DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

DKCERT Trendrapport 2018

Redaktion: Henrik Larsen og Torben B. Sørensen

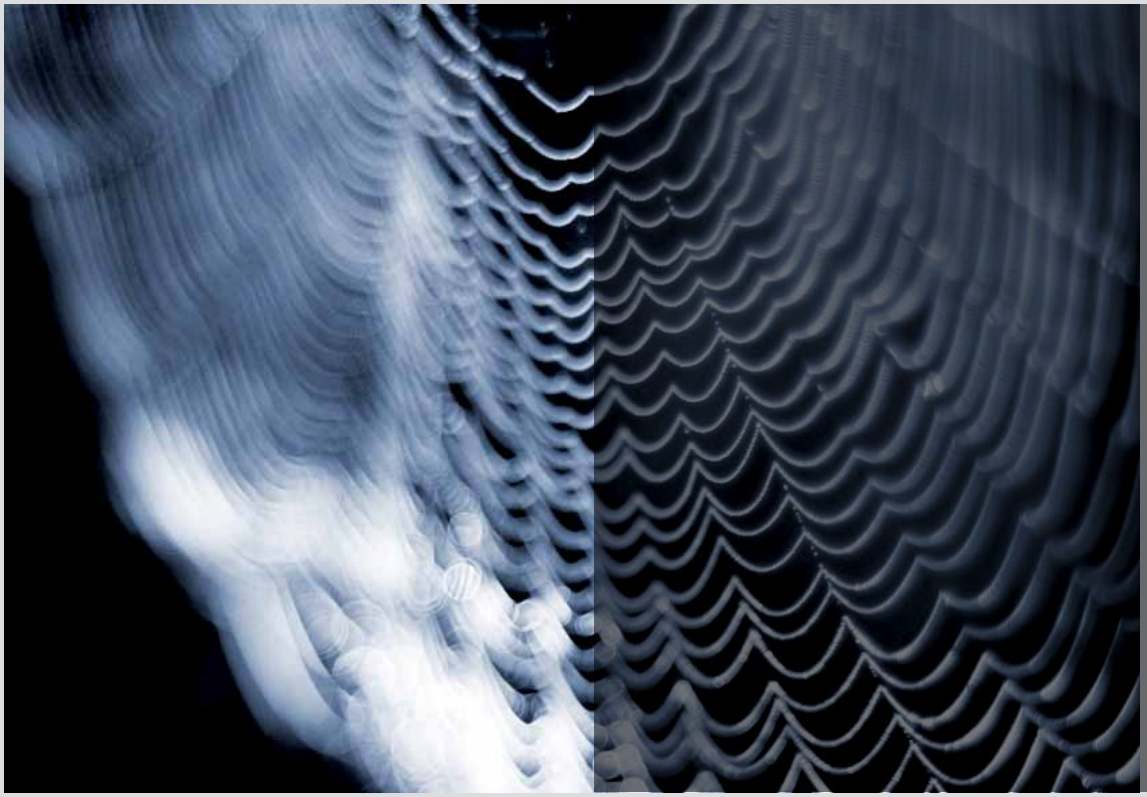
Tak til vore øvrige bidragydere:
Ole Hult, F-Secure,
Jesper Husmer Vang, Datatilsynet,
Henning Mortensen, Rådet for Digital Sikkerhed,
Lisa Ibenfeldt Schultz, Københavns Universitet,
Kathrin Otrel-Cass, Aalborg Universitet og
Morten Eeg Ejrnæs Nielsen, DKCERT, DeiC.

DeiC-journalnummer: DeiC JS 2018-01

Design og layout: Kiberg & Gormsen

DKCERT - en del af DeiC
DTU, Asmussens Allé, Bygn. 305
2800 Kgs. Lyngby

Om DKCERT



DKCERT, der er Danmarks akademiske CSIRT (Computer Security Incident Response Team), bygger på en vision om at skabe værdi for uddannelses- og forskningssektoren i form af øget informationssikkerhed. Det sker gennem offentliggørelse af viden om 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 grundidé i CERT/CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DKCERT om informationssikkerhed i uddannelsessektoren i Danmark. DKCERT er fuldt medlem af FIRST (Forum of Incident Response and Security Teams) samt akkrediteret medlem af Trusted Introducer og TF-CSIRT (Task Force Computer Security Incident Response Team) under GÉANT.

Indholdsfortegnelse

1. Velkomst

Vores egen historie kan løse vores fremtidige problemer - fra ITIL til GDPR.

Vi glemmer indimellem vores historie. Det er problematisk. Det mener jeg ikke kun i kraft af min baggrund som historiker og arkæolog, men fordi historieløsheden gør, at vi overser oplagte løsninger på aktuelle problemer.

I dag er alle offentlige og en god del private organisationer optaget af, hvordan de skal leve op til kravene i databeskyttelsesforordningen (GDPR). Der er mange krav, og det kan virke kompliceret. Men ser vi blot nogle få år tilbage, finder vi nogle bud på, hvordan det kan blive lettere at overholde kravene.

Tænk på ITIL (Information Technology Infrastructure Library). Det er et sæt retningslinjer for, hvordan man følger best practices inden for it-drift. ITIL var meget omtalt i det første årti af dette århundrede. Vi var en del, der prøvede at følge principperne. Min egen erfaring er, at ITIL var med til at lette ledelsesarbejdet og øge kvaliteten af it-servicen, fordi der kom styr på processerne.

Siden fulgte ISO 27000-serien af standarder for sikkerhedsarbejdet. Igen kom der struktur på processer, denne gang specifikt inden for informationssikkerhed.

De organisationer, der har taget først ITIL og siden ISO 27000 til sig, har et rigtig godt grundlag for at overholde GDPR-kravene. Implementeringen kan blive nogenlunde smertefri, fordi meget af forarbejdet er på plads. Har man også forholdt sig til Sikkerhedsbekendtgørelsen og Persondataloven – begge fra maj 2000 – er man rigtig godt på vej. Så er det jo heldigt, at overholdelse af ISO 27001 længe har været et krav til alle statslige organisationer. Bare en skam, at mange ikke er nået særlig langt med arbejdet.

Hvis man ikke er historieløs, ser man ruten fra ITIL over ISO 27000 til GDPR som skridt på den samme vej. Glemmer man historien, ser man GDPR som en uforudset udfordring, der dukker op som et lyn fra en klar himmel.

Uanset hvor velforberedt man er, skal alle organisationer og virksomheder efterleve kravene fra den 25. maj 2018.

Til at hjælpe institutioner inden for forskning og uddannelse har DeiC i 2017 etableret DPO-tjenesten i DKCERT. Den store interesse for tjenesten dokumenterer, at mange har brug for hjælp. Derfor har vi også sat databeskyttelsesforordningen i fokus i dette års trendrapport.

God fornøjelse med læsningen!

Henrik Larsen
chef for DKCERT

2. Resumé

DKCERT behandlede færre sikkerhedshændelser og indførte en ny tjeneste i 2017.

DKCERT behandlede 4.736 sikkerhedshændelser på forskningsnettet i 2017. Det er 45 procent færre end året før. De fleste hændelser var klager over piratkopiering.

DKCERTs sårbarhedsscanninger fandt sårbarheder på 44 procent af de IP-adresser, der blev undersøgt. I gennemsnit blev der fundet 8,4 sårbarheder på hver af de sårbare IP-adresser. De fleste sårbarheder lå i systemer til kryptering af web-trafik.

DKCERT registrerede knap 70.000 advarsler fra tredjepart om sårbare systemer på forskningsnettet. Over en tredjedel handlede om sårbarheden POODLE (Padding Oracle On Downgraded Legacy Encryption).

Mængden af modtagere af DKCERTs ugentlige nyhedsbreve steg otte procent til 1.451 abonnenter. Antallet af følgere på Twitter steg 31 procent til 2.065 personer.

2.1. TENDENSER FRA ÅRET DER GIK

Ransomware var igen udbredt. Det er skadelige programmer, der spærrer for adgangen til data og kræver en løsesum. To store angreb med ransomware vakte opmærksomhed: WannaCry og NotPetya. WannaCry anvendte en nyopdaget angrebsmetode, der udnyttede et nyopdaget sikkerhedshul i Windows. Pc'er, der ikke var opdateret, var sårbare.

NotPetya ramte få, men store ofre. Mærsk anslog, at det kostede virksomheden tæt på to milliarder kroner at rydde op efter angrebet.

Big data-systemer, hvor store datamængder lagres og analyseres på nettet, blev ramt af en anden form for afpresning: Uvedkommende overtager administrationen af databasen, kopierer og sletter data, og kræver derefter løsepenge for at frigive dem.

Data om millioner af mennesker kom i de forkerte hænder. I en af sagerne skyldtes det, at software ikke var blevet opdateret, så hackere kunne udnytte en sårbarhed til at få fat i data.

2.1.1. Databeskyttelse er i fokus

EU's databeskyttelsesforordning (GDPR) er vedtaget, men bliver først håndhævet fra den 25. maj 2018. Den medførte megen aktivitet, hvor virksomheder, myndigheder og organisationer begyndte at forberede sig på at efterleve de nye regler. Denne trendrapport indeholder et særligt afsnit med forskellige indgange til problemstillingen.

DeiC introducerede i 2017 en ny tjeneste, knyttet til DKCERT, der rådgiver institutioner om EU's databeskyttelsesforordning. Tjenesten tilbyder et netværk med erfaringsudveksling og muligheden for at leje en databeskyttelsesrådgiver (DPO, Data Protection Officer).

2.2. TENDENSER I 2018

Professionaliseringen af it-kriminalitet vil fortsætte. En professionel underverden tilbyder tjenester, produkter og værktøjer til nye kriminelle.

Flere skadelige programmer vil installere funktioner til at danne kryptovalutaer som Bitcoin og Monero på ofrenes computere.

Angreb på Internet of Things-enheder vil også ramme intelligente armbåndsure, smykker, tøj og øvrige enheder, der kan sættes på nettet.

Simple angrebsmetoder vil fortsat være udbredte: Udnyttelse af gammelkendte sårbarheder på systemer, der ikke er opdateret. Phishing-svindel, der narrer fortrolig information fra ofrene. Direktørsvindel, hvor mails giver sig ud for at komme fra en ledende medarbejder, der har brug for at overføre et beløb til en udenlandsk konto.

3. 2017 – året i tal

DKCERT behandlede 4.736 sikkerhedshændelser i 2017.

DKCERT behandler sikkerhedshændelser på forskningsnettet. Som oftest kommer henvendelserne fra andre CERT-organisationer, der har observeret uønsket adfærd fra IP-adresser på forskningsnettet. DKCERT svarer på henvendelsen og sender klagen videre til den institution, der anvender den pågældende IP-adresse.

3.1. ÅRETS SIKKERHEDSHÆNDELSER

I alt behandlede DKCERT 4.736 sikkerhedshændelser i 2017 (se Figur 1). Det er 45 procent færre end i 2016, hvor der var 8.604 (se Figur 2).

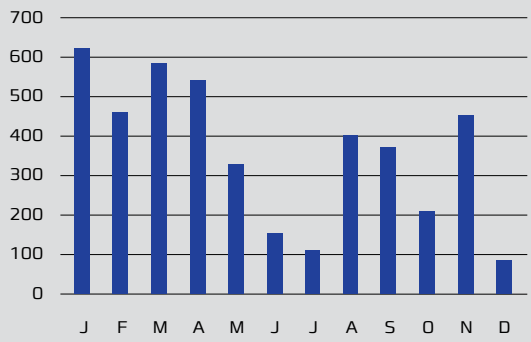
En mulig forklaring på faldet kan være, at sikkerheden på institutionerne på forskningsnettet er forbedret, så de bliver udsat for færre angreb.

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 ransomwareangreb bliver anmeldt til DKCERT.

Tallet omfatter ikke de advarsler fra tredjeparter om sårbare systemer, som tidligere har indgået i statistikken. Vi har i år valgt at flytte disse tal til afsnittet om sårbarheder, da de ikke er egentlige sikkerhedshændelser.

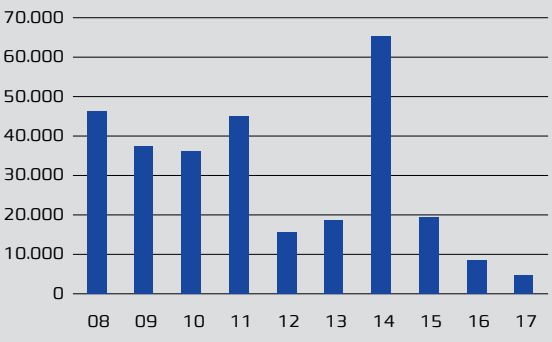
Figur 1: Sikkerhedshændelser behandlet af DKCERT i løbet 2017

Sikkerhedshændelser måned for måned



Figur 2: : Udvikling i antallet af sikkerhedshændelser, DKCERT behandler.

Der var flere sager frem til 2012, fordi DKCERT indtil da også behandlede henvendelser uden for forskningsnettet. Stigningen i 2014 skyldes advarsler fra tredjepart, der i de følgende år blev filtreret fra.



