018-10-12/password

Her er de ti mest anvendte adgangskoder
https://www.cert.dk/da/news/2018-12-17/password

Figur 27: Hvor langt er dit password?

Så langt er danskernes password.



Kilde: Danskernes informationssikkerhed 2018

4.2.5. Et år med store datalækager OG GDPR

2018 har – igen - været et år med enorme datalæk. To hotelkæder, en fitness app og to sociale medier står for dataproblemer, der alene berører cirka 15 procent af klodens befolkning. Det er blot et par enkelte eksempler ud af talrige.

Blandt de største datalæk i 2018 er:

Hotelkæden Starwood, der er en underafdeling af Marriott-kæden, berettede i slutningen af 2018 om, at der havde været uautoriseret adgang til virksomhedens reservationsdatabase siden 2014 og helt frem til den 10. september 2018. Potentielt kunne problemet ramme 500 millioner gæster.

Huazhu Hotels Groups er Kinas største hotelkæde, og også her var der problemer. En kæmpe database med informationer om 130 millioner gæster blev lækket og sat til salg.

Fitness-appen, Fitness Pal, der ejes af sportsvirksomheden Under Armor, lækkede 150 millioner brugeres data.

Også de social medier havde deres problemer. Twitter måtte bede sine brugere om at skifte password til tjenesten. På grund af en fejl blev adgangskoder lagret i en intern log, før hashing-processen blev udført. Her var 330 millioner konti berørt.

Facebook havde problemer med 147 millioner konti i forbindelse med tre episoder, hvor analysefirmaet Cambridge Analytica, der er sat i forbindelse med det amerikanske valg, nok var den mest omtalte.

Farvel til Google+

Googles bud på et socialt netværk, kaldet Google+, er ved at være fortid. Søgegiganten berettede i 2018, at den lukker helt ned for tjenesten, hvilket vil ske i 2019.

Denne melding kom i forlængelse af, at oplysninger fra flere hundrede tusinde profiler blev kompromitteret. Det har angiveligt været muligt, at eksterne kunne tilgå oplysninger som navn, e-mail, bopæl, arbejde eller køn i profilerne på tjenesten.

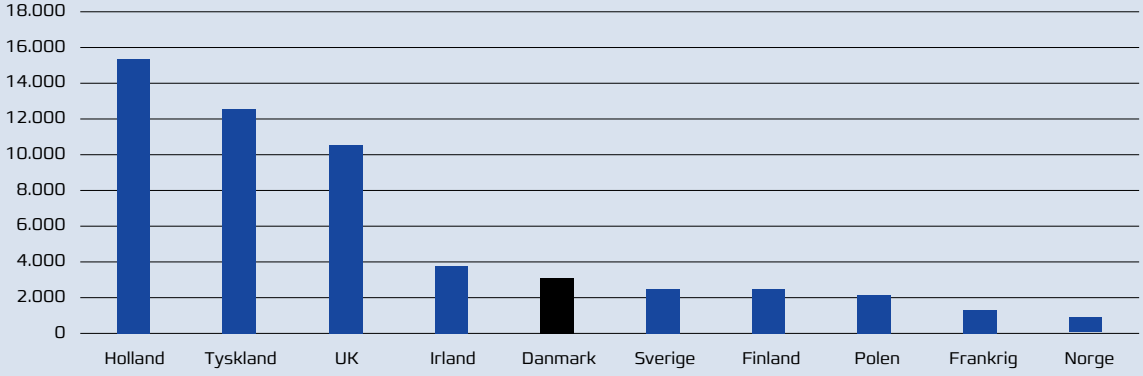
Ganske kort tid efter denne opdagelse måtte Google erkende et nyt problem, hvor op mod 50 millioner konti var kompromitteret. Derfor har virksomheden nu besluttet, at lukningen af det sociale medie fremskyndes fra august 2019, der var den oprindelige plan, til april 2019.

GDPR og læk i Danmark

I Danmark blev terapi-portalen GoMentor trukket frem i lyset for problemer med sikkerheden i forbindelse med brugernes data. Datatilsynet meldte GoMentor til politiet, der skal hjælpe myndigheden med at efterforske sagen.

Figur 28: Antal rapporterede databrud i EU fra 25. maj 2018 til 28. januar 2019

I Danmark har der været 3.100 indberetninger frem til den 28. januar 2019. Bemærk, at opgørelsen løber frem til den 28. januar 2019. Datatilsynet oplyser, at de i 2018 har modtaget 2.780 indberetninger.



Kilde: DLA Piper og Datatilsynet

Implementering af GDPR betyder også, at der siden maj 2018 indberettes om mange nye danske dataproblemer til Datatilsynet. I perioden fra 25. maj til udgangen af 2018 kom der ifølge Datatilsynet i alt 2.780 af disse anmeldelser (se Figur 28). De afgørelser, der for alvor skal være med til at afgøre hvor højt barren skal sættes i forbindelse med straffen, har vi dog stadig til gode.

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 også forventes fremover.

I den sammenhæng er gode password-vaner vigtige. Separate passwords til hver tjeneste er et nøglepunkt i forhold til datalæk. Omtanke for hvilke data du afgiver til hvem, er nødvendig.

Udvalgte referencer fra cert.dk:

Udskiftning af 14.000 betalingskort efter datalæk i flyselskab kan være nødvendig
https://www.cert.dk/da/news/2018-09-11/nets

Data om 130 millioner hotelgæster er sat til salg
https://www.cert.dk/da/news/2018-08-31/kina

Kæmpe hotelkæde fortæller nu om datalæk, der har stået på siden 2014
https://www.cert.dk/da/news/2018-12-03/data

92 millioner konti ramt af datalækage hos MyHeritage
https://www.cert.dk/da/news/2018-06-19/MyHeritage

Facebook: 29 millioner konti blev kompromitteret
https://www.cert.dk/da/news/2018-10-15/facebook

Google+ lægges i graven på grund af problemer med datasikkerheden
https://www.cert.dk/da/news/2018-10-09/google

Sjusk med persondata udløser en bøde på over 7 mio. kroner
https://www.cert.dk/da/news/2018-11-28/uber

Dansk Erhverv: GDPR koster danske virksomheder 8 mia. kroner
https://www.cert.dk/da/news/2018-05-22/gdpr

4.2.6. Router-angreb med VPNFilter

Federal Bureau of Investigation (FBI) advarer i midten af 2018 om router-problemer. Det skete på grund af, at FBI registrerede, at routere og netværksenheder i hundredetusindevis var blevet kompromitteret rundt omkring på kloden. Man anslår, at omkring 500.000 routere og NAS-enheder blev berørt.

Det var den ondsindede kode, kaldet VPNFilter, der blev benyttet til at angribe de mange hjemmerouter og netværksenheder i mindre virksomheder. Koden var i stand til at udføre flere opgaver, eksempelvis at indsamle informationer, udnytte enhederne eller blokere for netværkstrafik.

DKCERT MENER

Sagen om VPNFilter illustrerer, hvor afgørende det er at holde software opdateret. Når udviklere af software udsender rettelser, der lukker alvorlige sikkerhedshuller, er det kun et spørgsmål om tid, før it-kriminelle begynder at udnytte hullerne: Opdater altid med de nyeste rettelser fra producenten.

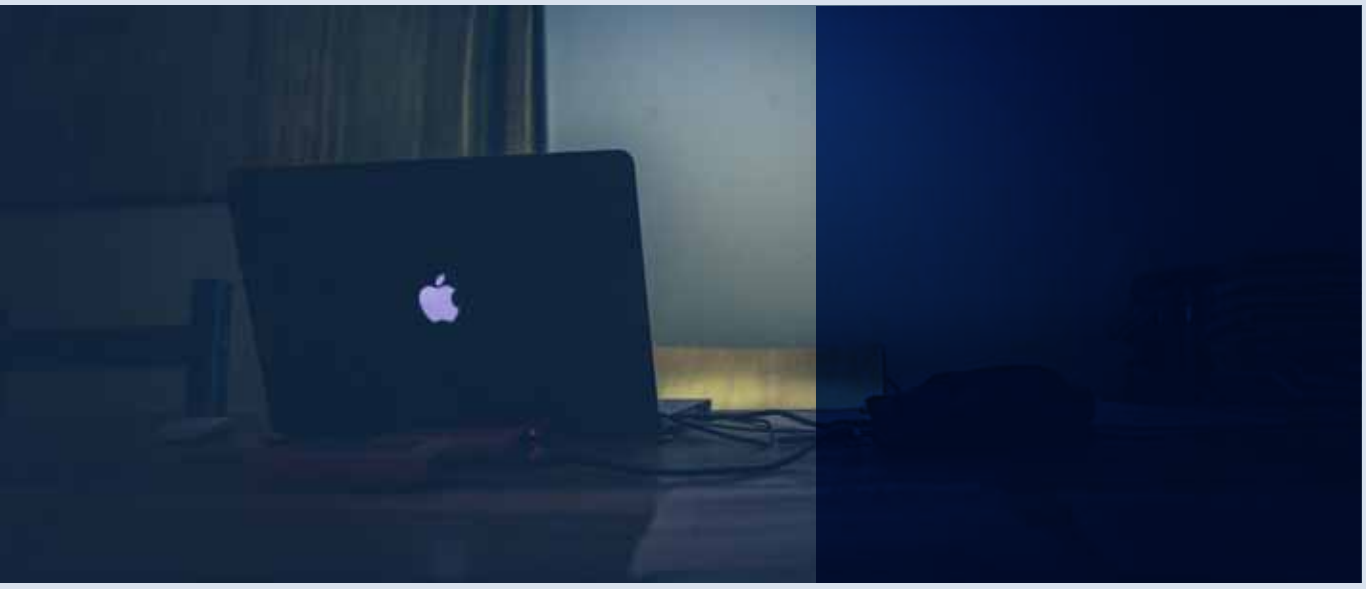
Husk at ændre standard-password på alle dine eksterne enheder, som routere, kameraer eller eksterne harddiske.

Disse store malware-kampagner kan give anledning til at tage en offentlig diskussion omkring nødvendigheden af eksempelvis en mærkningsordning eller officielle mindstekrav for it-sikkerhed.

Udvalgte referencer fra cert.dk:

VPNFilter spøger igen trods nedlukning
https://www.cert.dk/da/news/2018-06-04/vpnfilter

FBI advarer om malware-angreb mod routere og netværksenheder
https://www.cert.dk/da/news/2018-05-28/vpnfilter



5. Det eksterne perspektiv

Seks bidragydere uden for DKCERT giver her deres syn på arbejdet med at leve op til den nationale strategi for cyber- og informationssikkerhed.

I maj kom National strategi for cyber- og informationssikkerhed, der skal ruste landet til at stå skarpere, når det handler om cybersikkerhed. Der er mange tiltag i strategien, der dækker nationen bredt.

Derfor er det vigtigt, at vi får belyst flere tilgange til strategien, der derved kan blive trykprøvet i forholde til synspunkter og fra forskellige dele af it-branchen.

Til at gøre det, har vi inviteret seks eksterne bidragsydere til at give deres mening og holdning til kende.

Bidragsyderne er denne gang:

- Thomas Lund-Sørensen, chef for Center for Cybersikkerhed.
- Rikke Hougaard Zeberg, direktør i Digitaliseringsstyrelsen.
- Birgitte Hass, administrerende direktør, IT-branchen.
- Ole Kjeldsen, direktør for Teknologi og Sikkerhed, Microsoft, og medlem af bestyrelsen i Rådet for Digital Sikkerhed.
- Poul Halkjær Nielsen, informationssikkerhedschef, Københavns Universitet.
- Jakob Willer, direktør, Teleindustrien.