3.2. SIKKERHEDSHÆNDELSER FORDELT PÅ TYPER

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

3.2.1. Piratkopiering

Piratkopiering var igen i 2017 den sagstype, der forekom hyppigst. Det drejer sig typisk om sager, hvor et Firma klager over, at en bruger har hentet eller distribueret piratkopier af film, tv-serier eller musik. Firmaet repræsenterer som regel rettighedsindehaveren, der kan være et filmselskab eller lignende.

1.850 af sagerne i 2017 handlede om piratkopiering. Der skete imidlertid et voldsomt fald hen over året: Næsten 1.600 sager lå fra januar til april, hvorefter mængden faldt drastisk. I december var der kun to sager (se Figur 3).

En del af forklaringen kan være, at en bestemt IP-adresse, der modtog mange klager, lukkede ned efter henvendelse fra DKCERT sidst på foråret.

3.2.2. Portscanninger

Portscanninger var nummer to på listen over de hyppigste sagstyper i 2017. 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 og lignende forsøg på at finde information om potentielle angrebsmål steg efter sommerferien (se Figur 4). Årsagen er ukendt.

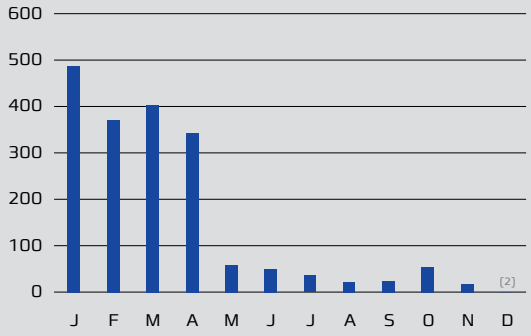
3.2.3. Spam

Sager om spam var nummer tre 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.

Der var en løbende stigning i antallet af sager frem til maj måned, hvorefter de stilnede af (se Figur 5).

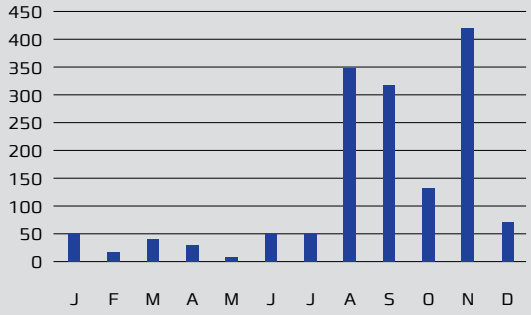
Figur 3: Sager om piratkopiering i årets løb

Antal sager faldt drastisk hen imod årets udgang.



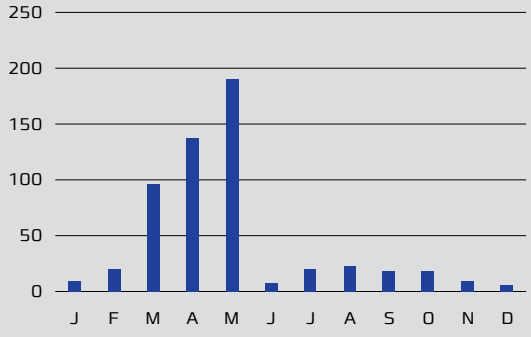
Figur 4: Portscanninger og andre forsøg på rekognoscering

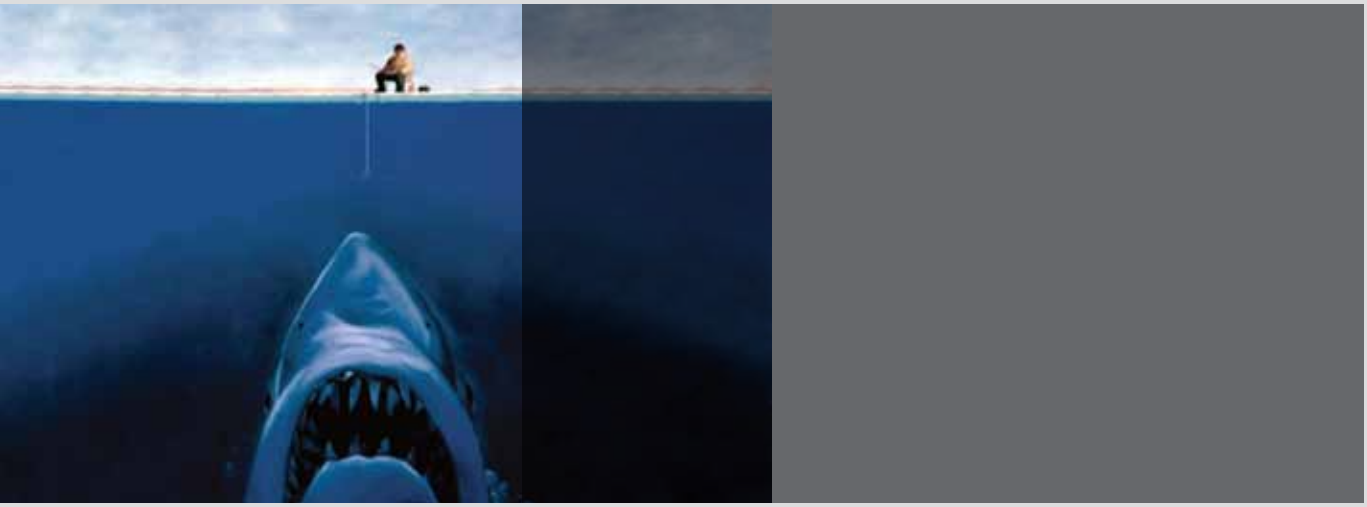
Antallet af portscanninger steg efter sommerferien.



Figur 5: Spam

De fleste klager over spam kom i løbet af foråret.





3.2.4. Uautoriseret adgang

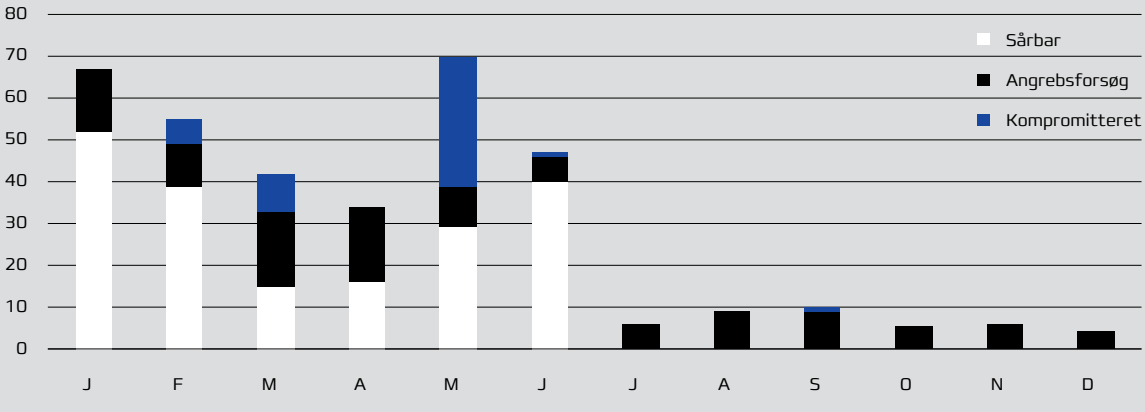
DKCERT opdeler hændelser om uautoriseret adgang til it-systemer i tre undertyper: Kompromitterede systemer, angrebsforsøg og systemer, der potentielt kan overtages, fordi de er sårbare. I første halvår så vi alle typer, derefter var det primært forsøg på angreb (se Figur 6).

3.2.5. Øvrige typer

Foruden de nævnte typer af sikkerhedshændelser har DKCERT behandlet nogle få sager om phishing.

Figur 6: Sager om uautoriseret adgang til it-systemer

Der var kun få sager med systemer, der blev overtaget af uvedkommende.



3.3. MALWARE-UDVIKLINGEN

Trojanske heste udgør en stadig større andel af de skadelige programmer, der rammer danskerne. Det fremgår af statistikker fra sikkerhedsfirmaet F-Secure over de trusler, firmaets produkter har standset hos danske kunder. En trojansk hest er et skadeligt program, der giver sig ud for at være et pålideligt program, som offeret har tillid til.

92 procent af truslerne var trojanske heste (se Figur 7). I 2016 var andelen 89 procent, året før 84 procent. På andenpladsen kom exploits – det er programmer, der udnytter kendte sårbarheder. De udgjorde tre procent mod seks procent året før.

Den mest udbredte trussel i Danmark i 2017 kalder F-Secure Trojan.Cryxos (se Figur 8). Programmet viser en skræmmende advarsel om, at computeren er blevet "blokeret" på grund af en virusinfektion, og at brugerens data er stjålet. Brugeren opfordres til at ringe til et telefonnummer, der mod betaling kan hjælpe med at fjerne infektionen. På den måde kombineres den skadelige software med falsk telefonsupport, en velkendt svindeltype. Cryxos blev i snit fundet hos 171 ud af 10.000 brugere.

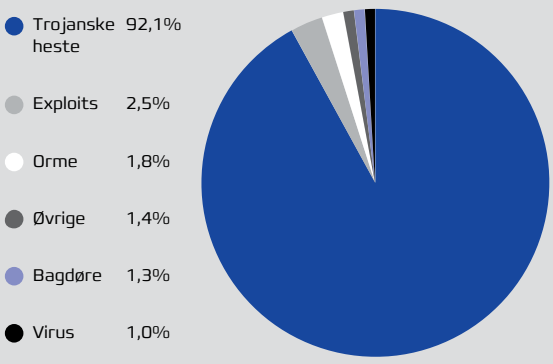
På andenpladsen lå Trojan:JS/Kavala. Det er en trojansk hest, der fx kan ankomme som en e-mail med en vedhæftet fil. Hvis man åbner filen, henter den et skadeligt program fra en server på nettet og installerer det.

På toptilisten finder vi også ransomwareprogrammerne Locky og Cryptolocker. Ny på listen er Trojan.BitCoinMiner, der udnytter den inficerede computer til at danne kryptovaluta af typen Bitcoin.

Nummer 10 på toptilisten er en gammel kending, som F-Secure kalder Downadup. Den er også kendt under navnet Conficker. Det er en orm, der først 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. Når den alligevel blev set på 12 ud af 10.000 danske computere i 2017, kan det være tegn på, at nogle computere ikke er opdateret i mange år.

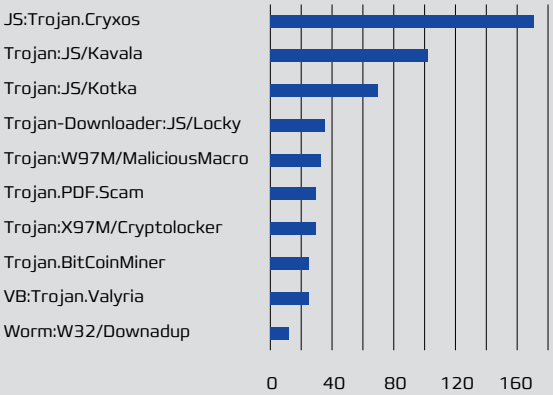
Figur 7: Skadelig software i Danmark

Fordelt på trusselstyper.



Figur 8: Topti over trusler

Topti over de hyppigst rapporterede former for skadelig software.



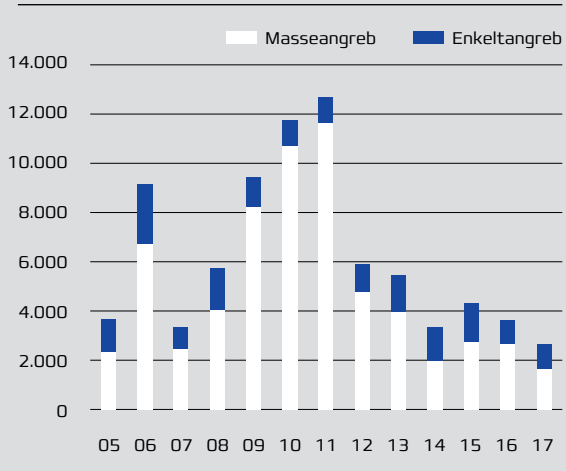
3.4. DEFACEMENTS

Den positive tendens inden for defacement-angreb fortsatte i 2017: Der blev registreret 27 procent færre angreb på danske domæner end i 2016 (se Figur 9). Ved et defacement-angreb placerer en hacker sine egne informationer på offerets websider.

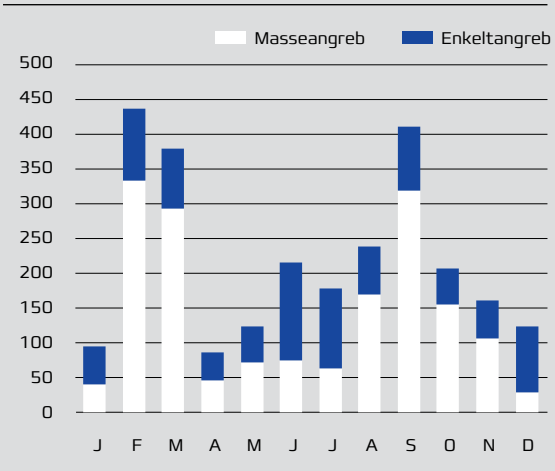
Ifølge statistikwebstedet Zone-H blev 2.626 dk-domæner overtaget ved defacement-angreb i 2017. 64 procent af angrebene var masseangreb, hvor flere domæner på den samme IP-adresse blev overtaget samtidig. Der var flest angreb i februar, marts og september (se Figur 10).