5.1. DEN NATIONALE CYBER- OG INFORMATIONSSIKKERHEDSSTRATEGI

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

Danmark står over for en meget høj cybertrussel, som kan skade landets sikkerhed og økonomi. Regeringen udstikker med den nationale cyber- og informationssikkerhedsstrategi rammen for arbejdet på tværs af myndigheder og sektorer for at styrke Danmark mod cyberangreb.

I Center for Cybersikkerhed (CFCS) er vi i fuld gang med at styrke samarbejdet med resten af samfundet om at gøre den infrastruktur, vores samfund er afhængig af, mere robust, så vi kan modstå truslerne. Da strategien blev lanceret i maj 2018, var blandt andet Digitaliseringsstyrelsen, Erhvervsstyrelsen og Center for Cybersikkerhed klar til at løbe de første initiativer i gang.

For CFCS betød det, at vi i oktober havde de første medarbejdere på plads i CFCS' nye cybersituationscenter. Vi har i dialog med erhvervslivet planlagt et nyt uddannelsesforløb, som skal give os de dygtige folk, der blandt andet bliver nødvendige i takt med, at vi udbygger cybersituationscenteret til at være bemandet 24/7.

Samtidig har vi dedikerede rådgivere i vores rådgivningsafdeling, der er i daglig kontakt med sektorerne om informationssikkerhed, ligesom en række af de samfundskritiske sektorer allerede nu har indstationeret en medarbejder i centerets trusselsvurderingsenhed.

5.1.1. Forskellige sektorer

Helt centralt i den nationale strategi er de sektorspecifikke strategier, som de seks samfundskritiske sektorer, energi, finans, sundhed, søfart, transport og tele har udarbejdet. Sektorerne er meget forskellige og har taget fat på opgaven og løst den forskelligt, og det er lige netop derfor, hver sektor skal have sin egen strategi. Sektorstrategierne er udarbejdet af sektorerne i et samarbejde mellem myndighederne og centrale aktører inden for de enkelte sektorer. Sektorerne har udført et stort stykke arbejde, som CFCS og Digitaliseringsstyrelsen samt PET har bidraget til ved at indgå i en task force med henblik på at støtte sektorernes arbejde.

Hver sektorstrategi indeholder en række konkrete initiativer, der skal løfte sikkerhedsniveauet. Bl.a. er der inden for de enkelte sektorer etableret decentrale cyber- og informationssikkerhedsenheder (DCIS), så koordinationen og kommunikationen på tværs af sektorerne håndteres bedst muligt.

DCIS'erne skal bidrage til at gennemføre sektorvise trusselsvurderinger, styrke monitoreringen, sikkerheds- og kompetenceopbygge og rådgive og vejlede myndigheder og virksomheder i sektoren.

Derudover er det op til den enkelte sektor og ansvarlige myndighed at vælge en konstruktion for DCIS'en, som bedst opfylder sektorens behov. CFCS er i tæt dialog med de decentrale enheder og organiserer ud over den daglige dialog med sektorerne et vidensdelingsnetværk, hvor sektorerne kan dele erfaringer og lære af hinanden.

5.1.2. Forebyggende arbejde i fokus

Netop det forebyggende arbejde er et vigtigt indsatsområde. Med det nye forsvarsforlig og den nationale strategi har CFCS fået tilført ressourcer til at udbygge rådgivningskapaciteten til de seks samfundsvigtige sektorer.

Vi skal ikke blande os i, hvordan den enkelte myndighed eller virksomhed løfter sin indsats på cybersikkerhed, men vi skal hjælpe med at sikre, at alle er opmærksomme på de mest relevante trusler og ikke mindst de mest effektive sikkerhedsforanstaltninger. De kan ofte virke banale, men det er afgørende, at den fundamentale sikkerhed er på plads, uanset om man er en stor eller en mindre virksomhed.

Den nationale strategi er en samlende ramme for, hvad vi gerne vil opnå. Cybersikkerhed er en fælles indsats, og med strategien i hånden har vi allerede i strategiens første år set, hvordan myndigheder, virksomheder og interesseorganisationer har samarbejdet om at søsætte de første initiativer.

Dermed er indsatsen ikke slut. Der venter mange opgaver forude frem mod 2021, og vi kan allerede nu se flere tendenser, der gør det vigtigt at holde tempoet oppe. Vores samfund bliver mere og mere afhængigt af digitale tjenester, og samtidig bliver flere enheder forbundet til internettet. Derfor skal vi hjælpe hinanden med at styrke Danmarks robusthed over for cybertruslen.

5.2. DET KRÆVER EN KULTURÆNDRING AT ØGE INFORMATIONSSIKKERHEDEN

AF RIKKE HOUGAARD ZEBERG,
DIREKTØR I DIGITALISERINGSSTYRELSEN.

It-kriminalitet er desværre ikke længere en sjælden overskrift i medierne. Tværtimod er angreb mod både borgere, virksomheder og offentlige myndigheder i løbet af de senere år blevet hyppigere og mere avancerede. Og det stiller nye krav til, hvordan vi som individer og organisationer håndterer den digitale sikkerhed.

Hverdagen er digital. Men ligesom vi skal gribe digitaliseringens muligheder, skal vi også ruste danskerne til at imødegå de digitale trusler. Den nationale strategi for cyber- og informationssikkerhed giver afsættet til at skabe den sikkerhedskultur, der er nødvendig i et digitalt Danmark.

5.2.1. Danskernes digitale kompetencer skal løftes

Netop kulturen er afgørende, når det handler om at løfte den digitale sikkerhed. Vi må indrømme, at "det svageste led" ofte er os selv – hver enkelt af os. Ét centralt pejlemærke i cyberstrategien er derfor at hæve danskernes kompetencer, så både borgere, virksomheder og myndigheder får en mere sikker digital adfærd.

For i modsætning til de forholdsregler, vi tager i trafikken – hvor de færreste af os kunne drømme om at starte bilen uden sikkerhedsselen på – så er vi ikke lige så gode til at beskytte os selv digitalt. Informationssikkerhed skal derfor i højere grad tænkes helt ind i vores digitale hverdag. Borgerne skal fx have gode digitale vaner som at bruge stærke kodeord, og myndighederne skal indtænke sikkerhed allerede i tilrettelæggelsen af opgaveløsningen.

Og selvom de fleste godt ved, at sikkerheden er vigtig, kan det alligevel være svært at vide, hvad man præcist skal gøre – og holde fokus på det i en travl hverdag. Derfor kræver det en reel kulturændring, både hos den enkelte borger, virksomhed og myndighed, for at nå strategiens mål om øget viden og bevidsthed om, hvordan man bedst beskytter sig.

Cyberstrategien indeholder derfor en række initiativer, der skal give danskernes digitale sikkerhedskompetencer et løft.

5.2.2. Sikkerdigital.dk

En væsentlig forudsætning for, at man kan løfte sin digitale sikkerhed er, at man kender truslerne og ved, hvordan man beskytter sig. Derfor blev portalen sikkerdigital.dk lanceret i oktober 2018. Den er udviklet og driftes i fællesskab af Digitaliseringsstyrelsen og Erhvervsstyrelsen.

Sikkerdigital.dk er målrettet både borgere, virksomheder og myndigheder. Borgere kan fx finde gode råd om alt fra sikkerhedskopiering af data, til hvordan man undgår at blive snydt på nettet. Virksomheder kan fx få hjælp til at stille krav til it-leverandørernes sikkerhed. Og offentlige myndigheder kan fx få hjælp til at implementere sikkerhedsstandarden ISO 27001 og til at udarbejde awareness-tiltag for medarbejderne.

Der er behov for et langt, sejt træk, hvis vi skal ændre danskernes digitale vaner. Derfor vil vi i Digitaliseringsstyrelsen, sammen med KL og Danske Regioner, løbende lave målrettede informationsindsatser for at sætte it-sikkerhed på dagsordenen for borgere og virksomheder og øge kendskabet til sikkerdigital.dk. Og så hviler der et stort ansvar på lederne – både i det private og det offentlige – for at sætte og holde fokus på awareness. Når kulturen skal ændres, kræver det opmærksomhed og indsats fra alle.

5.2.3. Kompetenceudvikling af offentlige ansatte

Særligt vigtigt er det, at offentligt ansatte har styr på sikkerheden. I det offentlige arbejder vi ofte med personoplysninger, som er følsomme eller skal behandles fortroligt. Det er derfor vigtigt, at ansatte er klædt på til at passe på borgernes oplysninger, både digitalt og fysisk.

Vi ville ønske, at vi fuldstændig kunne undgå fejl. Det er dog svært at garantere – for vi arbejder også med mennesker. Men med viden når vi langt, og myndighederne skal derfor sikre, at alle ansatte kender risici, forholdsregler og ansvar, når det kommer til at beskytte de informationer, de arbejder med. Det er en af de vigtigste opgaver, den offentlige sektor i disse år står overfor. Det handler nemlig om borgernes tillid.

Samtidig skal en række tiltag bidrage til kompetenceudvikling af offentlige ansatte og opbygning af en sikkerhedskultur i staten. Der vil bl.a. blive udviklet en kompetencegivende uddannelse på sikkerhedsområdet, og der vil blive sat øget fokus på cyber- og informationssikkerhed for ledere.

For at vi kan nå i mål med strategiens intentioner, skal vi alle tage ansvar og i langt højere grad få sat vores digitale sikkerhedssele på. Det arbejde sætter vi nu turbo på.

5.3. DROP SILOERNE OG START SAMARBEJDET

AF BIRGITTE HASS,
DIREKTØR I IT-BRANCHEN.

Cybersikkerhed er en afgørende forudsætning for vores gennemdigitaliserede samfund. Med den omfattende digitalisering af både erhvervslivet, den offentlige sektor og befolkningen stiger risikoen for og konsekvenserne ved cyberkriminalitet dag for dag.

Som Europas mest digitaliserede land har vi en national interesse i at styrke vores beredskab og indsats inden for cybersikkerhed. Sikkerhed er ikke blot en nødvendighed for beskyttelse af samfundets offentlige instanser, men er også afgørende for borgernes tryghed, erhvervslivets vækstmuligheder og udvikling af samfundets brug af teknologi.

Med regeringens cybersikkerhedsstrategi kan vi se, at sikkerheden bliver taget alvorligt på højeste niveau, og der er fundet penge til at understøtte arbejdet – ikke mindst til etablering af et nationalt cybersituationscenter.

Strategien søsætter en masse gode initiativer og placerer et klart ansvar for cybersikkerheden – nemlig hos de enkelte ministerier, ved at skubbe gang i en række vigtige sektorstrategier, bl.a. for energi-, sundheds-, tele- og finanssektoren.

5.3.1. Flere mangler i strategien

Man kan dog alligevel ikke lade være med at sidde tilbage med en lidt ærgerlig fornemmelse, primært fordi strategien fortsat mangler at blive en strategi for hele Danmarks cybersikkerhed.

Strategien bliver kaldt en "National strategi", men når man ser bort fra de vigtige sektorstrategier, så er strategien enten mangelfuld eller svag, når det gælder om at komme hele vejen rundt.

Hvor er kommunerne f.eks.? En ikke uvæsentlig del af vores følsomme data ligger hos kommunerne, og vi hører regelmæssigt om it-sikkerhedsproblemer i den kommunale verden.

Hvor er borgerne? Vi må ikke glemme at borgerne er vores "first line of defence", ikke mindst i deres rolle som medarbejdere. Her mangler vi både spidskompetencer og generel dannelse, når det kommer til it-sikkerhed.

Hvor er virksomhederne? virksomhederne er en kæmpe ressource i kampen om at sikre Danmarks cyberforsvar, samt en primær aftager af trusselsvurderinger og rådgivning.

5.3.2. Sammen er vi stærkest

Vi har tilsammen så meget viden og power, at vi kan gøre en reel forskel. Og er der noget, vi kan i Danmark, så er det netop at stå sammen om at løse brede problemer.

Men den offentlige organisering af cybersikkerhedsområdet er for fragmenteret, siloopdelt og usammenhængende og svarer ikke i tilstrækkelig grad til de cybertrusler, vi ser i dag.

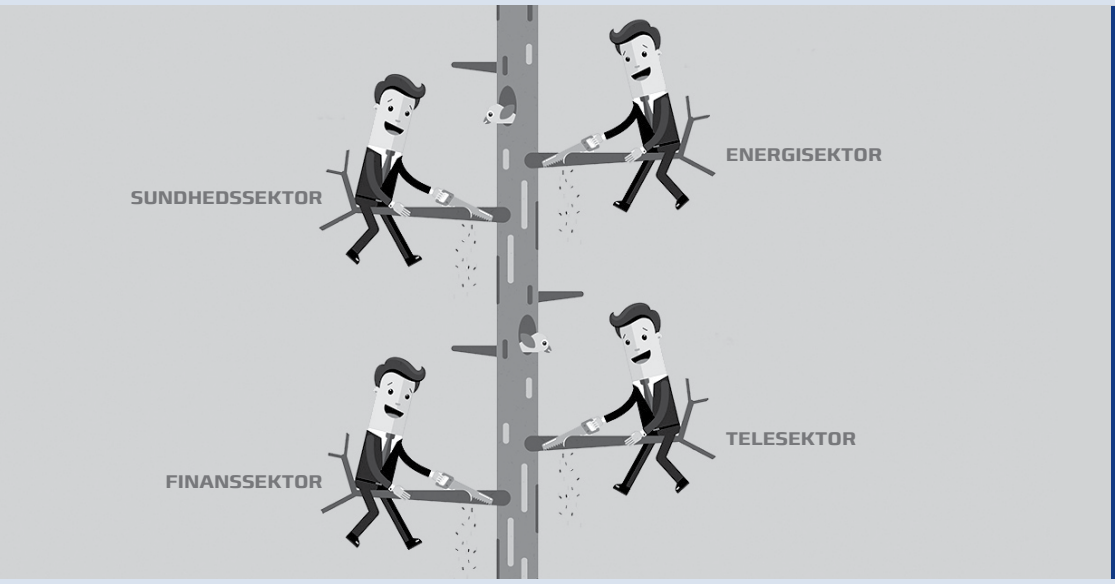
Der er nedsat en række branchespecifikke råd og overvågningstjenester, men de opererer uafhængigt af hinanden og med manglende koordination. Uden samarbejde risikerer vi både at lave spildt dobbeltarbejde – og endnu værre: At have blinde vinkler og uafdækkede huller.

5.3.3. Vi ønsker os en koordinerende myndighed

Det brede samarbejde omkring cybersikkerhed i Danmark skal styrkes, men vi mangler et forum, hvor it-leverandørerne, virksomhederne, borgerne og myndighederne kan udveksle viden, koordinere indsatser og planlægge fælles initiativer. Og vi mangler en myndighed der tager borgernes sikkerhed på sig som deres ansvar.

Center for Cybersikkerhed (CFCS) har i dag det overordnede ansvar for at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur. Men centerets militære placering giver dem en række begrænsninger, der gør det svært for dem at varetage den koordinerende og vejledende rolle, vi efterlyser.

Hvis jeg kunne beslutte ét enkelt initiativ til strategi for cyber og informationssikkerhed, ville jeg uden tøven vælge, at der skulle etableres en civil myndighed, hvis primære rolle skal være at sikre den nødvendige vidensdeling på tværs af alle relevante aktører samt at oplyse, vejlede og rådgive danske myndigheder, virksomheder og borgere om it-sikkerhed.



5.4. SÅDAN ARBEJDER VI MED AT SIKRE DEN BEDST MULIGE GENERELLE CYBER- OG INFORMATIONSSIKKERHED I DANMARK

AF OLE KJELDSEN,
DIREKTØR FOR TEKNOLOGI OG SIKKERHED, MICROSOFT, OG MEDLEM AF BESTYRELSEN I RÅDET FOR DIGITAL SIKKERHED.

Rådet for Digital Sikkerhed (RfDS) ønsker at tilskynde arbejdet med at sikre den bedst mulige generelle cyber- og informationssikkerhed i Danmark, for det offentlige, private organisationer og blandt alle samfundets borgere.

Vi mener der eksisterer et behov for generelt at opnå et højere niveau af digital dannelse og databeskyttelseskultur i alle lag af samfundet.

Den Nationale strategi for cyber- og informationssikkerhed er et væsentligt skridt, som fortjener både størst mulig støtte, kritisk stillingtagen og effektiv implementering for at få den ønskede positive effekt for alle danske organisationer og borgere.

5.4.1. Spændende 2018

2018 var på mange måder et skelsættende år for cyber- og Informationssikkerhed globalt og i Danmark. Ikke alene oplevede vi for første gang hvordan også større danske virksomheder kunne blive kraftigt økonomisk negativt påvirket af cybertrusler (NotPetya).

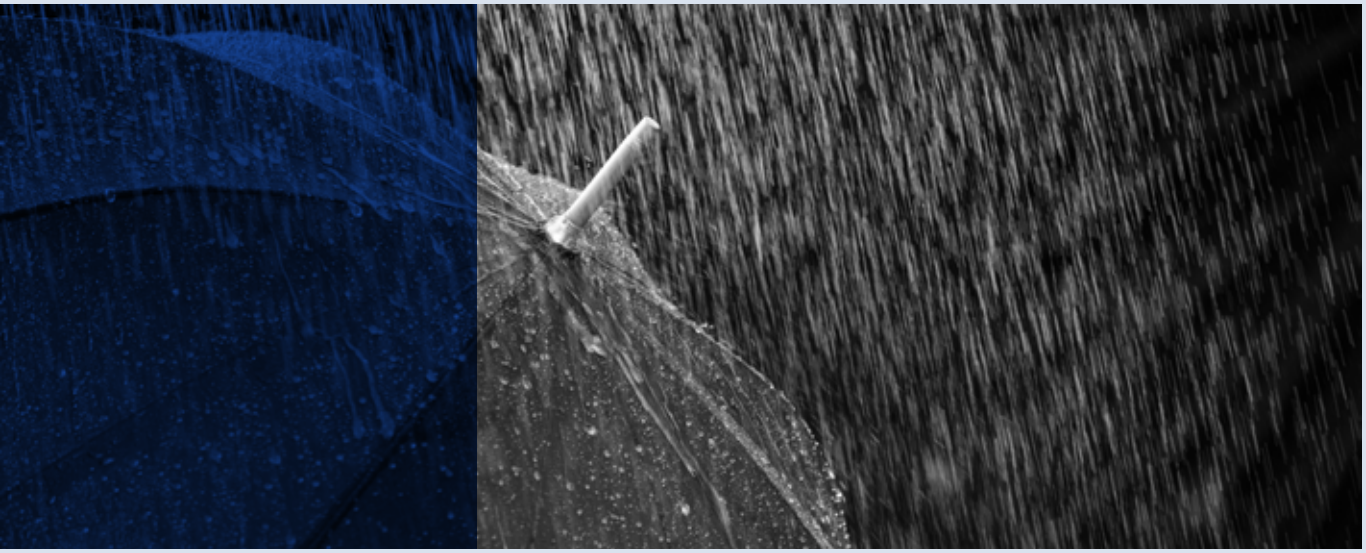
Det var også året, hvor den mest vidtrækkende regulering (GDPR) af hvorledes håndtering af persondata bør/skal foregå, fandt anvendelse. Og endelig var det året hvor Danmark efter lidt forsinkelse, fik en fornyet national strategi på området.

Det er derfor væsentligt at forsøge at analysere 2018 lidt nærmere og drage nogle konklusioner om, hvorledes vi i årene fremover bedst kan positionere Danmark, vore organisationer og borgere til at begå sig i den aktuelle og kommende digitale virkelighed.

5.4.2. Markante sikkerhedshændelser i 2018

Hændelserne omkring 'NotPetya' i maj 2018, viste tydeligt at trusler med baggrund i helt andre geografier og målsætninger, har potentialet til at påvirke organisationer mere eller mindre tilfældigt, hvis ikke beredskabet er på plads.

2018 introducerede verden til den generelt stærke innovation indenfor cyberkriminalitet, som ved hjælp af bl.a. værktøjer som kunstig intelligens, giver de kriminelle nye muligheder for at finde sårbare systemer, data, identiteter mm. Langt hurtigere og dermed mere effektivt. Våbenkapløbet mellem de gode og de kriminelle for bedst at anvende de nye teknologiske værktøjer i deres arbejde er i gang og en lang række regeringer og virksomheder introducerede da også offentligt i 2018, sikkerhedsløsninger som bl.a. implementerer kunstig Intelligens.



Endelig har 2018 budt på en række hændelser med alvorlige tab af persondata: Marriott, Voxox, Tyske politikere, Facebook, arkivskabe med danske sundhedsjournaler, GoMentor for blot at nævne de mest kendte. Ovenpå implementering af GDPR og den generelle offentlige debat om betydningen af sikker håndtering af persondata, har de alle været med til at bringe emnet endnu bredere ud i både det politiske og offentlige rum globalt.

Selvom det aldrig er godt, at 'der skal lig på bordet' før et emne få opmærksomhed, og man reelt igangsætter de nødvendige strategiske og praktiske tiltag, så har status omkring cyber- og informationssikkerheden ved udgangen af 2018, klart bevist hvor væsentlig området er for alle dele af samfundet – og for Danmark, qua vores høje digitaliseringsgrad i specielt høj grad.

5.4.3. Den Nationale Strategi & de 6 sektorstrategier

RfDS ser det naturligvis som en god udvikling, at disse strategier udarbejdes. Både overordnet og for de definerede kritiske infrastrukturelle sektorer, er det afgørende for Danmarks fortsatte succesfulde digitalisering, at man lykkes med at skabe reel sikkerhed og dermed tryghed til disse kerneelementer i det danske samfund.

Flere af strategierne har da også gode overlappende taktiske tiltag, som fx nødvendig erfaringsudveksling mellem det offentlige og private og ikke mindst bredere kompetenceforøgende aktiviteter.

Samtidig er det desværre sådan, at store dele af den kritiske databehandling som foretages i bl.a. det offentlige ikke er omfattet af strategierne. En stor del af den risiko som Danmark er udsat for i forbindelse med vores øgede digitalisering, er i sagens natur ikke at opfatte som kritisk infrastruktur eller har betydning for den nationale sikkerhed, og dermed er de ikke i fokus for Center for Cyber Sikkerhed (CFCS).

Det er den oplagte svaghed ved strategierne, at mange risici, som kan have stor betydning for den enkelte organisation og ikke mindst individ, ikke er omfattet. Om der er tale om den kommunale eller små & mellemstore virksomheders databehandling, så er de eksponerede for de nævnte risici i det digitale univers, og der er derfor behov for en cyber- og informationssikkerhedsstrategi, med nøje udvalgte taktiske og praktiske tiltag, på linje med de der udstikkes for den nationale kritiske infrastruktur.

5.4.4. 2019 og årene frem

De fleste forudser, at cyber- og informationssikkerhedsbilledet vil fortsætte de mønstre, som har tegnet sig de foregående år – naturligvis stadig de avancerede (og i nogle tilfælde statssponserede) angreb, men i langt højere grad og med potentielt større effekt, kraftig forøgelse af fx phishing som bl.a. leder til ransomware, spear-phising, som kan

lede til CxO fraud, datalæk med efterfølgende Xtorsion eller lignende cyberkriminalitet og desværre fortsat en række Phone Support Scams.