Zone-H bygger på frivillige indberetninger fra dem, der foretager angrebene. Derfor er tallene ikke nødvendigvis repræsentative, da faldet kan skyldes, at angriberne er holdt op med at oplyse om deres angreb.

Figur 9: Defacements på danske domæner 2005 - 2017



Figur 10: Defacements på danske domæner 2017



3.5. ÅRETS SÅRBARHEDER

I løbet af 2017 dukkede der flere sårbarheder og angrebsprogrammer op. En sårbarhed kan være en fejl i et program, der giver mulighed for at bryde sikkerheden. Et angrebsprogram udnytter en sårbarhed til at bryde sikkerheden.

USA's National Vulnerability Database registrerede 14.643 nye sårbarheder i 2017 (se Figur 11). Det er en stigning på 127 procent i forhold til året før. Stigningen kommer efter nogle år, hvor administratorerne af databasen har været kritiserede for ikke at registrere nye sårbarheder hurtigt nok.

15 procent af sårbarhederne fik den højeste risikovurdering, kritisk. Det vil sige, at de var udstyret med en CVSS-score (Common Vulnerability Scoring System) fra 9 til 10 (se Figur 12).

I det følgende gennemgår vi nogle af de sårbarheder, der blev kendt i 2017.

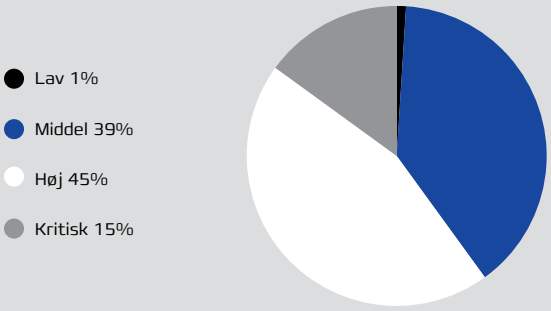
3.5.1. Cloudbleed

En lang række websteder kører bag tjenesten Cloudflare, der blandt andet beskytter mod DDoS-angreb. Tjenesten læser HTML-koden i websiderne og ændrer den, så links bliver omdirigeret.

I denne omskrivning af HTML opstod der i februar en fejl, så data fra arbejdslageret blev sendt med ud til browserne. Der skete lækage ved cirka en ud af 3,3 millioner HTTP-forespørgsler.

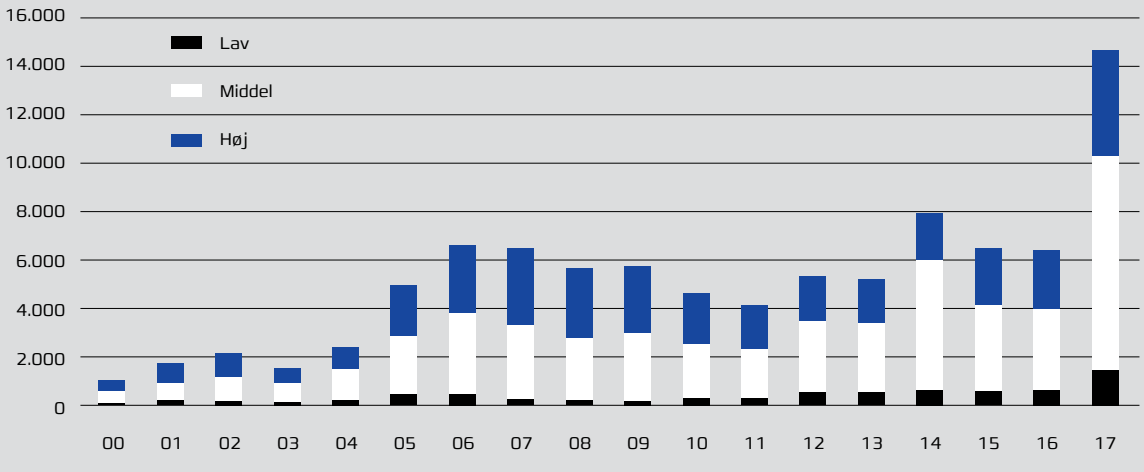
Fejlen, der fik navnet CloudBleed, medførte, at data kunne komme i uvedkommendes hænder[7].

Figur 12: Risikovurdering af sårbarheder fra National Vulnerability Database i 2017



[1] Cloudflare har lækket fortrolige data, DKCERT, 24-2-2017, https://www.cert.dk/da/news/2017-02-24_Cloudflare

Figur 11: Sårbarheder registreret i USA's National Vulnerability Database 2000-2017



3.5.2. Windows SMB – EternalBlue

EternalBlue er navnet på et angrebsprogram, der udnytter en sårbarhed i Windows' behandling af SMB-protokollen (Server Message Block). Angrebsprogrammet stammer sandsynligvis fra USA's NSA (National Security Agency). Det blev offentliggjort af hackergruppen Shadow Brokers, der antages at have tilknytning til Rusland.

Ransomwareprogrammet WannaCry var i maj blandt de første til at udnytte EternalBlue til at sprede sig[2]. Siden fulgte blandt andre ransomwareprogrammerne NotPetya og UIWIX, ormen EternalRocks og det skadelige program Adylkuzz, der danner digital valuta.

3.5.3. Apache Struts

I marts lukkede udviklerne af Apache Struts et alvorligt sikkerhedshul, der gav angribere mulighed for at afvikle programkode[3]. Struts er et udbredt system til udvikling af Java-baserede web-applikationer.

Sårbarheden blev udnyttet i et angreb på kreditoplysningsbureauet Equifax i USA, der blev opdaget i juli. Det gav hackere adgang til data om over 160 millioner forbrugere.

3.5.4. BlueBorne

BlueBorne er en samling sårbarheder i implementeringen af Bluetooth-standarden[4]. Android, Linux, iOS og Windows er alle berørt. Nogle af sårbarhederne giver en angriber mulighed for at afvikle skadelig programkode på enheden, få fat i fortrolige data eller udføre man-in-the-middle-angreb.

I alt indgår otte forskellige sårbarheder i BlueBorne. Fire af dem giver mulighed for at afvikle programkode.

Angribere skal være inden for Bluetooth-rækkevidde af den sårbare enhed for at kunne udnytte sårbarheden. Det vil oftest være omkring 10 meter. Desuden virker angrebene kun, hvis Bluetooth er aktivt på enheden.

3.5.5. KRACK (Key Reinstallation Attacks)

De fleste korrekte implementeringer af Wi-Fi-standarden WPA2 (Wi-Fi Protected Access) har sårbarheder i den måde, de håndterer den indledende kommunikation mellem to enheder. Sårbarhederne gør det muligt at gennemføre angrebet KRACK (Key Reinstallation Attacks)[5].

Den alvorligste sårbarhed findes på Linux- og Android-baserede enheder. Alle sårbarhederne kræver, at angriberen er inden for radiorækkevidde af det sårbare udstyr.

3.5.6. Intel Management Engine

I november udsendte Intel firmware-opdateringer, der lukkede alvorlige sikkerhedshuller i chipsæt i millioner af pc'er[6]. Det drejede sig om otte sårbarheder i Management Engine, Trusted Execution Engine og Server Platform Services. Det er teknologier, der indgår i Intels chipsæt til pc'er og servere.

Nogle af sårbarhederne kan kun udnyttes af en angriber med fysisk adgang til computeren. Da sårbarhederne findes i chipsæt, har de enkelte producenter af pc'er og servere ansvaret for at udsende opdateringer til deres kunder.

3.5.7. Oracle Jolt server

Oracle udsendte hovedparten af sine sikkerhedsopdateringer i de planlagte kvartalsvise Critical Patch Updates. I november brød firmaet med skemaet og udsendte ekstraordinære opdateringer til Jolt server, der indgår i produktet Tuxedo[7].

Rettelserne lukkede fem sikkerhedshuller, hvoraf det ene fik en CVSS-score (Common Vulnerability Scoring System) på de maksimale 10. Da Tuxedo indgår i programmet PeopleSoft, er brugere af denne applikation også berørt.

---

[2] Ransomware-ormen WanaCryptOr har ramt tusindvis af computere, DKCERT, 13-5-2017, https://www.cert.dk/da/news/2017-05-13/WanaCryptOr

[3] Angreb udnytter sårbarhed i Apache Struts, DKCERT, 10-3-2017, https://www.cert.dk/da/news/2017-03-10_Struts

[4] Sårbarheder i Bluetooth gør angreb mulige, DKCERT, 13-9-2017, https://www.cert.dk/da/news/2017-09-13/BlueBorne

[5] Kryptering af trådløse netværk har alvorligt sikkerhedshul, DKCERT, 16-10-2017, https://www.cert.dk/da/news/2017-10-16/KRACK

[6] R Intel lukker alvorlige huller i chipsæt, DKCERT, 23-11-2017, https://www.cert.dk/da/news/2017-11-23/Intel

[7] Oracle lukker alvorlige huller i Tuxedo, DKCERT, 22-11-2017, https://www.cert.dk/da/news/2017-11-22/Oracle

3.6. SÅRBARHEDSSCANNINGER

DKCERT tilbyder institutioner tilsluttet forskningsnettet gratis sårbarhedsscanninger. Scanningerne undersøger, om it-systemer har kendte sårbarheder, som angribere kan udnytte.

I 2017 scannede vi 204.638 IP-adresser. Det er mere end en halvering i forhold til 2016. Faldet skyldes, at vi kun foretog nogle få interne scanninger i 2017 – det vil sige scanninger inde bag institutionens firewall.

7.888 IP-adresser svarede på vores forsøg på scanning. Vi fandt sårbarheder på 3.504 af dem. Dermed steg andelen af sårbare systemer fra 28 procent i 2016 til 44 procent i 2017 (se Figur 13).

Vi fandt i alt 29.299 sårbarheder, det er næsten dobbelt så mange som i 2016 (se Figur 14).

En del af forklaringen på stigningen kan være, at nogle institutioner har øget frekvensen af scanninger: Hvor de før blev scannet to gange om året, scannes de nu hvert kvartal. Hvis institutionen samtidig er længe om at opdatere software, tæller den samme sårbarhed med i flere scanninger.

Fordelt på risiko var der færre med lav risikovurdering og flere med vurderingen middel. Sårbarheder med høj eller kritisk risiko var stort set uændrede: Fire procent høj og tre procent kritisk (se Figur 15).

I gennemsnit fandt vi 8,4 sårbarheder pr. sårbar IP-adresse. I 2016 var gennemsnittet 7,6. Den mest sårbare adresse havde 120 sårbarheder.

Der var 471 unikke sårbarheder i 2017, 76 procent flere end året før. En stor del af dem er sårbarheder i forbindelse med web-krypteringsteknologien SSL (Secure Sockets Layer). Således var den hyppigste sårbarhed relateret til, at algoritmen SHA-1 (Secure Hash Algorithm 1) blev trukket tilbage den 1. januar 2017. Hvis institutioner har digitale certifikater signeret med SHA-1, bliver de derfor regnet for sårbare.

Ingen af de 20 hyppigst forekommende sårbarheder i 2017 blev opdaget i 2017. To var fra 2016, mens de fleste var ældre (se Tabel 1). Blandt de mindre hyppige sårbarheder var der hovedsagelig to fra 2017: En i webserverprogrammet Apache og en i webprogrammeringssproget PHP. Scanningerne fandt ingen tilfælde af Apache Struts-sårbarheden fra marts måned på forskningsnettet.

DKCERT MENER

44 procent af de computere, DKCERT scannede i 2017, havde en eller flere sårbarheder. Det er en høj andel, der tyder på, at institutionerne bør oprioritere indsatsen med at holde systemerne opdateret med de seneste sikkerhedsrettelser.