2019 kan også blive året, hvor de cyberkriminelle i meget større omfang vil benytte kunstig intelligens til fx at minimere deres indsats for at finde sårbarheder. Men det kan også meget vel blive året, hvor kunstig intelligens virkelig kan vise sin berettigelse i forsvaret og gøre det enklere og mere overkommeligt at lokalisere angreb ud fra mønstre i de ekstreme digitale datamængder, i stedet for at skulle kende nøjagtige angrebsmetoder, værktøjer eller kode. Våbenkapløbet fortsætter altså mellem kriminelle og de, der arbejder for at beskytte vore data.

For at minimere angrebsfladen er det derfor væsentligt netop, at alle niveauer af vores samfund opkvalificeres og spiller positivt med på at sikre data bedst muligt – lad os derfor blive praktiske og se på hvordan man identificerer det, der skal/kan gøres.

Risikovurderinger:
Som altid når sikkerhed er emnet, må udgangspunktet være en *risikovurdering*. Uanset om man er CFCS, en offentlig eller kommerciel organisation eller borger, bør aktiviteter man implementerer alene være baseret på en vurdering af, om en risiko er sandsynlig og hvilken konsekvens det vil have, hvis risikoen bliver effektueret.

Det gælder naturligvis fysisk sikkerhed - du låser døren til dit hjem, fordi der er en vis sandsynlighed for, at nogle vil begå indbrud og konsekvensen af et evt. indbrud, ønsker du ikke at leve med.

Ligeledes for digital sikkerhed - du sikrer dig at dine digitale enheder er opdaterede med de seneste sikkerhedspakker, fordi der er en relativ stor sandsynlighed for, at ikke patchede sårbarheder vil blive udnyttet af cyberkriminelle, og du ønsker heller ikke at leve med konsekvensen af det indbrud.

Og det gælder for persondatabehandling, hvor GDPR netop tager udgangspunkt i en risikovurdering, således at dataansvarlige og databehandlere, har pligt til at foretage den bedst mulige beskyttelse, for at minimere sandsynlige og afgørende risici for den person, hvis data de behandler. Alt i alt er risikovurderinger altså et rigtigt godt udgangspunkt hver eneste gang, man overvejer hvorledes sikkerheden skal forbedres – ikke overraskende, men desværre ofte overset.

Kompetenceløft:
For kvalificeret at kunne foretage disse risikovurderinger på alle niveauer af samfundet, er det netop væsentligt, at de rette kompetencer er til stede – derfor stor ros til alle de strategier, som indeholder dette helt fundamentale element. Det er et første og vigtigt skridt frem imod at skabe den rette sikkerhedskultur overalt i det danske samfund.

De lavthængende og evigt-grønne frugter:
Top-5 af de gode råd om hvordan man bedst beskytter sig digitalt, har basalt set ikke ændret sig gennem de seneste 15-25 år, men er desværre stadig det rigtige sted at starte. Størstedelen af de mulige risici kan minimeres ved at:

1. Opdatér enheder, software og tjenester – Det gælder om både at sikre at bruge tidssvarende løsninger, som er skabt til at fungere i en digital verden anno 2019, at sikre at alle tilgængelige sikkerhedspakker implementeres og at leverandører opretholder bedst mulige sikkerheds- og compliance-niveau.
2. Brug stærke log-on mekanismer – allerhelst fler-faktor løsninger, men som minimum stærke kodeord, som skiftes ofte.
3. Benyt opdaterede anti-virus, anti-malware og anti-spam løsninger. Meget gerne løsninger, som trækker på globalt beredskab og kilder til intelligence om det top-aktuelle trusselsbillede.
4. Tag backup og ikke mindst test indimellem at din backup/genskab-proces fungerer.
5. Brug din sunde fornuft og være gerne ligeså skeptisk overfor det du møder digitalt, som du er i den fysiske verden.

Andre referencer:

- National Cyber & Informationssikkerheds strategi:
  https://digst.dk/nyheder/nyhedsarkiv/2018/maj/ny-national-strategi-styrker-cybersikkerheden/
- Forbrugerrådet/Trygfondens app Digitalt Selvforsvar:
  https://taenk.dk/aktiviteter-og-kampagner/apps-fra-forbrugerraadet-taenk/app-mit-digitale-selvforsvar
- Erhvervsstyrelsen & Digitaliseringsstyrelsens www.sikkerdigital.dk som giver gode råd til både private og små og mellemstore virksomheder
  https://www.sikkerdigital.dk/
- Rådet for Digital Sikkerhed:
  https://www.digitalsikkerhed.dk/10-tips/

5.5. NÅR MAN IKKE ER KRITISK I DAG

AF POUL HALKJÆR NIELSEN,
INFORMATIONSSIKKERHEDSCHEF, KØBENHAVNS UNIVERSITET.

Danmark ser sig selv som meget digitalt og som et vidensamfund. I uddannelsessektoren er vi en stor del af dette og også frontløbere.

Vi former både adfærden og løsningerne for fremtiden, og er således måske ikke i dag samfundskritiske, men det varer ikke længe før, at både vores viden og vores studerende er en del af den kritiske infrastruktur og viden, som regeringens nationale strategi søger at beskytte bedre fremadrettet.

Netop fordi vi ligger så tæt op ad de kritiske sektorer, er strategien af interesse. Dels ud fra et nationalt synspunkt, men ikke mindst ud fra et dagligt fagligt synspunkt.

5.5.1. En tone i dialogen

Uddannelsessektoren er som nævnt ikke i dag anset for at være en kritisk sektor, og derfor er vi ikke direkte omfattet af National strategi for cyber- og informationssikkerhed.

Men selve strategien er med til at sætte en tone i dialogen herhjemme, og derfor er det også godt at kunne læse sig til, at det både er det it-tekniske (det store cyber-ord) OG informationssikkerhed, der tages fat i.

Uden at skulle slås om ord er det it-tekniske dog blot en delmængde af informationssikkerhed i min verden. It-teknologierne er billedligt talt bagdørene og informationssikkerheden er den, der sikrer hoveddøren OG sørger for at dørmanden ved hoveddøren også sørger for at holde et øje med bagdøren en gang i mellem.

5.5.2. Sikkerhed i hænderne på den enkelte

I uddannelsessektoren fylder informationssikkerhed mere, nærmest det omvendte af fordelingen i regeringsstrategien. Det er i høj grad begrundet i økonomiske forhold og, at vi bedriver meget små enkeltproduktioner (hver forsker sin egen fabrik).

Oveni er disse enkeltproduktioner skabt igennem internationale samarbejder og med krav fra sponsorerne om åbenhed og offentliggørelse så hurtigt som muligt. Derfor ligger vores sikkerhed i høj grad i hænderne på den enkelte ansatte og dennes adfærd og skal derfor adresseres mest igennem ledelsesansvaret og det personlige ansvar samt den personlige interesse for at beskytte egne resultater, frem for igennem stor teknisk overvågning.

Desværre fylder det ledelsesmæssige ansvar kun lidt i strategien, og man skal helt om på side 48 for at finde en direkte sproglig kobling til ledelse. Når det er et desværre, er det fordi, vi jo ved at rigtig mange mennesker, og derved brugere, fortsat anser det for et it-teknisk problem at beskytte os selv mod os selv og vores ikke så sikre gerninger, når vi benytter de digitale muligheder i vores arbejde og private hverdag. Og rigtig mange datatab sker ved, at der er brugerne, der bevidst eller ubevidst, afgiver data og giver adgang til systemerne.

Det er igennem ledelse, at vi får samtalen med den enkelte bruger om at sikre de data, vi har adgang til - både fordi der er brug for at forbedre kvaliteten af den enkeltes brug af eksempelvis passwords og også fordi, det er igennem ledelsens klare udmelding og dialog om det, vi arbejder med, at vi lærer, at vi nok skal prøve at gøre det rette første gang.

5.5.3. Informationssikkerhed skal være en målbar ledelseskvalitet

Det står desværre ikke klart, hvorledes man vil gøre op med den manglende dialog i de kritiske – og afledt heraf, de mindre kritiske sektorer. Og det er ærgerligt for det kunne også være med til at undgå en del af de tab, vi har set i samfundet i de sidste år, at der var en mere gennemsigtig dialog på de enkelte arbejdspladser om, hvad vi går og laver, hvorfor og hvordan samt hvorledes vi gør det rigtigt.

Oveni kunne det give bedre trivsel og ansvar for det digitale Danmark og måske modarbejde en trist trend:

En undersøgelse viste for nylig, at 28 procent ikke aner, hvorledes vi reelt bruger vores tid på arbejdet og at 37 procent ikke mener, at deres chef aner, hvad de går og laver.

Ved at gøre informationssikkerhed til en målbar ledelseskvalitet og ved at stille os til ansvar for vores gerninger, udført under frihed, vil vi kunne opnå en større og bedre beskyttelse end det, alene et it-teknisk cyberforsvar giver.

Men det kræver, at vi tør tage dialogen, herunder tør indrømme at det er komplekst. Det forudsætter, at ledelser og bestyrelser stiller krav om det, og det er er desværre for få, der gør.

Henvisninger:

28 percent of us can't answer the question, 'how do you spend your time at work?'
https://www.nbcnews.com/better/pop-culture/28-percent-us-can-t-answer-question-how-do-you-ncna953806

CA TECHNOLOGIES INSIDER THREAT 2018 REPORT
https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

PONEMONS 2018 COST OF A DATA BREACH REPORT
https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018

Danskernes Informationssikkerhed 2018
https://www.cert.dk/da/information/borgernes_informationssikkerhed

LASTPASS GLOBAL PASSWORD SECURITY REPORT
https://blog.lastpass.com/2018/10/introducing-2018-global-password-security-report-lastpass.html

5.6. SAMARBEJDE I TELESEKTOREN OM CYBERSIKKERHED

AF JAKOB WILLER,
DIREKTØR I TELEINDUSTRIEN.

Som opfølgning på regeringens cybersikkerhedsstrategi fra maj 2018 inviterede Center for Cybersikkerhed telesektoren til selv at tage stafetten for at få udarbejdet en sektorstrategi på teleområdet.

Det var en god mulighed for telesektoren til at tage ansvar for indholdet af strategien på cybersikkerhedsområdet og kvittere positivt for den tillid, som myndighederne viste sektoren.

Strategien for telesektoren blev offentliggjort i januar 2019 efter en meget konstruktiv proces, hvor teleselskaber og brancheorganisationer havde udarbejdet en risiko- og sårbarhedsvurdering for den samlede branche og i samarbejde med Center for Cybersikkerhed kommet frem til 12 initiativer, der bidrager til en højere sikkerhed.

5.6.1. Strategiens indhold og etablering af en DCIS

Med strategien og initiativerne er det målet at øge den generelle sikkerhed i telesektoren i Danmark og målrette indsatsen til de specifikke områder, der er blevet identificeret i sårbarhedsanalysen. Det gælder fx i forhold til angreb eller fejl fra egne medarbejdere (insidere) og sikkerheden i forhold til underleverandører.

Et centralt punkt i strategien er at øge sikkerhedssamarbejdet gennem etablering af en såkaldt decentral cyber- og informationssikkerhedsenhed – en DCIS. DCIS'ens primære opgave er at dele informationer om relevante informationssikkerhedsforhold mellem sektorens aktører og Center for Cybersikkerhed.

Når en trussel rammer ét selskab, kan den hurtigt ramme andre og dermed større dele af samfundet. Det kan en DCIS bl.a. modvirke. Med DCIS'en opstilles der klare rammer for, hvordan information kan deles, og også deles på måder, så viden kommer ud til alle uden nødvendigvis at afsløre, fra hvilket selskab informationen kommer fra.