Tabel 1: Top 20 over de hyppigst fundne sårbarheder ved DKCERTs scanninger i 2017

CVE-2004-2761
- SSL Certificate Signed Using Weak Hashing Algorithm
- SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

CVE-2016-2183
- OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32)
- OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET32)
- SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

CVE-2016-6329
- SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

CVE-1999-0524
- ICMP Timestamp Request Remote Date Disclosure

CVE-2011-3389
- SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

CVE-2013-2566
- SSL RC4 Cipher Suites Supported (Bar Mitzvah)

CVE-2015-2808
- SSL RC4 Cipher Suites Supported (Bar Mitzvah)

CVE-2004-2320
- HTTP Reverse Proxy Detection
- HTTP TRACE / TRACK Methods Allowed

CVE-2003-1567
- HTTP TRACE / TRACK Methods Allowed

CVE-2010-0386
- HTTP TRACE / TRACK Methods Allowed

CVE-2003-1418
- Apache Server ETag Header Information Disclosure

CVE-2008-5161
- SSH Server CBC Mode Ciphers Enabled

CVE-2015-4000
- SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
- SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

CVE-2014-3566
- Mac OS X < 10.10 Multiple Vulnerabilities (POODLE) (Shellshock)
- OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)
- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

CVE-2002-1700
- Web Server Generic XSS

CVE-2003-1543
- Web Server Generic XSS

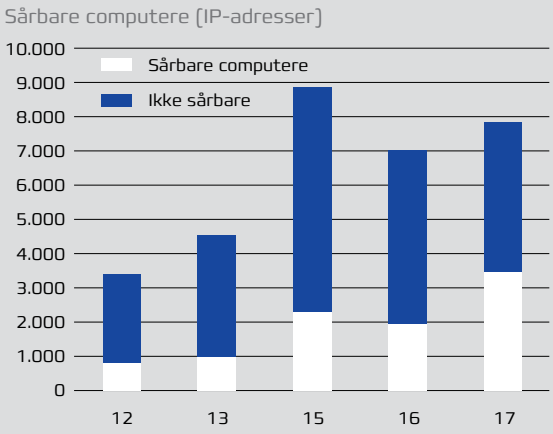
CVE-2002-1060
- Web Server Generic XSS

CVE-2012-3382
- Web Server Generic XSS

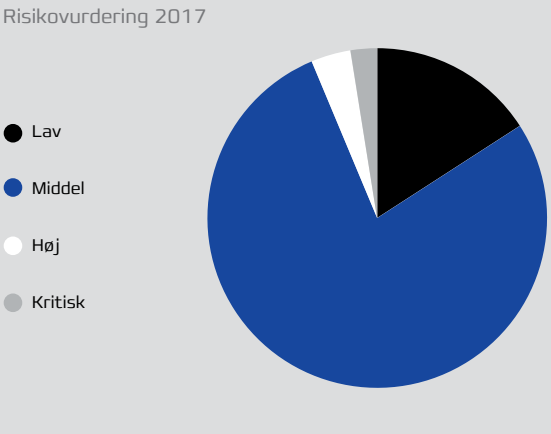
CVE-2005-2453
- Web Server Generic XSS

CVE-2006-1681
- Web Server Generic XSS

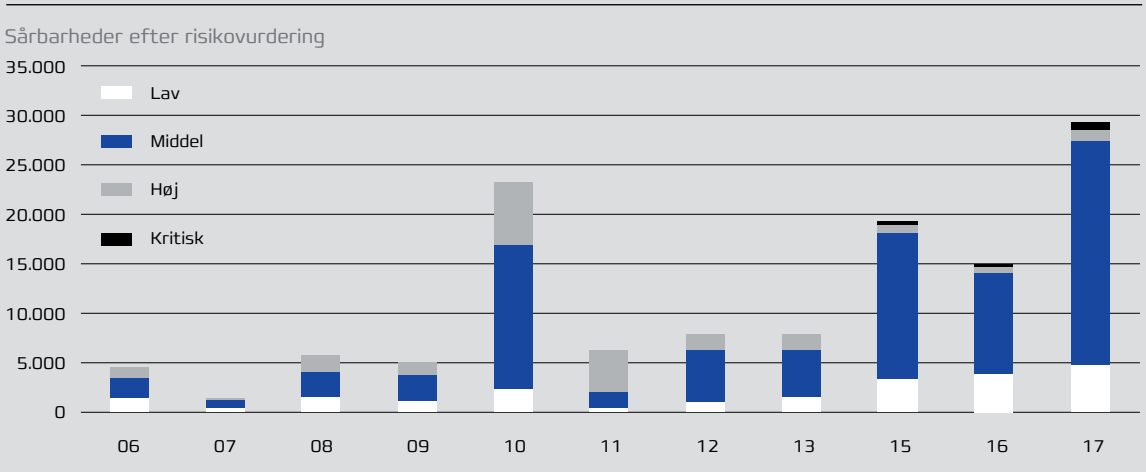
Figur 13: Flere af de scannede computere var sårbare. Der blev ikke scannet i 2014

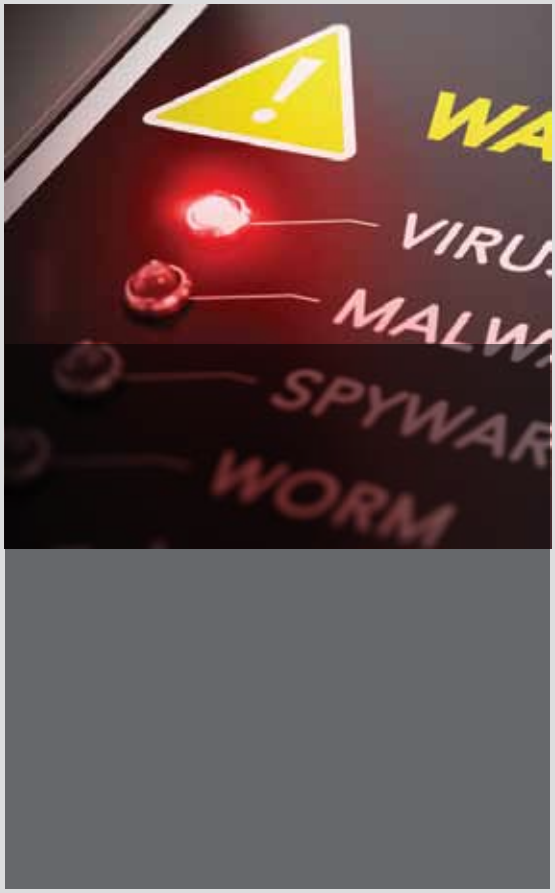


Figur 15: De fleste sårbarheder fik risikovurderingen middel



Figur 14: DKCERTs scanningstjeneste fandt næsten dobbelt så mange sårbarheder i 2017 som året før





3.7. ADVARSLER FRA TREDJEPARTER

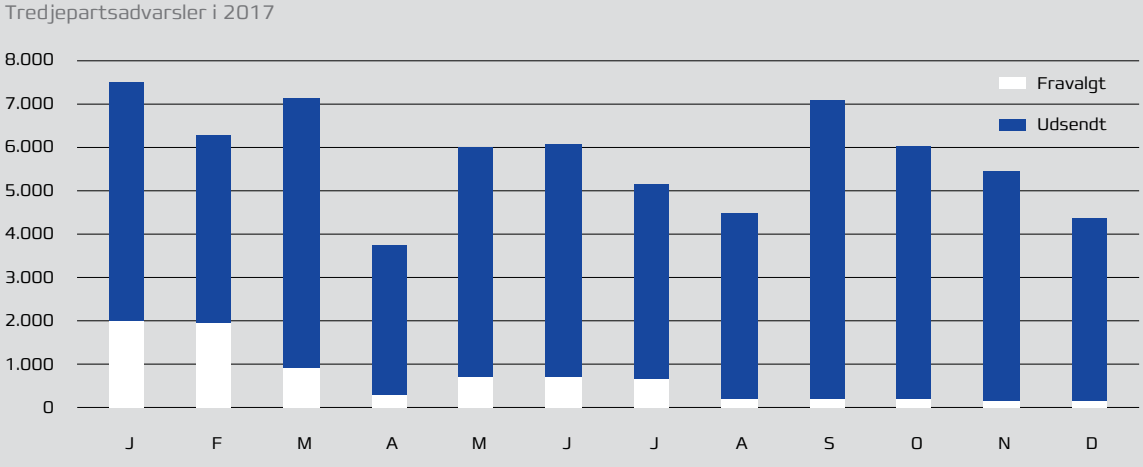
2017 udsendte DKCERT 61.249 advarsler fra tredjeparter. Denne service, som blev introduceret i slutningen af 2014, giver institutionerne på forskningsnettet advarsler om potentielt sårbare systemer på deres netværk. Advarslerne kommer fra tredjeparter, der løbende scanner internettet for kendte sårbarheder, 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. Tallene angiver altså ikke antallet af sårbare systemer hos institutionerne. De siger heller ikke noget om, hvorvidt angribere har forsøgt at udnytte sårbarhederne.

Tallene kan primært bruges til at give indtryk af, hvordan udbredelsen af de forskellige sårbarheder udvikler sig hen over året.

Institutionerne har 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. Til sammen blev 8.438 advarsler fravalgt i 2017. I alt registrerede DKCERT altså 69.687 advarsler (se Figur 16).

Figur 16: Advarsler fra tredjepart modtaget i 2017



3.7.1. POODLE-sårbarheden

Over en tredjedel af advarslerne handlede om sårbarheden POODLE (Padding Oracle On Downgraded Legacy Encryption) (se Figur 17). POODLE er en udbredt sårbarhed i behandlingen af SSL-kryptering (Secure Sockets Layer), der blev kendt i foråret 2014. I 2016 udgjorde advarsler om POODLE over halvdelen af alle advarsler, så udviklingen går mod færre sårbare systemer.

En stor del af advarslerne må formodes at handle om de samme systemer, som ikke bliver opdateret.

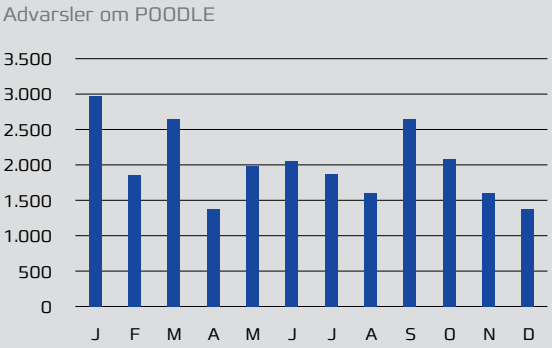
3.7.2. Åbne RDP-computere

Advarsler om åbne RDP-computere (Remote Desktop Protocol) tegnede sig for 15 procent af årets advarsler (se Figur 18). 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.

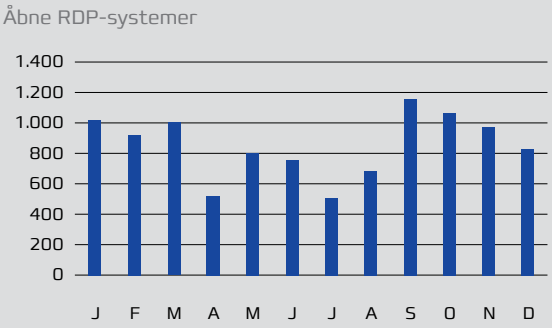
3.7.3. Åbne tidsservere

Nummer tre på listen over de hyppigst forekommende advarsler 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 af mange samtidige svar på forespørgsler, den ikke har afsendt (se Figur 19).

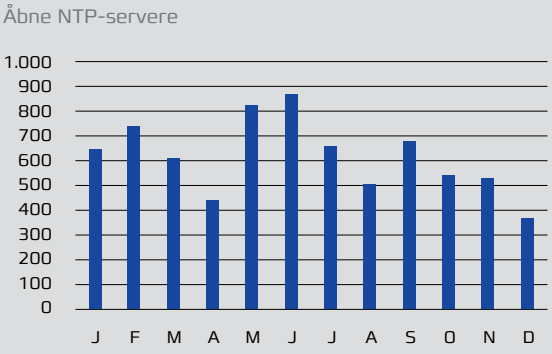
Figur 17: Advarsler fra tredjepart modtaget i 2017



Figur 18: Advarsler om RDP (Remote Desktop Protocol), der giver mulighed for fjernstyring



Figur 19: Advarsler om NTP-servere (Network Time Protocol)



4. 2017 – året i ord

DKCERT introducerede en tjeneste om databeskyttelsesforordningen i et år, hvor mange fortrolige data kom i de forkerte hænder.

DKCERT videreudviklede en tjeneste til dataanalyse og introducerede en ny tjeneste om EU's databeskyttelsesforordning i 2017. Behovet for bedre beskyttelse af persondata fremgik af en række sager internationalt om lækager af fortrolige data.

Henrik Larsen optrådte jævnligt som ekspertkilde i medierne i årets løb. Han skrev også månedlige klummer på Computerworld Online. Henrik Larsen blev i foråret genvalgt til bestyrelsen i Rådet for Digital Sikkerhed.

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 ugentlige nyhedsbreve og Twitter. Ved indgangen til 2017 abonnerede 1.348 personer på DKCERTs forskellige nyhedsbreve. Tallet steg til 1.451 ved årets udgang (se Figur 20).

I september blev nyhedsbrevet Sektornet lukket ned. En del af modtagerne flyttede over til et af de øvrige nyhedsbreve.

Twitter bliver en stadig mere populær kilde til information. I begyndelsen af året fulgte 1.575 personer @DKCERT på Twitter, det tal steg til 2.065 i slutningen af december. Dermed er mængden af følgere næsten fordoblet på to år.

4.1.2. DKCERT-CAB

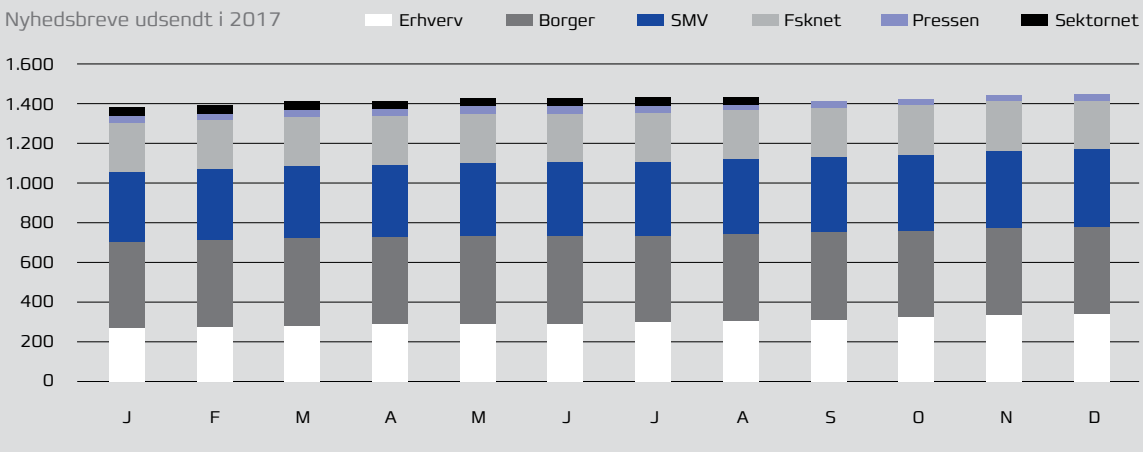
DKCERT-CAB (Change Advisory Board) er et rådgivende organ med repræsentanter for brugerne af DKCERTs tjenester. Gruppen mødtes fire gange i 2017.

4.1.3. Dataanalyse

Data om netværkstrafik fra forskningsnettet kan give ny viden om sikkerhedshændelser. Ud fra den tanke har DKCERT etableret en tjeneste, der kan analysere trafikdata fra routerne på nettet. Tjenesten bygger på teknologierne Elasticsearch og Apache Spark.

På grund af udfordringer i forbindelse med overgangen til nye routere på forskningsnettet har det ikke været muligt at sætte tjenesten i drift i 2017.

Figur 20: Abonnenter på DKCERTs nyhedsbreve. I september blev nyhedsbrevet Sektornet lukket ned.



4.1.4. Rådgivning om databeskyttelsesforordningen

Universiteter og andre institutioner på forskningsnettet skal som alle andre overholde EU's databeskyttelsesforordning. 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.

Tjenesten har oprettet et netværk for databeskyttelsesrådgivere og GDPR-projektdeltagere, hvor de kan udveksle erfaringer og information. Endvidere har flere institutioner anvendt projektlederen, Morten Eeg Ejrnæs Nielsen, som sparringspartner eller DPO.

4.1.5. Internationalt samarbejde

CERT'erne (Computer Emergency Response Team) for de nordiske forskningsnet holdt videomøder sammen med NORDUnet-CERT en gang om måneden. De mødtes også fysisk i forbindelse med NORDUnet Technical Workshop i Kastrup i september. På møderne diskuterede deltagerne aktuelle sikkerhedshændelser og erfaringer med værktøjer og metoder.

DKCERT har deltaget i flere møder i TF-CSIRT, der er en organisation for CERT'er under de europæiske forskningsnets paraplyorganisation GÉANT. Fire medarbejdere fra DKCERT deltog i en workshop om krisehåndtering arrangeret af GÉANT i Malaga i november.

Henrik Larsen deltog i årskonferencen og generalforsamlingen i FIRST (Forum of Incident Response and Security Teams), der fandt sted i juni i Puerto Rico.

Henrik Larsen deltager i GÉANTs SIG-ISM (Special Interest Group Information Security Management) og i styregruppen for den nordiske regionale gruppe under SIG-ISM.

Projektleder Morten Eeg Ejrnæs Nielsen var i august 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.

4.1.6. Kommende tjeneste: Phishing-test

DKCERT er i gang med at udvikle en tjeneste 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.

4.2. TENDENSER OG TRUSLER I 2017

4.2.1. Afpresning på flere måder

En tendens fortsatte uændret i 2017: It-kriminelle går i høj grad efter økonomisk gevinst. De senere år har det især været via afpresning.

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 2017 gjorde ransomware sig især bemærket ved to store angreb. WannaCry slog til i danskernes bededagsferie, men ramte ikke mange i Danmark. Derimod blev store dele af den britiske sundhedssektor ramt. Det skadelige program udnyttede den nyopdagede angrebsmetode EternalBlue, der anvender en sårbarhed i Windows til at sprede sig.

Det andet store angreb var NotPetya. Det ramte langt færre ofre, men var mere målrettet. NotPetya blev spredt ved, at et udbredt program til skatteindberetning i Ukraine, Me-Doc, blev inficeret. Via programmets automatiske opdateringsfunktion blev dets brugere inficeret i slutningen af juni. Blandt de tilfældige ofre var Mærsk, der anslog, at det kostede virksomheden næsten to milliarder kroner at rydde op efter angrebet.

Flere sikkerhedsfirmaer og den amerikanske efterretningstjeneste CIA mener, at angrebet reelt ikke havde til formål at afpresse penge. I stedet skulle formålet være at destabilisere økonomien i Ukraine. Det russiske militær skulle stå bag angrebet[8].

[8] Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes, Washington Post, 12-1-2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

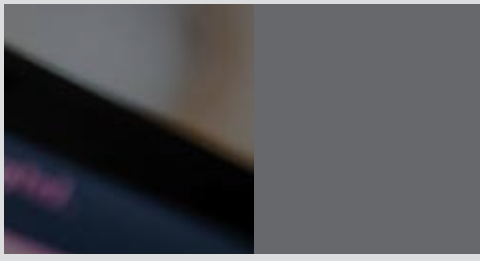
En anden form for afpresning går ud på, at de kriminelle truer med at udføre angreb mod offerets it-systemer. Et større overbelastningsangreb kan sætte systemer ud af drift, så kunder fx ikke kan købe ind i webshoppen. Den type angreb har vi også set i 2017.

En tredje form for afpresning har især ramt brugere af systemet MongoDB og lignende store databaser. Mange af dem er installeret på en måde, så enhver på internettet har fuld kontrol over dem. Det udnytter it-kriminelle til at kopiere alle data over på en anden server, slette dem fra offerets server og efterlade en besked om, at der skal indbetales en løsesum.

I nogle tilfælde lukker de kriminelle ikke for muligheden for, at alle kan administrere serveren. Andre kriminelle kommer senere ind på serveren og udskifter beskeden om løsesum med en ny, hvor pengene skal overføres til deres egen konto. Dermed har offeret ingen chance for at få sine data tilbage, da de nye afpressere ikke har adgang til dem.

DKCERT MENER

Udbredte ransomwareangreb understreger behovet for sikkerhedskopiering og netværkssegmentering. Med en sikkerhedskopi kan man gendanne data i tilfælde af ransomware-infektioner. Segmentering af netværk kan begrænse skaden, idet den skadelige programkode får sværere ved at sprede sig.



4.2.2. Sårbarheder får konsekvenser

I marts udsendte udviklerne af Apache Struts en opdatering, der lukkede et alvorligt sikkerhedshul. I juli opdagede det amerikanske kreditoplysningsbureau Equifax, at hackere siden midten af maj havde haft adgang til virksomhedens fortrolige data. Hackerne udnyttede sårbarheden i Apache Struts.

Data om over 160 millioner personer blev på den måde kompromitteret.

DKCERT MENER

Sagen fra Equifax 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.

4.2.3. Internet of Things blev ramt

Webkameraer, routere og meget andet udstyr på nettet, det såkaldte Internet of Things (IoT), kan misbruges. Det var botnettet Mirai, som vi beskrev i DKCERT Trendrapport 2017, et eksempel på. Et botnet er et netværk af enheder, som bagmænd kan fjernstyre. Enhederne kan bruges til forskellige former for it-kriminalitet såsom DDoS-angreb, udsendelse af spam og svindel med annonceklik.

I 2017 fandt myndighederne frem til de tre bagmænd bag Mirai-botnettet, og de tilstod.

Et nyt botnet baseret på Internet of Things-enheder var Reaper. Det udnytter en række kendte sårbarheder i forskelligt udstyr til at sprede sig.

DKCERT MENER

Internet of Things-enheder er blevet populære angrebsmål, fordi de er vanskelige at opdatere. Leverandørerne bør gøre det enkelt og brugervenligt at holde udstyret opdateret, så sikkerhedshuller bliver fundet og lukket.

4.2.4. Kryptovalutaer fik to roller

Kryptovalutaer som Bitcoin og Monero har i nogen tid været populære blandt it-kriminelle, fordi de tilbyder anonym betaling uden om bankerne. Derfor opkræves løsesummen fra ransomwareprogrammer ofte i den type valuta.

I 2017 var der også en række eksempler på en anden rolle for kryptovalutaerne inden for it-kriminalitet: Skadelige programmer begyndte at installere moduler, der danner valuta for bagmændene.

Pengene i en kryptovaluta dannes som regel ved såkaldt mining. Det går ud på, at et program foretager en række beregninger. Nogle websider blev inficeret med mining-funktioner, der udnyttede de besøgendes browsere til at danne kryptovaluta.

Mindst fire danske universiteter blev sidst på året ramt af skadelig software med mining-funktionalitet. Det skete ved, at angribere udnyttede en kendt sårbarhed i Oracle Weblogic til at få adgang og installere softwaren.

4.2.5. Phishing – en udbredt trussel

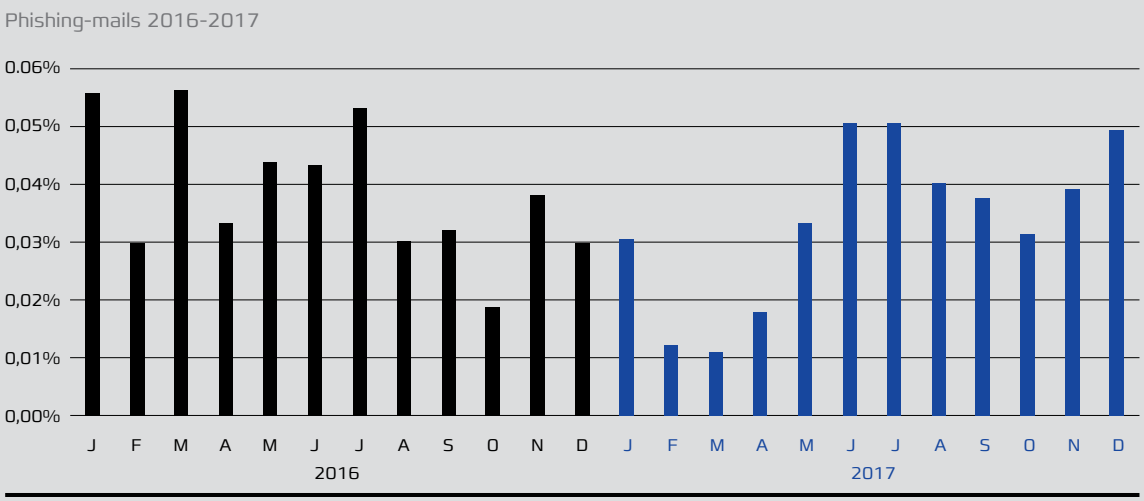
Igen i år var phishing udbredt. Det er vores fornemmelse, men vi har ikke danske tal at bygge det på. Det skyldes, at universiteterne og de øvrige institutioner på forskningsnettet oftest behandler den type sager lokalt.

På internationalt plan var der en stor mængde phishing i begyndelsen af 2016. Den faldt fra august 2016, men begyndte igen at stige i april 2017. Ifølge tal fra sikkerhedsfirmaet Symantec var omkring 0,05 procent af alle mails forsøg på phishing i juni og juli og igen i december (se Figur 21).

DKCERT MENER

Der mangler et samlet overblik over e-mails med phishing-svindel og skadelig software, som danskerne modtager. Et skridt på vejen kan være, at institutionerne på forskningsnettet indrapporterer den type sikkerhedshændelser til DKCERT.

Figur 21: Phishing-mails som andel af den samlede mail-mængde. Kilde: Symantec



4.2.6. Et år med store datalækager

I løbet af første halvår af 2017 kom flere data i forkerte hænder end i hele 2016. Ifølge en analyse fra firmaet Gemalto optrådte over 1,9 milliarder dataposter i lækager og andre brud på datasikkerheden. Firmaet registrerede 918 sikkerhedshændelser, hvor uvedkommende fik adgang til fortrolige data[9].

Blandt årets større hændelser var følgende[10]:

- Dun & Bradstreet, marts, data om 33,7 millioner personer.
- Deep Root Analytics, juni, data om 198 millioner vælgere fra USA.
- Verizon Communications, juli, data om 14 millioner brugere.
- Transportstyrelsen, Sverige, juli, database med alle svenske kørekortfotos og andre transportdata var tilgængelig for tjekkiske it-medarbejdere uden sikkerhedsgodkendelse[11].
- Storbritanniens National Health Service, august, data om 1,2 millioner patienter.
- Equifax, september, data om 145,5 millioner amerikanere og 15,2 millioner briter.
- Yahoo, oktober (angrebet fandt sted i 2013), data om tre milliarder brugere.
- Uber, november, data om 57 millioner brugeres mail-adresser og kørekort.