Den 15. marts 2019 stiftede de 11 teleselskaber, der er udpeget som kritiske, en forening og afholdt den stiftende generalforsamling. Her besluttede medlemmerne, at den kommende DCIS skal placeres hos DKCERT.

Det var der flere gode grunde til. For det første kan telebranchen drage nytte af DKCERTs mangeårige arbejde med it-sikkerhed og gennem et fagligt samarbejde mellem DCIS-medarbejderne og DKCERTs ansatte forventes det faglige niveau at være højt, lige fra starten. Ligeledes er det en vigtig begrundelse, at DKCERT er neutral i forhold til både politiske - og konkurrencemæssige hensyn.

Det forventes også, at der med etableringen af DCIS vil kunne ske en mere struktureret udveksling af information og viden med Center for Cybersikkerhed, og at den information, som centeret opsamler fra sine samarbejdspartnere og fra andre sektorer kan deles med teleselskaberne på en brugbar måde.

I DCIS'en vil der blive tilknyttet ressourcer på fuld tid, som vil kunne opbygge et godt overblik over infrastrukturen, varetage driften og håndtere opgaver med fx at arrangere fælles uddannelsesaktiviteter, netværksmøder og opdatere branchens risiko- og sårbarhedsvurdering.

Tankegangen bag etableringen af DCIS'en er, at alle har en interesse i at samarbejde og dele viden og informationer, og jo bedre vi er til det, jo bedre bliver hvert selskab i stand til at bygge mere robuste net, opdage sårbarheder og håndtere angreb på infrastrukturen.

Pointen er, at vi ved at dele viden og informationer på tværs mellem selskaberne får flere øjne og ører på de konkrete hændelser og problemstillinger, og ved at samarbejde løfter vi den samlede sikkerhed på tværs af hele branchen.

5.6.2. Tillid og begyndende ny samarbejdskultur

Det er ikke nyt, at teleselskaber samarbejder på sikkerhedsområdet. Der har i en længere årrække været et mere uformelt samarbejde mellem selskaberne i branchen i regi af det såkaldte ISP Sikkerhedsforum. Med etableringen af DCIS på teleområdet udvides samarbejdet og gøres mere forpligtende og målrettet.

Et velfungerende samarbejde mellem selskaberne og mellem selskaberne og Center for Cybersikkerhed er i høj grad afhængig af, at parterne har tillid til hinanden og har tillid til, at udvekslede informationer behandles med den fornødne fortrolighed, hvilket DKCERT forventes at gøre. Allerede med den proces, som branchen og selskaberne har været igennem med udarbejdelse af strategien, er der etableret en begyndende ny samarbejdskultur på tværs mellem selskaberne.

Medarbejdere, der arbejder med sikkerhed, har lært hinanden bedre at kende, og der er flere eksempler på, at den øgede dialog har ført til nye samarbejdsrelationer og løsning af sikkerhedsudfordringer.

Det er er udvikling, som vil blive yderligere styrket med den permanente etablering af en DCIS på teleområdet.

Næste skridt er, at vi også kan begynde at få glæde af hinandens viden og informationer på tværs af de samfundskritiske sektorer, hvor der er udarbejdet strategier og etableret cybersikkerhedsenheder. Det er et af de områder, der også er sat fokus på i det samarbejde, der er etableret på tværs mellem brancheforeninger i de samfundskritiske sektorer.

5.6.3. Cybersikkerheds-kompetencer

En af de udfordringer, som der også er blevet peget på i strategiarbejdet, handler om adgangen til de rette kompetencer på cybersikkerhedsområdet. Mange selskaber oplever, at det kan være vanskeligt at finde kvalificerede medarbejdere til stillinger på cybersikkerhedsområdet, og med den øgede digitalisering og indsatsen for højere sikkerhed på tværs af mange sektorer er efterspørgslen efter medarbejdere med cybersikkerhedskompetencer også voksende.

Det gælder eksempelvis til stillinger som sikkerhedsarkitekter eller analytikere, hvor teleselskaber oplever, at det kan være vanskeligt at finde de rigtige medarbejdere. Et af initiativerne i strategien er derfor også i samarbejde med de andre samfundskritiske sektorer at arbejde for at øge udbuddet af cyber- og informationssikkerhedskompetencer, både ved at efter- og videreuddanne medarbejdere og ved at arbejde for flere uddannelsesmidler til sikkerhed på forskellige uddannelsesniveauer og fagområder.

5.6.4. Vi har taget de første skridt

Med lanceringen af de forskellige strategier i de samfundskritiske sektorer har der også været en del kritiske røster fremme om fx manglende fokus på borgerne og på privacy, manglende koordination på tværs mellem sektorerne, knopskydning i initiativer og manglende finansiering på nogle af områderne. Kritikken er sikkert i en vis udstrækning både rigtig og berettiget.

Men hvis man lige løfter blikket og ser, hvor langt vi reelt er kommet på relativ kort tid, så er det samlet set en kæmpe succes for regeringen, at vi nu i seks samfundskritiske sektorer på et halvt år har fået udarbejdet risiko- og sårbarhedsanalyser, er begyndt at arbejde strategisk med cybersikkerhed på sektorniveau, har styrket samarbejdet på tværs i sektorerne og etableret cybersikkerhedsenheder på alle områder.

Vi har taget de første og vigtige skridt i retning af en højere sikkerhed. Nu skal vi fastholde fokus og fortsætte indsatsen med implementeringen af de mange initiativer i strategierne. Og mon ikke der er flere brancher, der kan blive inspireret til at se nærmere på, hvordan man i fællesskab kan tage initiativ til en højere cybersikkerhed. Måske i byggebranchen, i fødevareerhvervene, i medicoindustrien, i medicinalindustrien eller i oliebranchen. Med den øgede digitalisering vil behovet for højere cybersikkerhed kunne findes flere og flere steder.

Strategiens 12 initiativer

> Indsats mod angreb fra insidere
> Bedre leverandørstyring
> Sikring mod fysisk sabotage i forbindelse med kriser og lignende
> Samarbejdet mellem el- og telesektoren
> Styrkelse af evnen til at imødegå cyberangreb
> Etablering af DCIS
> Styrket øvelsesaktivitet
> Fælles kurser i telesektoren indenfor cyber- og informationssikkerhed
> Mulig etablering af incident response kapacitet i branchen
> Styrke samarbejdet med andre samfundskritiske sektorer i Danmark for at øge udbuddet af cyber- og informationssikkerhedskompetencer
> Klassificerede kommunikationsmidler
> Forbedret IoT-sikkerhed

Strategisamarbejdet

Telesektorens strategi for cybersikkerhed er udarbejdet i et samarbejde mellem Dansk Industri, Dansk Erhverv, Dansk Energi, IT-Branchen og Teleindustrien.

De teleselskaber, der har deltaget strategiarbejdet er Aura, Dansk Beredskabskommunikation, Eniig, Ewii, Fibia, GlobalConnect (inkl. Nianet), HI3G, STOFA (inkl. SE), TDC (inkl. Dansk Kabel TV), Telenor, Telia, Teracom og Waoo.

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, Henrik Larsen har skrevet til Computerworld i 2018.

6.1. Derfor vil processor-sårbarhederne Spectre og Meltdown plage os i månedsvis

Sårbarhederne Meltdown og Spectre rammer de mest udbredte processortyper og vil tage tid at få styr på.

Året begyndte med et par sårbarheder, som vi kommer til at beskæftige os med i de kommende måneder: Meltdown og Spectre. Det drejer sig om sårbarheder i de processorer, der indgår i computere, smartphones og andet udstyr omkring os. Dele af dem kan rettes i software, andre kræver hardwareopdateringer.

Både Meltdown og Spectre ligger i processorens mulighed for at forsøge at forudsige, hvad et program vil gøre senere. Moderne processorer er lynhurtige. Det meste af tiden venter de på at få data at arbejde med. Ventetiden udnytter de til at afvikle kommandoer, der kommer senere i det program, de er ved at udføre.

Det kan være kommandoer, der kommer efter en valgmulighed: Hvis svaret er ja, skal denne kommando udføres, ellers skal den springes over.

Når en processor på den måde forsøger at afvikle kode, vil den som regel også arbejde med data. Men den forsøgsvise afvikling må naturligvis ikke få indflydelse på data, før det er helt sikkert, at kommandoerne rent faktisk skal gennemføres.

6.1.1. Snuser i cachen

Vor tids processorer henter deres data fra cachelageret, der igen henter dem fra arbejdslageret.

Sårbarhederne ligger i, at det efterlader spor i cachen, når processoren forsøgsvis afvikler kommandoer. Dermed kan en proces få adgang til data, der tilhører en anden proces. Meltdown giver således en uprivilegeret proces mulighed for at tilgå data, der tilhører operativsystemets kerne. Det burde ellers være forbudt.

En angriber kan lade processoren afvikle et program, der forsøger at hente data fra kernens dataområde. Derefter skal det skrive en bestemt variabel, hvis en del af de hentede data opfylder et kriterium. Den indbyggede sikkerhed i processoren forhindrer, at programmet kan køre: Det må ikke tilgå data, der tilhører kernen.

Men sikkerhedssystemet forhindrer ikke, at processoren forsøgsvis prøver at afvikle kommandoerne. Det sørger heller ikke for at slette de foreløbige data, som bliver gemt i cachen.

Derefter prøver det skurkagtige program at læse den variabel, det bad om at få skrevet. Det tager tid på operationen.

Går det hurtigt, blev variablen hentet fra cachen. Det er tegn på, at kriteriet var opfyldt – for eksempel at en bestemt værdi fandtes et sted i kerne-dataene.

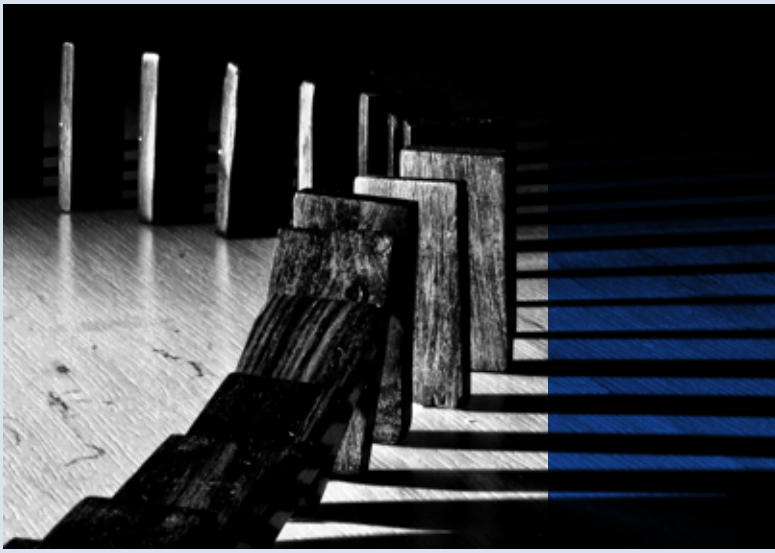
Tager det længere tid at hente variablen, findes den ikke i cachen, så kriteriet var øjensynlig ikke opfyldt.

6.1.2. Et side channel-angreb

Der er altså tale om et såkaldt side channel-angreb, hvor man ikke direkte kan tilgå fortrolige data. Men ved at observere andre fakta kan man slutte sig til, hvad de fortrolige data er.

Spectre bygger på lignende metoder. Her er det muligt for en proces at få fat i data fra andre processer. Man kan beskytte mod Meltdown ved at installere opdateringer til operativsystemet. Spectre kræver derimod en firmwareopdatering.