Datasikkerheden blev kompromitteret på flere måder. I nogle tilfælde sløser virksomhederne med sikkerheden. Det gjaldt fx i sagen fra juni om amerikanske vælgeres oplysninger. Analysefirmaet Deep Root Analytics, der udførte en opgave for det republikanske parti, lagde dataene ud på en offentligt tilgængelig server.

Andre gange har virksomhederne ikke opdateret software, så hackere kan udnytte sårbarheder. Det gjaldt blandt andet for Equifax, der blev ramt via en sårbarhed i Apache Struts.

[9] 2017: Poor Internal Security Practices Take a Toll, Gemalto, http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

[10] Year in Review: Notable Data Breaches for 2017, Trend Micro, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017

[11] Alla svenska körkortsfoton läckte till Tjeckien, SVT, https://www.svt.se/nyheter/inrikes/alla-svenska-korkortsfoton-lackte-till-tjeckien

5. Det eksterne perspektiv

Fire bidragydere uden for DKCERT og en intern giver her deres syn på arbejdet med at leve op til databeskyttelsesforordningens krav.

Når EU's databeskyttelsesforordning bliver håndhævet fra den 25. maj, får det betydning for alle organisationer, der behandler persondata. Derfor har DKCERT bedt en række interessenter skrive om konsekvenserne for dem.

Jesper Husmer Vang fra Datatilsynet fortæller, hvad forordningen betyder for forholdet mellem organisationer og tilsynet.

Henning Mortensen fra Rådet for Digital Sikkerhed gennemgår, hvordan man sikrer databeskyttelse allerede ved designet af it-løsninger.

Databeskyttelsesrådgiver Lisa Ibenfeldt Schultz forklarer, hvordan Københavns Universitet indfører regler og procedurer – og sikrer sig, at brugerne kan finde og forstå dem.

Professor Kathrin Otrel-Cass fra Aalborg Universitet beskriver de problemer med beskyttelse af persondata, forskning med videooptagelser medfører.

Endelig fortæller Morten Eeg Ejrnæs Nielsen fra DKCERT/DeiCs DPO-tjeneste om de erfaringer, han har gjort gennem kontakten med universiteter og andre brugere af tjenesten.

5.1. DATATILSYNETS ROLLE UNDER DATABESKYTTELSESFORORDNINGEN

AF KONTORCHEF JESPER HUSMER VANG, DATATILSYNET

Databeskyttelsesforordningen ændrer på flere områder forholdet mellem Datatilsynet og organisationer, der behandler persondata.

En vigtig forskel er, at de nugældende regler om anmeldelse i vidt omfang bliver afløst af et krav om, at alle offentlige og visse private organisationer skal have en databeskyttelsesrådgiver (DPO, Data Protection Officer). Vi forventer, at det vil være en fordel for både os i Datatilsynet og for organisationerne selv, at der fremover vil være en person, der både kender sin organisation og reglerne for behandling af persondata. Det vil utvivlsomt lette dialogen.

En anden ændring er, at der med forordningen indføres en pligt for organisationerne til – inden 72 timer – at indberette eventuelle brud på persondatasikkerheden til Datatilsynet. Denne nye indberetningspligt vil medføre en ny form for dialog mellem os og organisationerne, selvom der er flere organisationer, der allerede har taget forskud på glæderne og er begyndt at indberette brud på persondatasikkerheden. Vi forventer i den forbindelse – i samarbejde med Erhvervsstyrelsen – at have en indberetningsløsning klar på virk.dk, når vi rammer den 25. maj.

Databeskyttelsesforordningen giver os også en række nye kompetencer i forhold til vores tilsynsvirksomhed, der også vil komme til at berøre organisationerne.

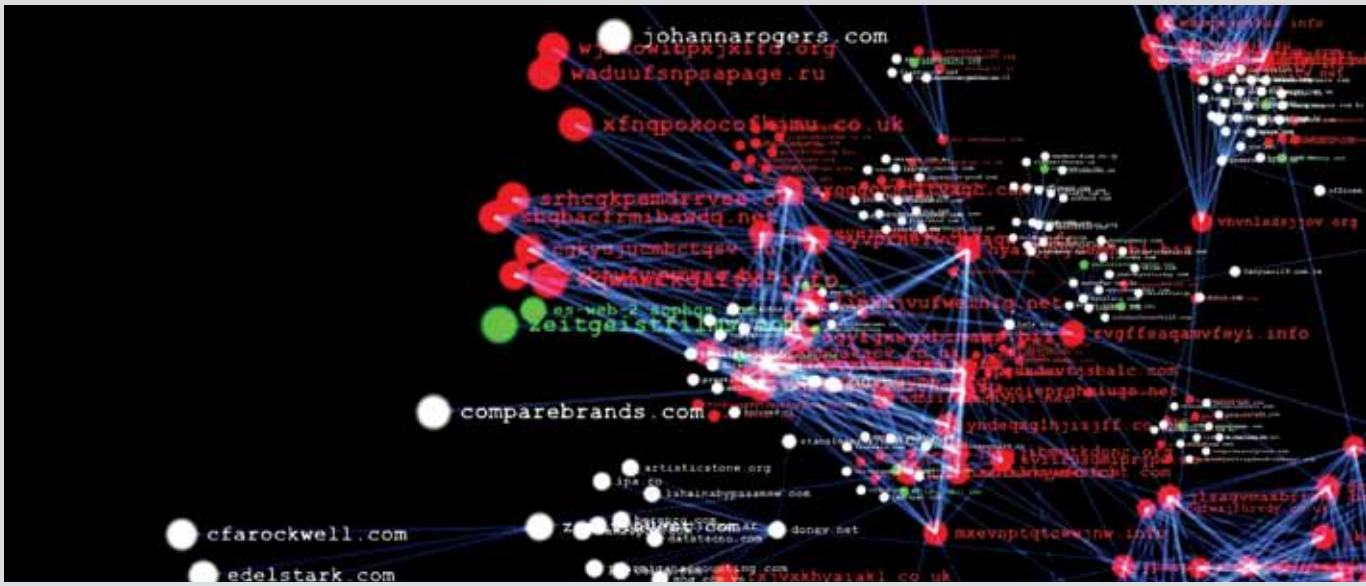
Vi vil blandt andet fremover selv kunne udstede bødeforlæg i visse mindre komplicerede sager. Det vil næppe være mange sager i begyndelsen, da der først skal etableres en retspraksis på området.

Ud over bødeforlæg vil vi også få udvidet vores beføjelser til at meddele påbud og forbud, idet vi fremover også vil kunne meddele offentlige myndigheder sådanne. Hvis vi f.eks. flere gange ser, at et universitet ved en fejl kommer til at offentliggøre fortrolige data om studerende på deres intranet, kan vi blandt andet meddele universitetet et påbud om at lukke for adgangen til deres intranet, indtil de får styr på persondatasikkerheden.

For så vidt angår private virksomheder, bliver vores tilsynskompetencer ligeledes udvidet, idet vi som noget nyt vil kunne foretage fysiske tilsyn hos alle private virksomheder og ikke kun de virksomheder, der har modtaget en tilladelse fra os.

5.1.1. Husk at fastsætte slettefrister

Vi kan se, at især mange private virksomheder har nogle udfordringer i forhold til at huske at slette persondata, når det ikke længere er nødvendigt for virksomheden at behandle data. Vi hører sågar



nogle virksomheder omtale forordningens artikel 5, stk. 1, 1, litra e om sletning som en ny regel. Men faktisk har der været krav om sletning, siden vi fik registerlovene tilbage i 1979. Kravet er således ikke nyt, men virksomheder skal blive bedre til at huske at efterleve kravet.

I forhold til sletteproblematikken vil organisationerne kunne hjælpe sig selv ved at få fastlagt, hvilke kategorier af behandlinger de foretager og derefter fastsætte slettefrister inden for de enkelte kategorier. Eksempler på kategorier kunne bl.a. være 1) oplysninger om ansatte, 2) oplysninger om stillingsansøgere og 3) oplysninger der benyttes til sagsbehandling mv.

5.1.2. Persondatasikkerhed skal bygge på risikovurderinger – også hos offentlige myndigheder

Hidtil har offentlige myndigheder skullet være opmærksomme på at overholde sikkerhedsbekendtgørelsen. Sikkerhedsbekendtgørelsen bortfalder imidlertid med forordningen, hvorfor offentlige myndigheder fremover vil skulle fastlægge deres sikkerhedstiltag baseret på en risikovurdering i forhold til de enkelte behandlinger.

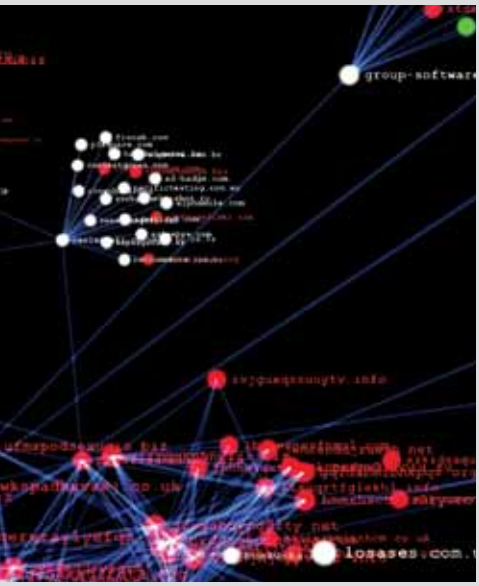
Myndighederne vil naturligvis godt kunne finde inspiration i den gældende sikkerhedsbekendtgørelse, herunder f.eks. i forhold til autorisation af medarbejdere og logning, men der vil som sagt skulle laves risikovurderinger. En risikovurdering vil kunne munde ud i, at myndigheden måske kan slække på kravene i den nugældende sikkerhedsbekendtgørelse, eller at myndigheden omvendt skal indføre yderligere sikkerhedsforanstaltninger.

5.1.3. Få styr på databehandleraftaler

Vores tilsynsbesøg har i den seneste tid vist, at en del myndigheder og virksomheder ikke er tilstrækkeligt opmærksomme på at få indgået de fornødne databehandleraftaler med deres databehandlere. Vi har også konstateret store udfordringer hos myndigheder og virksomheder i forhold til at få påset persondatasikkerheden hos deres databehandlere.

Fra Datatilsynets side skal der således lyde en stor opfordring til, at offentlige myndigheder og private virksomheder benytter den kommende tid til at undersøge, om de har de fornødne databehandleraftaler på plads med alle deres databehandlere. De bør ligeledes sikre sig, at de har procedurer for, hvordan de påser, at persondatasikkerheden hos databehandlerne er tilstrækkelig.

Datatilsynet forventer i øvrigt inden for kort tid at offentliggøre et bud på en skabelon til en databehandleraftale, ligesom tilsynet senere vil komme med en vejledning om, hvordan man kan påse persondatasikkerheden hos sine databehandlere.



5.2. DATABESKYTTELSE GENNEM DESIGN

AF HENNING MORTENSEN,
FORMAND FOR RÅDET FOR DIGITAL SIKKERHED

Databeskyttelse gennem design er et nyt selvstændigt begreb, som introduceres i dansk ret med persondataforordningens artikel 25. Under en række forudsætninger skal der gennemføres passende tekniske og organisatoriske foranstaltninger, således at de garantier for de registrerede som forordningen giver, understøttes i de it-systemer, som behandler personoplysninger.

5.2.1. Potentialet

Det betyder med andre ord, at fremtidige løsninger, som behandler personoplysninger, skal designes på en sådan måde, at personoplysningerne og de registrerede beskyttes i selve løsningen og ikke kun af alle mulige andre tiltag rundt om løsningen.

Når man designer næste generation digital signatur, elektroniske patientjournaler eller andre store elektroniske infrastrukturkomponenter, der behandler personoplysninger, skal udviklerne dermed allerede under designet af løsningen fastlægge, hvordan systemet kan understøtte garantierne i forordningen.

Kravet om design får dermed indflydelse på, hvordan løsningen udformes: Der kan ikke alene tænkes i funktionalitet. Der skal tænkes i funktionalitet, som understøtter garantierne. Funktionalitet, der er i konflikt med garantierne, kan dermed ikke etableres.

Det nye krav i artikel 25 kommer dermed til at rykke databeskyttelsen op som en af de vigtigste parametre, når nye it-løsninger skal designes. Det vil bidrage til, at vi får mere sikre og mindre invasive løsninger i fremtiden.

5.2.2. Hvad betyder databeskyttelse gennem design?

Forordningen siger desværre meget lidt om, hvad der så konkret ligger i begrebet. I artikel 25 gives kun eksempler i form af pseudonymisering og dataminimering.