Intel udsendte opdateringer tidligere på måneden. Men de viste sig at medføre problemer: Nogle computere begyndte at genstarte.Firmaet har fundet årsagen til problemerne, og en ny firmware-opdatering skulle være på trapperne.



6.1.3. Vurder risikoen

Før vi går i panik over Meltdown og Spectre, må vi overveje risikobilledet. Hvor realistisk er en fjendtlig udnyttelse af sårbarhederne?

Der er tale om sårbarheder, der kan give adgang til fortrolige data. Vi taler altså ikke om mulighed for at afvikle skadelig programkode. For at få adgang til dataene skal en proces køre på den sårbare computer. Hvis vi har styr på, hvilken software der kører, kan vi forhindre udnyttelse af sårbarhederne.

Det sidste er sværere, end det lyder. Afvikling af software er blevet et vidt begreb. Kan en webside for eksempel udnytte sårbarheden via Javascript afviklet i en browser?

Risikoen er lille på servere, der kun afvikler en enkelt applikation. Den typiske mail- eller filserver er således ikke i risikozonen – medmindre den kører på sårbar virtualiseringsinfrastruktur.

Netop virtualiserede systemer er oplagte angrebsmål: Hvis angriberen kan afvikle kode på en virtuel maskine, kan koden tilgå data fra andre virtuelle maskiner. Dermed er cloud-systemer mulige ofre. De store udbydere har da også været hurtige til at opdatere deres systemer.

6.1.4. Svært at rette hardware

Der opdages tusindvis af nye sårbarheder hvert år. Når Meltdown og Spectre vækker så megen opmærksomhed, skyldes det, at de findes i hardware, som er meget udbredt. Derfor er mange potentielt berørt.

Endvidere er det vanskeligt at lukke sikkerhedshuller i hardware: Rettelserne skal distribueres gennem computerproducenterne, der skal få deres kunder til at opdatere firmwaren. Derfor kommer vi til at beskæftige os med Meltdown og Spectre i adskillige måneder endnu.

Sikkerhedsopdateringerne kan medføre, at systemer kører langsommere. Derfor er det værd at foretage en risikovurdering, før man installerer dem.

Mit råd lyder: Sæt jer ind i sårbarhederne og den skade, de kan medføre. Foretag en risikovurdering, og brug den som grundlag for at beslutte, hvad I skal gøre.

Oprindelig offentliggjort den 26. januar 2018.

6.2. ADVARSEL: IT-KRIMINELLE SKIFTER TIL KRYPTOVALUTA

En række angreb med skadelig software bruger de inficerede computere til at danne kryptovaluta.

Sig farvel til ransomware og goddag til software, der danner kryptovaluta.

Det er en klar tendens, når vi ser tilbage på 2017: Kryptovaluta fik sit gennembrud som en metode til at tjene penge til it-kriminelle. Og tendensen ser ud til at fortsætte i år. Kryptovaluta er digitale penge, der typisk implementeres via blockchain-teknologi. Det mest kendte eksempel er Bitcoin.

Men de it-kriminelle foretrækker valutaen Monero. Det er der flere gode grunde til, dem vender jeg tilbage til senere. Kriminelle kan typisk bruge kryptovalutaer til to ting: Til at modtage løsepenge eller betaling for kriminelle ydelser og til at danne penge via skadelig software.

6.2.1. Fald i ransomware

Ransomware-programmer har længe brugt kryptovalutaer til at opkræve løsepenge: Hvis offeret vil have adgang til sine data igen, skal vedkommende betale et beløb i Bitcoin eller en anden valuta.

Men vi har set et fald i ransomware den senere tid. Det kan hænge sammen med, at det er en usikker metode til at tjene penge. Hvis offeret har en sikkerhedskopi, er der ingen penge at hente.

Desuden har sikkerhedseksperter knækket krypteringen i nogle ransomware-programmer. Dermed er det muligt for ofrene at få deres data retur uden at betale bagmændene. Derfor er dannelse af kryptovaluta blevet mere tillokkende for de it-kriminelle.

6.2.2. Programmer danner penge

Det kan foregå ved, at de kriminelle inficerer offerets computer eller smartphone med et skadeligt program. Det kører i baggrunden, hvor det arbejder på at udføre de opgaver, der skal til for at danne nye digitale penge.

Bitcoin stiller store krav til hardwaren, når der skal dannes nye penge via det såkaldte proof of work. Derfor er Bitcoin mindre egnet til de kriminelles behov. De vil gerne have programmer, der kan køre på almindelige computere uden at optage så mange ressourcer, at brugerne opdager det.

Derfor er Monero blevet populær. Denne kryptovaluta har en arkitektur, der gør det mindre krævende at danne ny valuta. Oven i købet findes der en implementering af algoritmen i JavaScript. Den gør det muligt at indlejre kode på websider, der danner Monero-valuta i browseren hos dem, der besøger webstedet.

En anden fordel ved Monero er, at udviklerne har gjort meget ud af privatlivsbeskyttelsen. Derfor er det enklere at anonymisere overførsler, så politiet ikke kan se, hvor pengene ender.

6.2.3. Venter vækst

Jeg forventer, at vi vil se flere eksempler på skadelig software, der danner kryptovaluta. Det skyldes, at det giver en mere sikker indkomst end ransomware: Ved ransomware er den kriminelle afhængig af, at offeret betaler.

Men ved skadelig software er gevinsten garanteret, så snart det er lykkedes at inficere offerets computer. Det kan for eksempel ske ved at udnytte kendte sårbarheder. I DKCERT har vi således hørt fra flere universiteter, der blev ramt af kryptovaluta-malware. De blev inficeret ved, at angriberne udnyttede en ikke-opdateret version af programmet WebLogic på nogle servere.

Foruden servere kan de it-kriminelle også udnytte andre platforme. Der er set eksempler på apps til Android, der åbner en skjult webside, som danner Monero-valuta. For nylig blev Mac-webstedet MacUpdate ramt af en infektion: Når man hentede Firefox, OnyX eller andre programmer fra tjenesten, fik man en uønsket ekstrafunktion med i form af dannelse af Monero-penge.

Et lignende angreb gik ud over firmaet Texthelp, der tilføjer oplæsningsfunktioner til websteder. Angribere lagde kode ind i de JavaScript-filer, som kundernes websteder kalder.

På den måde blev omkring 4.200 websteder ramt, så deres gæster uden at vide det var med til at danne kryptovaluta til bagmændene.

Senest har bilproducenten Tesla været ramt. Her havde it-folkene glemt at sætte password på en Kubernetes-server. It-kriminelle udnyttede hullet til at installere software, der dannede kryptovaluta.

Bagmændene gjorde sig umage for at undgå at blive opdaget. Således skjulte de deres server bag tjenesten Cloudflare, så den var vanskeligere at spore. Programmet var også sat til at begrænse trækket på serverens ressourcer, så der var mindre risiko for, at det blev opdaget.

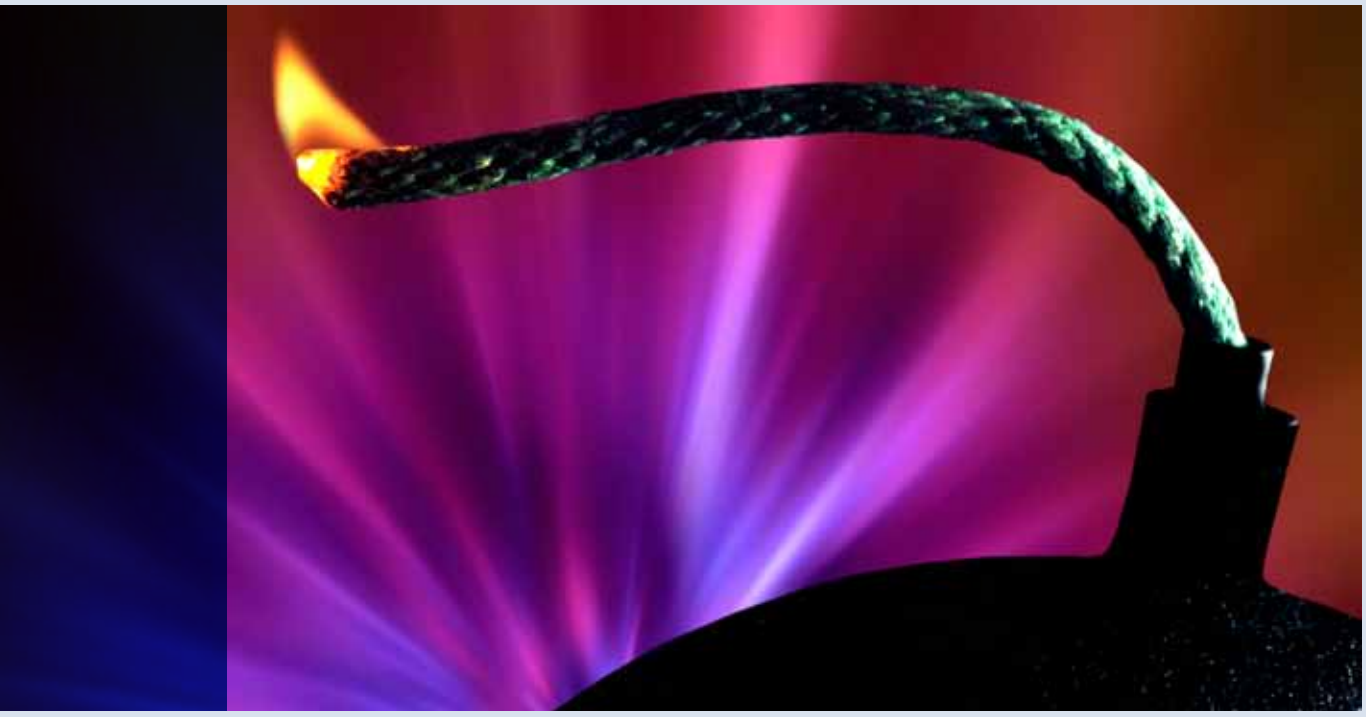
6.2.4. Velkendte spredningsmetoder

Som sikkerhedsmand har jeg ingen holdning til kryptovaluta. Det er et værktøj, som kan bruges til både gode og dårlige formål. Når it-kriminelle kaster sig over det, er årsagen enkel: Der er penge at hente.

Metoderne til at sprede skadelig software, der danner kryptovaluta, er velkendte: Udnyttelse af kendte sårbarheder eller svindel.

Så vi har ikke brug for at udvikle nye beskyttelsesværktøjer. I stedet kan vi gentage de gode, gamle råd: Hold software opdateret. Lad være med at klikke på noget, du ikke har bedt om.

Oprindelig offentliggjort den 23. februar 2018



6.3. KUNSTIG INTELLIGENS HAR STOR BETYDNING PÅ IT-SIKKERHEDSOMRÅDET: KAN HJÆLPE BÅDE ANGRIBERE OG FORSVARERE - MEN SKAL ANVENDES RIGTIGT

Machine learning og andre teknologier inden for kunstig intelligens kan hjælpe såvel hackere som sikkerhedsfolk.

Ansigtsgenkendelse. Selvkørende biler. Diagnosticering af patienters sygdomme.

Tre eksempler på områder, hvor kunstig intelligens indgår. Teknologien kan løse problemer på nye måder og åbne for nye muligheder. Men den medfører også sikkerhedsmæssige udfordringer.

Jeg mener, vi bør betragte kunstig intelligens og sikkerhed fra to vinkler: Angriberens og forsvarerens. Angriberen kan være en it-kriminel, der er ude efter penge eller fortrolige oplysninger. For en angriber indebærer kunstig intelligens mindst tre muligheder.

For det første kan traditionelle typer af angreb forstærkes og forbedres med kunstig intelligens.