Begrebet stammer fra Ann Cavoukian, som i 90'erne var direktør for datatilsynet i den canadiske delstat Ontario og internationalt har været en utrættelig forkæmper for beskyttelse af personoplysninger. Cavoukian udkrystalliserede syv principper, som hun mente burde guide designet af alle it-systemer, der skal behandle personoplysninger.

Heraf fremgår det f.eks. at foranstaltningerne skal indlejres, iværksættes inden en risiko materialiserer sig, være i drift i hele systemets livscyklus. Endvidere skal der være fuld funktionalitet, og der må således ikke gives køb på garantierne for at opnå en bestemt funktionalitet. Brugerne kommer også meget i centrum i løsningerne i og med, at de ikke selv er pligtige til at skulle slå foranstaltninger til. Der skal sikres let gennemsigtighed i den behandling, som foretages. Brugercentrisk design skal sikre, at brugerne kan komme i kontrol med deres personoplysninger.

Cavokians designprincipper er ikke den eneste kilde til forståelse af begrebet. For en mere uddybende gennemgang kan der henvises til artiklen "Databeskyttelse gennem design" i Revision og Regnskabsvæsen[12].

5.2.3. Sammenhæng med andre artikler i forordningen

Der er en god sammenhæng mellem artiklerne i persondataforordningen. Man kan sige, at artikel 24 er overliggeren, hvor den dataansvarlige pålægges at implementere passende tekniske og organisatoriske foranstaltninger til at understøtte forordningen i en bred forstand.

Efter artikel 35 skal der i en række sammenhænge laves konsekvensanalyser, hvor risiciene af behandlinger set fra den registreredes synspunkt kortlægges. Den identificerede risiko skal så mitigeres (begrænses) i passende omfang gennem designet af løsningen, som er genstand for denne artikel og forordningens artikel 25, og gennem mere klassiske sikkerhedsmæssige foranstaltninger som omtalt i forordningens artikel 32.

[12] Databeskyttelse gennem design" i Revision og Regnskabsvæsen, https://www.karnovgroup.dk/artikler/rr-12-2017-databeskyttelse

Dermed får man som dataansvarlig altså en operationel tre-trins-raket:

1. Kortlæg risici fra de registrerede.
2. Vælg et passende design, der understøtter hele forordningen.
3. Implementer desuden de rette sikkerhedstiltag.

5.2.4. Eksempler

Rådet for Digital Sikkerhed har udgivet en samling praktiske eksempler på databeskyttelse gennem design[13]:

- Man kan undlade at identificere de registrerede i de behandlingssituationer, hvor det ikke er strengt nødvendigt.
- Man kan sætte udløbsdatoer på personoplysninger, allerede når de skabes.
- Man kan implementere klassifikation af data, når de skabes.
- Man kan hindre, at data utilsigtet forlader et givent system.
- Man kan lave indsigtsknapper, så det bliver let gennemskueligt, hvilke personoplysninger der behandles til hvilke formål.

Ann Cavoukians designprincipper

1. **Proaktiv, ikke reaktiv**
   Foranstaltninger skal iværksættes, inden en risiko materialiserer sig.
2. **Privacy som standardindstilling**
   Den registrerede skal ikke selv foretage sig noget for at beskytte sine oplysninger; beskyttelsen skal være slået til fra starten.
3. **Privacy skal være indlejret i systemet**
   Foranstaltningerne skal designes ind i et systems arkitektur og ikke tilføjes efterfølgende.
4. **Der skal være fuld funktionalitet**
   Der må ikke være modstrid mellem sikkerhed og databeskyttelse.
5. **Beskyttelse i hele livscyklussen**
   Beskyttelsen skal indbygges i designfasen, inden systemet sættes i drift, og være aktiv i hele systemets levetid.
6. **Transparens**
   Der skal være gennemsigtighed i forretningsmodeller og teknologier. Det der signaleres, skal kunne verificeres (af en uafhængig tredjepart).
7. **Brugeren i centrum**
   De registreredes interesser skal være i fokus f.eks. gennem standardindstillinger, notifikation og empowerment af brugerne, så de er i kontrol.

[13] Rådet for Digital Sikkerhed: Vejledning om Databeskyttelse gennem Design, https://www.digitalsikkerhed.dk/nyheder/2017/11/22/rdet-for-digital-sikkerhed-vejledning-om-databeskyttelsen-gennem-design

5.3. KØBENHAVNS UNIVERSITETS TILPASNING TIL PERSONDATAFORORDNINGEN

AF LISA IBENFELDT SCHULTZ,
DATABESKYTTELSESRÅDGIVER, KØBENHAVNS UNIVERSITET

Københavns Universitet er med sine knap 10.000 ansatte og 40.000 studerende en stor organisation med mange forskelligartede opgaver inden for forskning og undervisning. Universitetets størrelse har haft betydning for valget af metode til at sikre, at de nye bestemmelser i persondataforordningen bliver fulgt på alle institutter, centre og fakulteter, samt i forhold til universitetets fælles systemer.

Der er valgt nogle principper for universitetets aktiviteter:

- Ansvaret for overholdelse af persondataforordningen følger ansvaret for løsning af den opgave, som databehandlingen indgår i.
- Tilpasningerne skal integreres i eksisterende processer og systemer.
- Det skal være let at følge reglerne, således at de rigtige løsninger bliver medarbejderens naturlige valg.

De valgte principper for universitetets aktiviteter har ført til, at der er iværksat og helt eller delvist gennemført en række konkrete aktiviteter:

5.3.1. Tilgængelige regler og retningslinjer

Regler og retningslinjer er beskrevet på universitetets intranet: Et site er målrettet administrative medarbejdere, et andet site er målrettet forskere, som håndterer forskningsdata enten fra forsøgspersoner eller i form af registerforskning.

Siderne på intranettet beskriver reglerne i persondataforordningen og "oversætter" reglerne til en kontekst, som universitetets medarbejdere møder i hverdagen. Der er udarbejdet standardbreve og tekster, som sikrer, at afgørelser om fx afslag på indsigt er formuleret juridisk korrekt. Der findes også nye skabeloner for databehandleraftaler, og universitetet er i gang med at genforhandle aftaler med eksisterende leverandører og samarbejdspartnere, som håndterer universitetets persondata.

Herudover udarbejdes retningslinjer for håndtering af data om forsøgspersoner på den del af universitetets intranet, som er målrettet studerende. I forbindelse med projekter og specialer har flere studerende behov for at håndtere oplysninger om forsøgspersoner.

Alle sites findes på dansk og på engelsk.

5.3.2. Workzone til fortegnelser og indberetning af sikkerhedshændelser

Persondataforordningen kræver, at universitetet som dataansvarlig fører fortegnelser over behandlingen af data. Fortegnelserne erstatter de eksisterende anmeldelser til Datatilsynet.

Københavns Universitet har valgt at udarbejde online formularer til registrering af oplysninger om databehandling til brug for fortegnelserne og ligeledes til indberetning af informationssikkerhedshændelser. Formularerne integreres med Workzone, som er universitetets sags- og dokumenthåndteringssystem.

Når en medarbejder udfylder en online formular, vil fortegnelsen eller indberetningen automatisk blive journaliseret. Dette system giver sikkerhed for, at oplysningerne bliver journaliserede. Endvidere giver det databeskyttelsesrådgiveren adgang til de enkelte indberetninger og til at udtrække statistikker. Fortegnelser for persondata i forskningsprojekter vil følge samme metode. Workzone vil blive udnyttet til at sikre opmærksomhed på krav om sletning eller anonymisering, når forskningsprojektet afsluttes. Indberetninger og fortegnelser vil kunne udleveres til Datatilsynet.

5.3.3. Harmonisering af dataopbevaring

Københavns Universitet har den 1. december 2017 samlet universitetets decentrale it-afdelinger under en fælles ledelse. Det giver basis for at harmonisere universitetets eksisterende it-løsninger, herunder løsninger til sikker og lovlig behandling af persondata.

Selv om den gældende sikkerhedsbekendtgørelse bliver ophævet sammen med persondataloven, vil universitetet – efter råd fra Datatilsynet – fortsat arbejde på, at persondata håndteres i overensstemmelse med bekendtgørelsens regler om fx autorisationer og logning.

Universitetets generelle fokus på informationssikkerhed har betydet, at universitetet har etableret en informationssikkerhedsenhed med 3-4 årsværk, herunder informationssikkerhedschefen og databeskyttelsesrådgiveren.

5.3.4. Den menneskelige faktor

I løbet af foråret vil der blive iværksat forskellige aktiviteter med henblik på at styrke bevidstheden om reglerne hos universitetets ansatte og studerende.

Det omfatter fx e-læringskurser til forskere (måske fælles for flere danske universiteter), en temadag for tillidsrepræsentanter, netværk for administrative medarbejdere, nyheder på intranettet, oplæg for administrative ledelser og generelle kampagner målrettet henholdsvis studerende og ansatte.

5.4. ER BESKYTTELSE AF PRIVATE DATA MULIG I VIDEODATA?

AF KATHRIN OTREL-CASS,
PROFESSOR MSO I VISUEL FORSKNING VED AALBORG UNIVERSITET

Jeg leder et video lab og et pilotprojekt om Video Data Management, der skal undersøge og udvikle en infrastruktur, der understøtter forskning i video. I forskning kan videodata kvalificeres som "big data", idet de gør det muligt for forskere at få overblik over en myriade af detaljer, der ikke kan opnås på anden vis.

Video afslører samtidig identiteten på de optagede deltagere. Det skaber en fundamental konflikt mellem udnyttelse af de omfangsrige data og beskyttelse af personlige data.

For at forstå deltagernes interaktioner og opførsel skal videodata være tilgængelige for forskere, alt imens deltagernes personlige data skal være beskyttet.

Forestil dig følgende scenarier:

1. Forskere præsenterer optagede observationer med billeder eller videoklip til konferencer, hvor andre forskere blandt publikum optager dele eller hele præsentationen på deres egne telefoner. Forskerne kan have fået samtykkeerklæringer fra deltagerne i de aktuelle forskningsprojekter til at indsamle visuelle data til forskning, men kan ikke garantere sikker opbevaring eller beskyttelse af de personlige data, specielt med tanke på den hastige udvikling inden for ansigtsgenkendelses-software.
2. Forskere kan udgive artikler med uddrag fra video i akademiske journaler, eksempelvis Video Journal of Education and Pedagogy, hvor en artikel kan suppleres med videoklip på op til 15 minutter. I andre tilfælde kan uddrag af video gøres tilgængelig på en webbaseret platform. Når en anden forsker downloader artiklen, kan forfatteren ikke længere garantere sikker opbevaring på de præmisser, der indgik i samtykkeerklæringen mellem forsker og deltagere.
3. Nogle forskningsprojekter kan inkludere forskere fra forskellige institutioner. I forlængelse heraf kan der sættes spørgsmålstegn ved, hvorvidt der eksisterer fælles protokoller for deling og opbevaring af ubehandlede og behandlede data med vedhæftede analyser som eksempelvis transskriberinger.

Redigeringssoftware kan anonymisere ansigtstræk. Men netop analyse af ansigtsudtryk er mange forskere, der arbejder med video, interesseret i.

5.4.1. Vi mangler retningslinjer

Nuværende retningslinjer, der er tilgængelige for videoforskere, adresserer ikke, hvordan den hastigt udviklende kommunikation og deling af information skal imødekommes.

Det er derfor nødvendigt, at forskningsfællesskabet

1. Udvikler fælles terminologi
2. Kommunikerer relevansen og den foranderlige praksis inden for videoforskning mere effektivt
3. Udvikler modeller og retningslinjer for deling af data og
4. Uddanner forskere og universiteter i problematikker vedrørende private data.

Det er desuden nødvendigt at oprette en sikker struktur til opbevaring og deling af følsomme videodata.

.

5.5. GDPR-PROJEKTER SAVNER RESSOURCER

AF PROJEKTLEDER MORTEN EEG EJRNÆS NIELSEN, DKCERT/DEICS DPO-TJENESTE

Næsten alle implementeringsprojekter i uddannelsessektoren oplever, at opgavens omfang langt overstiger de ressourcer, som er til rådighed. De fleste steder mangler også medarbejdere med kompetencer inden for området.

Det fremgår af de tilbagemeldinger, DKCERT har fået fra sektoren. Det gælder dels et netværk for de folk, der arbejder med at implementere databeskyttelses¬forordningen på universiteter og andre uddannelsesinstitutioner, dels de institutioner vi har rådgivet direkte.

For at hjælpe uddannelsesinstitutionerne med at imødegå udfordringerne med implementeringen af de nye regler oprettede DeiC i august 2017 en DPO-tjeneste i DKCERT. En DPO er en Data Protection Officer eller en databeskyttelsesrådgiver.

Formålet med tjenesten var først og fremmest at etablere et netværk mellem de folk, der arbejder med implementeringen af forordningen på universiteterne, således at der kunne skabes en fælles forståelse og vidensdeling mellem dem.

Netværket havde første møde i oktober 2017 og det andet møde i december 2017.