Et eksempel kan være målrettet svindel, såkaldt spear phishing. En angriber kan bruge machine learning til at analysere potentielle ofres opførsel.

Når et offer klikker på et link til en forfalsket loginside, bruger systemet den viden til at forbedre sin indsats: Det bliver klogere på, hvad der skal til for at lokke folk i fælden. For det andet kan de kriminelle angribe kunstig intelligens-systemer hos deres ofre.

Det kan eksempelvis ske ved at forgifte de data, der indgår i modellerne til machine learning. Den type systemer lærer ved at blive præsenteret for store mængder data. For eksempel kan et system lære at genkende et billede af et får ved at se en masse billeder af får. Men hvis en angriber har held til at smide en bunke billeder af ulve ind i datasættet, bliver modellen forvirret, så den ikke længere kan genkende et får.

Den tredje mulighed for angribere går ud på at stjæle den værdi, som indgår i systemerne med kunstig intelligens. Det kan for eksempel være hele den model, som en virksomhed anvender til at vurdere værdipapirer med.

Dermed kan angriberen udnytte virksomhedens viden til at score kassen på børsspekulationer.

6.3.1. Analyse af trafikdata

Og nej, angreb med og på systemer med kunstig intelligens er ikke noget fundamentalt nyt sikkerhedsmæssigt.

Vores opgave som sikkerhedsfolk er fortsat at sikre informationernes tilgængelighed, fortrolighed og autenticitet. Men der kan blive brug for nye værktøjer til at beskytte de nye typer systemer. Et af de værktøjer kan være – kunstig intelligens.

I DKCERT undersøger vi således mulighederne i at bruge machine learning til at analysere netværksdata. Vi har adgang til metadata om den trafik, der går gennem de centrale routere i forskningsnettet.

Ved at hente de data ind i et paralleliseret big datasystem kan vi analysere dem. Vores plan er at opbygge et system, der lærer at genkende trafikmønstre, som vi er interesserede i. Machine learning kan gøre det muligt at se angrebsmønstre, som ellers kan være svære at opdage. Dermed vil vi hurtigere kunne opdage og standse angrebsforsøg.

Måske vil teknologien ligefrem kunne hjælpe os med at forudsige fremtiden: Ud fra data om tidligere angreb kan vi forudse kommende angreb.

6.3.2. Styrker password-sikkerhed

Machine learning kan også gøre autentifikation af brugere mere sikker. Traditionelt har vi stolet på kombinationen af et brugernavn og et password. Men erfaringen viser, at den kombination ikke er stærk nok: Brugere genbruger passwords på tværs af tjenester eller vælger svage passwords, der er lette at gætte.

Her kan machine learning komme ind: Autentifikationssystemet nøjes ikke med at tjekke, om brugernavn og password passer sammen. Det ser også på, om login-proceduren ser rigtig ud: Plejer brugeren at logge ind fra dette netværk med denne enhed på denne geografiske placering? Er der mange fejlslagne forsøg? Er klokken tre om natten – og er det normalt for brugeren?

Hvis systemet synes, noget virker tvivlsomt, kan det stille krav om ekstra sikkerhed, for eksempel via to-faktor-autentifikation.

6.3.3. Kig på teknologien

Hvis jeres organisation anvender kunstig intelligens-teknologier, bør I overveje, hvilke særlige krav det stiller til sikkerhedssystemerne. Uanset om I bruger kunstig intelligens, kan jeg anbefale at tage teknologien med i overvejelserne, når I planlægger fremtidens sikkerhed. Kunstig intelligens kan øge truslerne mod jeres informationer. Men den kan også forbedre sikkerheden, hvis den bruges rigtigt.

Oprindelig offentliggjort 26. april 2018

6.4. KRIMINELLE ER BEGYNDT AT BRUGE SEX, ADGANGSKODER OG TELEFONNUMRE TIL AT SKRÆMME DIG TIL AT BETALE LØSEPENGE

Sofistikerede afpresningsmails med informationer om din adgangskode eller dit telefonnummer er begyndt at pible frem. Her er tendenserne i fremtidens digitale personangreb og metoder til at undgå dem.

"I will directly come to the point. I'm aware [fjernet af DKCERT] is your password. More importantly, I know about your secret and I have proof of your secret."

Sådan indledes en afpresningsmail, som en række danskere modtog tidligere på sommeren. Længere nede i mailen fortæller angriberen, at han har overtaget ofrets computer og benyttet det indbyggede kamera til at optage sekvenser, der viser vedkommende i færd med at se pornografisk materiale - og hvad der hører med i den forbindelse.

Hvis ofret ikke betaler en angivet sum, så trues der med offentliggørelse af de kompromitterende videoer. Ofret, der modtog denne konkrete mail, henvendte sig til DKCERT, blandt andet fordi der var overensstemmelse med det password (som jeg har fjernet) og et password, som ofret tidligere har anvendt til sine konti.

6.4.1. Slår på de bløde punkter

De (næsten) matchende adgangskoder er typisk blevet opsamlet i forbindelse med data-brud på databaser med adgangskoder og koblet sammen med andre data om brugeren. Sådanne oplysninger kan købes for ganske få kroner på lyssky net-fora.

Afpresseren rammer på denne måde ofret på flere bløde områder med sine slag, og det kan få nogle til at betale den ønskede mængde bitcoin i løsepenge. Faktisk har jeg flere eksempler på, at det er sket.

Big data og analyse af store datamængder er altså på vej til at blive et vigtigt værktøj, som de kriminelle anvender i deres aktiviteter med at svindle penge fra uskyldige ofre. Hvilket, der er flere eksempler på.

6.4.2. Jeg har dit telefonnummer

Ovenstående forsøg på afpresning er nemlig ikke enestående, og der findes flere forskellige udgaver af personhenvendte udsendelser, eksempelvis, hvor de sidste fire cifre af ofrets telefonnummer er angivet.

Disse oplysninger er sandsynligvis opsamlet via sms-godkendelser og igen solgt videre på nettet. Men princippet er det samme. Angriberen rykker tættere på sit offer gennem udnyttelse af informationer, der er samlet op på nettet og ved at stykke informationerne sammen på en ondskabsfuld måde.

Ved at samkøre data som bopæl, navn, seksuelle præferencer, datingvaner, adgangskoder eller telefonnumre bliver angrebet yderst personligt og presser ofret meget hårdt. Og det er desværre den tendens, som jeg forventer vil udvikle sig i fremtidens afpresningskampagner.

Og angrebene begrænser sig ikke til computeren. Telefonen vil i større omfang blive en vigtig angrebsplatform for de kriminelle, der forsøger afpresning.

6.4.3. Det kan du selv gøre

Du kan selvfølgelig ikke sikre dig mod at modtage en afpresningsmail i indbakken, men du kan tage forholdsregler mod de kriminelle.

Vi ved det selvfølgelig alle sammen, men desværre glemmer vi det ofte i hverdagens netbrug: Alle de data, der er lagt på nettet, kan genfindes og stykkes sammen på en måde, der ikke nødvendigvis afspejler sandheden. Derfor skal du huske, at være kritisk i forhold til hvad du gør, og hvad du deler. Stol på din sunde fornuft.

Gode password-vaner er ligeledes et meget effektivt værktøj til god sikkerhed. Sørg altid for at dine adgangskoder er lange, gerne mere end 12 tegn. Du må ikke bruge den samme adgangskode til flere tjenester og anvend så to-faktorsikkerhed alle de steder, det er muligt.

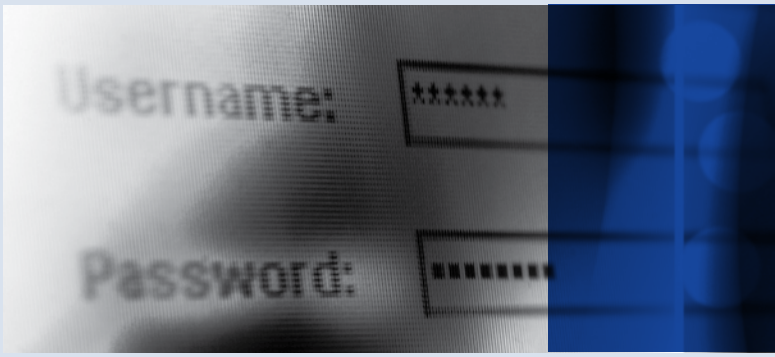
En krypteret tunnel via VPN giver også stærkere sikkerhed. En mulighed, der understøttes direkte i nogle browsere, i nogle antivirusprogrammer eller du kan købe tjenesten særskilt.

6.4.4. Sådan sparer du penge

Og så lige et tip til at spare penge: Du skal ikke betale én eneste krone til ondsindede kriminelle, der presser uskyldige ofre.

Dem kan du roligt beholde selv. Hvis du betaler, så ved den kriminelle, at der er mulighed for at hente endnu flere penge, hvilket er skruen uden ende.

Oprindelig offentliggjort 31. august 2018



6.5. NÅR KRISEN BRYDER LØS, BEDØMMES DU PÅ FORBEREDELSEN

Her er tre grundelementer, der skal sørger for, at du holder organisationen oven vande, når lokummet for alvor begynder at brænde. Dette skal du have med i din kriseplanlægning.

Forberedelse er roden til alt godt.

Det gælder naturligvis også, når det handler om håndtering af en krise i organisationen. Både hvis det handler om nedbrud på netværket, alvorlige GDPR-problemer eller interne vanskeligheder, der sætter organisationen i stå og truer dens overlevelse.

Jeg deltager jævnligt i krisehåndteringsøvelser og er netop hjemvendt fra CLAW, der er en workshop for europæiske forskningsnet, hvor man skal håndtere et krisescenarium.

Den fiktive krise min team blev præsenteret for, var en kombination af eksterne angreb og interne netværksfejl, der satte en stopper for, at 200.000 studerende kunne afslutte deres online-eksamen. Vi havde halvanden time til at løse de tekniske problemer, holde pressen orienteret og få sikkerheden på plads.

Selv om denne opgave var udtænkt bag et skrivebord, så er krisestyring også meget aktuel i den virkelige verden. Skræmmeeksemplet er fra sidste år, hvor Mærsk-koncernens it-systemer kom under belejring af NotPetya-malware-angrebet i ni dage. En krise, der 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 din plan og øvet den strategi i planlægger, så alle ved, hvad der skal gøres.

6.5.1. Rollerne skal fordeles

Det første du bør gøre, er at definere de forskellige roller samt beslutte hvem, der kan igangsætte et kriseberedskab. Husk, at en krise kan strække sig over lang tid, hvilket betyder, at der kan være behov for afløsning på de enkelte pladser.

Du skal planlægge, hvem der skal gøre hvad og uddanne dem i det.

Helt konkret kan teamet bestå af en beredskabsleder, en eller flere kommunikationsansvarlige, nogle, der kan rådgive om sikkerhed og databeskyttelse, samt nogle, der kan koordinere den tekniske genoprettelsesproces og så fremdeles.

Der vil altid være behov for både intern og ekstern kommunikation under krisen. Det kan være mellem kriseberedskabet og virksomhedens ledelse, til de øvrige medarbejdere samt udadtil, hvor kunderne, pressen, og måske politiet og/eller andre myndigheder skal informeres.

Derfor er kommunikationsfolkene altid med i temaet, uanset krise-typen.

Sidst men ikke mindst skal der være nogle, der fører en log over forløbet med henblik på evaluering, så den samme situation kan undgås i fremtiden. Af skade bliver man nemlig tit klog, men sjældent rig. Derfor er det altid vigtigt at evaluere en hændelse.

6.5.2. Planlæg det unormale

Det næste element er den største opgave.

Når der er udpeget folk, skal du udvikle en plan for, hvordan de skal arbejde og handle, når hverdagen ramler. En krise er jo netop defineret ved, at normale tjenester/funktioner er ude af drift.

Derfor er det vigtigt, at du forudser at ting, der normalt bare fungerer, kan svigte. Det kan eksempelvis være planer for, hvordan man får fat i eksterne og interne personer, hvis mail- eller telefonsystemet bryder sammen.

Ligeledes bør man definere hvem, der skal informere eksempelvis brugere, kunder, bestyrelse og medarbejdere, når der opstår problemer. Igen skal du beslutte, hvordan informationen bringes videre, hvis den webside, du normalt anvender, er nede.

Et andet element i en kriseplan er, at der er dele af virksomhedens ansatte, som skal skærmes af og vejledes i et roligt og forståeligt sprog, der kan relateres til. Direktøren skal således ikke overdynges med it-tekniske problemer, men informeres om status og konsekvenser på overordnet niveau, der eksempelvis kan videregives pressen.

Husk også de lav-praktiske ting som eksempelvis hvilke lokaler, der skal anvendes og sørg altid for god forplejning samt godt humør under krisehåndtering.

Denne plan skal være så enkel som mulig og generisk, forstået på den måde, at den kan passe til forskellige kriser og være den platform, som man kan arbejde ud fra, når tingene bevæger sig i ukendte retninger.

6.5.3. Øvelse gør stadig mester

Det sidste grundelement er øvelse.

En forkromet plan, der havner i en skuffe uden, at der er nogen, som kender den, har ingen værdi i praksis. Et beredskab kræver øvelse, der skal være efterfulgt at en evaluering, så der kan optimeres på processen. Som den preussiske generalstabschef Helmuth von Moltke ofte bliver citeret: "Selv den bedste plan holder kun til første møde med fjenden".

Men hvis du er godt forberedt og har øvet din plan, så kan du også improvisere og tilpasse dig situationen. Og det er det, der skal til for at vinde slaget.

Oprindelig offentliggjort 29. november 2018

7. Fremtidens trusler og trends

It-kriminelle bliver stadig mere professionelle, og deres angreb bliver i højere grad baseret på brugerens frygt. Beskyttelsen af personlige data kommer i centrum sammen med dataetik.

De kriminelle går efter pengene og udnytter alle de beskidte tricks i bogen. Det er den korte beskrivelse af de typiske it-kriminelle i 2019.

7.1. TRUSLER MOD INFORMATIONS-SIKKERHEDEN I 2019

7.1.1. Afpresning gennem frygt

En af de tendenser, vi har oplevet i 2018, er digital afpresning og i det kommende år, vil angrebene blive yderligere raffinerede og spille mere på brugernes frygt.

Ransomware, hvor indholdet på brugerens, virksomhedens eller organisationens computer bliver krypteret af en kriminel, der kun vil frigive det igen mod betaling, er stadig på dagsordenen.

I 2018 har vi også haft flere opblomstringer af såkaldt sextortion, hvor de kriminelle forsøger at afpresse ofrene via trusler om offentliggørelse af vedkommende i kompromitterende situationer af seksuel karakter.

I den sidstnævnte kategori anvendes angst/ydmygelse som angrebsvåben og denne form for afpresning, kan vi desværre forvente mere af: Ved at skræmme ofrerene med områder som seksualitet, sundhed eller trusler i familiemæssig sammenhæng, kan der tjenes penge. Det er metoder, som kriminelle kan opfatte som gode forretningsmodeller for deres lyssky aktiviteter.

Til at håndtere betalingerne mellem den kriminelle og ofret anvendes digitale valutaer. Krypto-valutaer er en nem og ofte anonym måde at få betaling på for kriminelle tjenester. Endvidere vil vi se endnu flere eksempler på hacking og skadelig software, der lader ofrenes computere danne kryptovaluta for de kriminelle.

7.1.2. GDPR-hacktivisme blusser op

Et andet områder DKCERT forventer at se aktivitet omkring i 2019, er hacktivisme i forbindelse med offentliggørelse af data.

GDPR-implementeringen betyder, at der er udsigt til store bøder, hvis man ikke passer godt på folks data. Dette kan udnyttes i forbindelse med politisk motiveret hacking - hacktivisme. Ordet er en sammentrækning af "hack" og "aktivisme". Det dækker forfølgelse af politiske mål ved hjælp af midler som defacement, DDoS-angreb og altså informationstyveri.

Ved at skaffe sig adgang til - og derefter lække data, der burde være fortrolige, kan firmaer sættes i miskredit hos brugerne, i medierne og samtidig komme i problemer med Datatilsynet og derved være i risikozonen for en klækkelig bøde.

7.5.3. Phishing – den evige trussel

Phishing har længe været et af de kriminelles foretrukne angrebsværktøjer. Denne forholdsvis enkle metode forventes stadig at udgøre hovedparten af al it-kriminalitet.

Det gælder fx phishing-mails til at narre passwords fra ofrene. Test viser, at phishing er en effektiv metode: En del af brugerne lader sig stadig narre til at udlevere fortrolige oplysninger.

7.2. SIKKERHEDSTRENDS I 2019

7.2.1. Persondata kommer - igen - i centrum

Beskyttelsen af persondata kommer også til at fylde meget i 2019. En væsentlig årsag er, at databeskyttelsesforordningen trådte i kraft den 25. maj 2018. Det har naturligvis gjort mange offentlige myndigheder og private virksomheder opmærksomme på, at de skal have styr på data.

Der er gjort mange tiltag i kølvandet på GDPR, og i den kommende tid skal det så vurderes, om disse virker i praksis. Vi skal have kortlagt, om vi har gjort tingene godt nok. Tiltagene skal testes i sin helhed og i forhold til revision.

Det betyder også, at vi må regne med, at flere af de sager, der er anmeldt til Datatilsynet i løbet af 2018, kommer til at få en afgørelse i 2019. Datatilsynet modtog i 2018 næsten 3.000 indberetninger, der nu skal undersøges til bunds.

7.2.2. Dataetik er i fokus

2019 bliver året, hvor dataetik kommer i fokus i sammenhæng med sikkerhed. Og vi er allerede i gang.

Siden marts 2018 har en ekspertgruppe arbejdet på at identificere et sæt anbefalinger, der kan bidrage til ansvarlig og bæredygtig anvendelse af data i erhvervslivet. Anbefalingerne kom i november.

Sideløbende med ekspertgruppens arbejde, der især retter sig mod den private sektor, har organisationen Dansk IT udarbejdet et sæt dataetiske regler, der udvider anbefalingen til at omfatte offentlige myndigheder. En række af de største dataetiske udfordringer i disse år opstår faktisk i den offentlige sektor, fremhæver Dansk IT.

Allerede nu snakker vi således om initiativer vedrørende dataetik affødt af udviklingen i retning af mere kunstig intelligens og robotics. Disse vigtige områder kommer til at stå højt på 2019-dagsordenen.

Ligeledes kan vi forvente aktivitet i forbindelse med både Folketingsvalg og valg til EU-parlamentet, hvor etikken kommer til at handle om spredningen af falske nyheder eksempelvis via sociale medier.

7.2.3. Password managers i fremmarch

I 2018 har der været meget fokus på adgangskoder, og nye anbefalinger betyder, at de skal være længere. Ulempen er, at lange adgangskoder kan være svære at huske, hvilket betyder, at der er brug for en hjælpende hånd i form af en password manager.

En password manager er et program, der opbevarer brugernavne og passwords. For at åbne programmet skal brugeren indtaste et password. Dermed behøver brugeren kun at huske et password, hvorefter der er adgang til et ubegrænset antal passwords. Til gengæld er det afgørende, at adgangskoden til password manager-programmet er meget sikkert.

I takt med en øget bevidsthed om stærke adgangskoder, forventer DKCERT en stigning i brugen af password managers.

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 dem.
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 øget 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 – tænk her også på kravene i databeskyttelsesforordningen.
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 kan koste dyrt i form af økonomisk tab, brud på databeskyttelseslovgivningen, 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 informationssikkerheden.
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.
11 Afsæt tid, penge og personale til håndtering af informationssikkerhed.

9. Ordliste

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

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 pc er inficeret med et botnet-program 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 it-sikkerheden betegner det afprøvningen af kombinationer af brugernavne og kodeord, ofte ud fra foruddefinerede lister og ordbøger.

Command & control server (C&C)
Et botnets centrale servere, hvorigennem det er muligt at sende kommandoer, som udføres af computere i botnettet, der er inficeret med botnet-programmer.

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.

Cryptomining
Infektion af offerets computer med malware, der skjult udnytter regnekraften til at danne kryptovaluta (typisk Monero) til fordel for angriberen. Processen er meget strømforbrugende og kan være dyr for offeret.

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.

DCIS
Decentral Cyber- og InformationsSikkerhedsenhed, et begreb fra National strategi for cyber- og informationssikkerhed 2018. Seks samfundskritiske sektorer skal hver oprette en DCIS, der kan bidrage til gennemførelsen af sektorvise trusselsvurderinger, overvågning, beredskabsøvelser, sikkerhedsopbygning, vidensdeling, vejledning mv.

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
Falske e-mails ofte sendt til regnskabsafdelingen. Mailen 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.

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.

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.

GDPR (General Data Protection Regulation)
Databeskyttelsesforordning, vedtaget af EU-parlamentet og medlemsstaternes regeringer i 2016, der trådte i kraft i maj 2018. Forordningen stiller krav til beskyttelsen af persondata.

God selskabsledelse (corporate governance)
En metode til at sikre en hensigtsmæssig rolle- og ansvarsfordeling i forbindelse med kontrol og styring af organisationen. Et væsentligt element af god selskabsledelse er risikostyring og revision.

GovCERT
GovCERT-funktionen (Government Computer Emergency Response Team) skal sikre, at der i staten er overblik over trusler og sårbarheder i produkter, tjenester, net og systemer. På den baggrund skal tjenesten foretage en løbende vurdering af informationssikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler. I Danmark er GovCERT placeret i Center for Cybersikkerhed under Forsvarets Efterretningstjeneste.

Hacker
På dansk betyder hacker en person, der uden foregående tilladelse forsøger at kompromittere computersystemers sikkerhed. 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.

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.

Kryptovaluta
En digital valuta baseret på teknologierne kryptering og blockchain. Eksempler er Bitcoin og Monero.

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.

Man-in-the-middle
En angrebsform, hvor kommunikationen mellem to parter uden parternes vidende videresendes til en mellemmand, der aktivt kan kontrollere kommunikationen.

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.

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.

Phishing
Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på phishing optræder ofte i e-mails, der henviser til websider. Websiden angiver at tilhøre offerets bank, kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol.

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

Sextorsion
Sammentrækning af ordene "sex" og "extorsion" (afpresning). Phishing-kampagne, der påstår at have overtaget brugerens computer med kamera og at have optaget brugeren i kompromitterende situationer. Afpresseren truer med at offentliggøre optagelserne.

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.

SQL injection (SQL-indsætning)
Et angreb der ændrer i indholdet på en webside ved at sende kommandoer til den bagvedliggende SQL-database gennem usikre input-felter på websiden, som for eksempel søgefelter eller kommentarfelter, eller gennem usikre parametre i websidens URL'er.

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 supplerer brugernavn og password med en yderligere faktor, som brugeren skal angive for at få adgang. Det kan være en engangskode, der sendes til brugerens mobiltelefon som sms, et fingeraftryk, der angives via en fingeraftrykslæser, en kode fra et papirkort eller lignende.

Trojansk hest
Et program der har andrefunktioner end dem, som det foregiver at have. Trojanske heste indeholder ofte dialer-, bagdørs- eller keylogger-funktionalitet, eller benyttes til installation af virus, botnet-programmer og lignende.

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.

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

10. 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