Det har været positivt at se, at mange uddannelsesinstitutioner har opbakning fra direktøren eller andre dele af det øverste ledelseslag til arbejdet med implementeringen. Det viser, at der er bevidsthed om opgaven, og at ledelsen på de danske uddannelsesinstitutioner tager opgaven alvorligt.

5.5.1. Gode muligheder for erfaringsudveksling

De mange implementeringsprojekter er typisk organiseret meget forskelligt alt afhængig af, hvor i organisationen arbejdet med forordningen er startet. Dog er der gode muligheder for erfaringsudveksling, da der er en lang række skabeloner og dokumenter, som alle institutioner skal udarbejde.

Til begge møder har der været et stort fremmøde fra uddannelsesinstitutionerne. Der har været megen drøftelse af de konkrete problemstillinger, som institutionerne står over for i deres arbejde med implementeringen af de nye regler.

Netværket har også haft eksterne til at holde oplæg, der blandt andet har fortalt om, hvordan de så mulighederne for at bruge e-læring til at skabe awarenes, om kravene til databehandleraftaler og endelig har Datatilsynet også beredvilligt stillet op til mere end en times Q&A.

5.5.2. Rådgivning

Yderligere forsøger DPO-tjenesten at hjælpe de interesserede uddannelsesorganisationer med forskellige problemstillinger, hvor de har brug for det.

Det første halve år med DPO-tjenesten har resulteret i en lang række møder med især universiteter og university colleges rundt omkring i hele landet. Møderne har givet indsigt i de forskellige måder, hvorpå uddannelsesinstitutionerne tilgår opgaven, og hvordan de organiserer sig i forhold til implementeringen.

5.5.3. Internationalt samarbejde

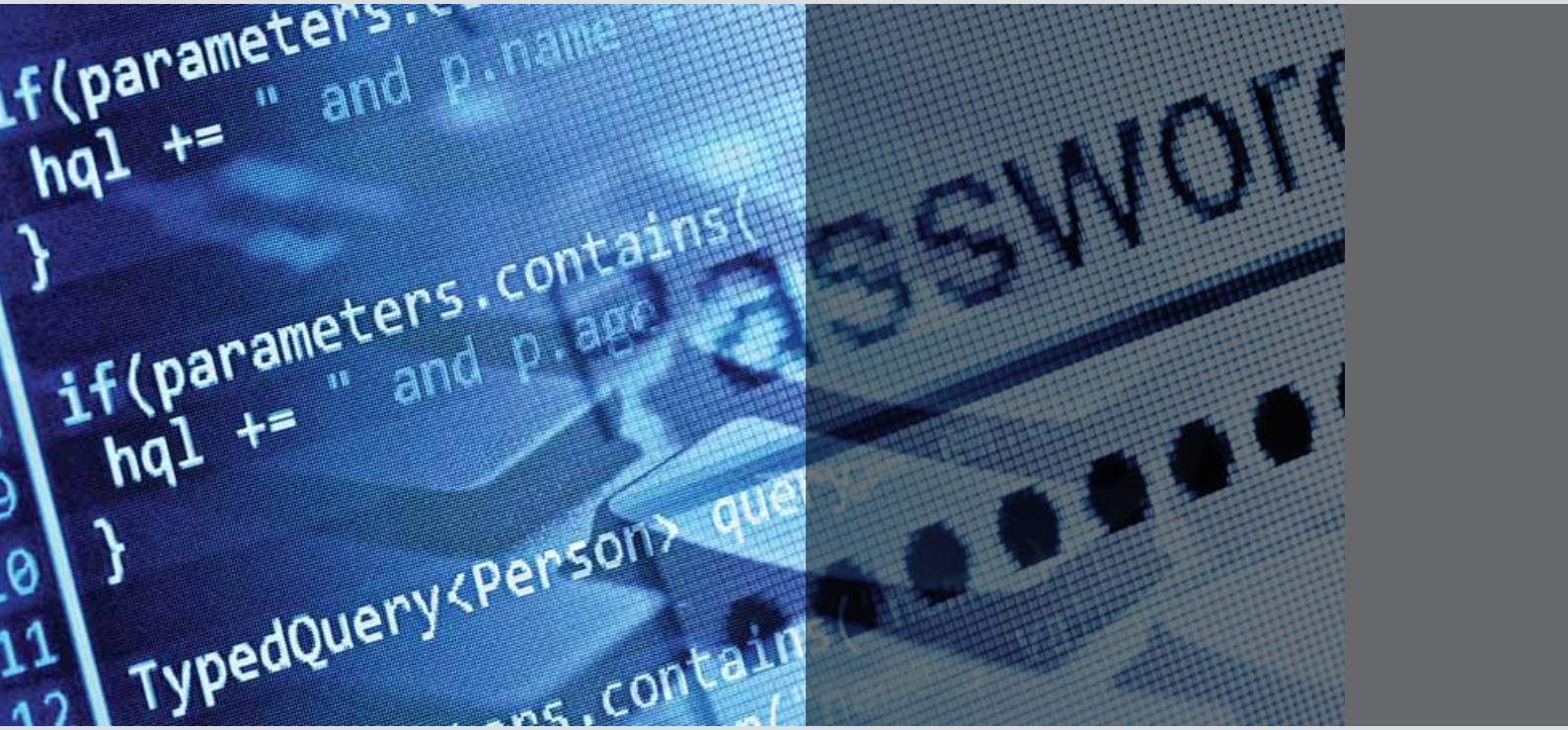
DPO-tjenesten deltager også i en nystartet taskforce i regi af GÉANT, de europæiske forskningsnets paraplyorganisation. Taskforcen ser på, hvordan forordningen fortolkes og implementeres forskelligt i de europæiske lande. Yderligere skal den taskforce også fokusere på at sikre GÉANT's egne tjenester i forhold til forordningens regler.

Taskforcen har haft to møder og forventer at afholde endnu to møder inden den 25. maj 2018, hvor forordningen træder i kraft. Der har været et godt fremmøde, både fysisk og virtuelt, og interessen er stigende.

5.5.4. DeiCs øvrige tjenester

DPO-tjenesten gennemfører også et forordningsrelateret arbejde internt i DeiC, hvor de forskellige DeiC-tjenester gennemgås for at sikre overholdelse med forordningens regler.

Dette arbejde består blandt andet i at kortlægge, hvilke tjenester der indeholder persondata, hvilke typer persondata, hvordan data beskyttes, samt hvordan DeiC kan understøtte henvendelser fra registrerede til uddannelsesinstitutionerne.



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 2017. De har været bragt på web og i nogle tilfælde i det trykte magasin.

6.1. MILLIONER AF LEDIGE JOB OM FÅ ÅR: VI VIL FÅ HÅRDT BRUG FOR DISSE TYPER IT-SIKKERHEDSFOLK

Om fem år mangler der 1,8 millioner it-sikkerhedsfolk på verdensplan.

Det tal er organisationen Center for Cyber Safety and Education nået frem til ved at spørge over 19.000 it-sikkerhedsfolk om deres forventninger til fremtiden.

Da samme undersøgelse blev gennemført i 2015, forventede deltagerne et behov på 1,5 millioner fuldtidsansatte i år 2020.

Bag undersøgelsen står de it-sikkerhedsprofessionelles internationale forening (ISC)2. Den har naturligvis en interesse i at få foreningens medlemmer til at fremstå som nødvendige og eftertragtede.

Men jeg mener alligevel, at foreningen har ret: Vi har et problem. Problemet består i, at der er for få it-medarbejdere med kompetencer inden for sikkerhed.

6.1.1. Både teknikere og organisationsfolk

Et job inden for informationssikkerhed kan have mange facetter. Nogle er tæt på teknikken, andre er tæt på ledelsen og det organisatoriske.

Vi har brug for folk af begge typer. Både dem, der kan konfigurere en firewall og beskytte data på medarbejdernes smartphones, og dem, der udfører risikovurderinger og sætter sikkerhedsforanstaltninger i perspektiv i forhold til forretningens krav og risikovillighed.

Tidligere har mange opbygget kompetencer inden for informationssikkerhed gennem "learning by doing": Ved at installere antivirus eller sætte en firewall op lærte de, hvad de havde brug for.

I dag er informationssikkerhed blevet et så omfattende område, at der er behov for specialisering og uddannelse.

6.1.2. For få kommer på kursus

Men det kniber med at få virksomheder og organisationer til at sende deres folk på kursus.

En it-medarbejder har ellers mange muligheder for at øge sine kompetencer inden for informationssikkerhed.

Universiteterne tilbyder en række forskellige uddannelser. For eksempel kan man bliver master i sikkerhed på Aalborg Universitet. DTU Compute har også en linje med en mere teknisk tilgang. Endvidere findes der en række mellem- og efteruddannelser samt certificeringer.

Et eksempel er CISSP (Certified Information Systems Security Professional), en certificering fra (ISC)2. Foreningen ISACA tilbyder flere certificeringer, bl.a. CISM (Certified Information Security Manager) og en serie nye CSX-certificeringer (Cybersecurity Nexus).

Jeg er selv involveret i en af uddannelsesmulighederne: Den danske ESL-uddannelse (Eksamineret IT-Sikkerhedsleder). Jeg tog uddannelsen for nogle år siden og har siden været med til at uddanne nye kursister.

Det er altid dejligt at møde folk, der har valgt uddannelsen. Men der kunne sagtens være flere.

6.1.3. De nye trusler

En årsag til det øgede behov for sikkerhedsfolk er det ændrede trusselsbillede.

I dag foregår store dele af vores private og professionelle liv over internettet. Dermed får it-kriminelle langt lettere ved at ramme os og få fat i vores data.

Samtidig er gevinsten for de it-kriminelle også vokset. De kan i dag tjene store penge på deres ulovlige aktiviteter. Et eksempel er afpresning med ransomware eller trusler om DDoS-angreb.

Og der er også penge i at skaffe og sælge oplysninger om betalingskort.

6.1.4. Værktøjer kræver viden

De af os, der lever af at beskytte informationsaktiver, får også nye værktøjer til hjælp. Et af de vigtigste der er dukket op de senere år, er ISO 27000-familien af standarder.

Ved at følge ISO 27001 kan en organisation opbygge en klart defineret proces for, hvordan den sikrer sine informationer.

Men det er ikke enkelt. Det kræver viden.

Derfor har vi brug for folk, der bliver certificeret inden for ISO 27001. Og de, der ikke selv bliver certificeret, skal som et minimum lære begreberne at kende.

EU har sat ind for at beskytte borgernes persondata. Det sker med databeskyttelsesforordningen, som bliver håndhævet fra den 25. maj næste år. Til den tid skal virksomheder og organisationer overholde reglerne.

Det kræver uddannelse. For eksempel skal en række organisationer til at ansætte en databeskyttelsesrådgiver.

Sådan en skal være uddannet i forordningens krav. Det kan være en jurist med en passende efteruddannelse. Eller det kan blive en it-medarbejder med interesse for jura, som de tager de nødvendige kurser.

6.1.5. Uddannelse giver overblik

ISO 27001 og databeskyttelsesforordningen er to årsager til, at vi har brug for flere uddannede it-sikkerhedsfolk.
Hvis man kaster sig ud i at indføre ISO 27001 eller efterleve databeskyttelsesforordningen uden uddannelse, kan det gå godt. Men ofte vil man mangle det nødvendige overblik.

Resultatet kan blive, at man fokuserer på nogle detaljer, men overser væsentlige komponenter.

Indførelsen af rammeværk som ISO 27001 indebærer altid en risiko for at ende som ringbindsløsninger: En hylde med ringbind fyldt med papirer med forskrifter, som ingen læser og følger.

En veluddannet medarbejderstab er første skridt mod at sikre, at organisationen får reel værdi ud af et ISO 27001-projekt.

Det samme gælder for informationssikkerhed som helhed: Det kræver kompetente medarbejdere at bekæmpe de voksende sikkerhedsudfordringer, vi møder både på jobbet og i fritiden.

Oprindelig offentliggjort den 5. maj 2017.

6.2. OPRÅB: VI ER NØDT TIL AT KOORDINERE INDSATSEN MOD IT-KRIMINALITET

Vi er nødt til at koordinere indsatsen mod it-kriminalitet.

Den konklusion drager jeg, efter at jeg i sidste uge deltog i arrangementet "Hvordan stopper vi de cyberkriminelle?" arrangeret af Finans Danmark, Tænketanken Ret & Sikkerhed og Forbrugerrådet Tænk med støtte fra TrygFonden.

Der bliver allerede gjort en stor indsats for at bekæmpe it-kriminalitet og øge informationssikkerheden. Det sker blandt andet hos Center for Cybersikkerhed, Rigspolitiets Nationale Cyber Crime Center (NC3) og i sektororganisationer som vores egen DKCERT, der behandler sikkerhedshændelser på forskningsnettet.

Men der mangler koordinering. Det var en af hovedpointerne i et indlæg fra lektor Karen Lund Petersen fra Institut for Statskundskab ved Københavns Universitet.

"Der er ikke et samlet organ, som virksomheder kan rapportere sikkerhedshændelser til," påpegede hun.

Jeg er enig. Og jeg vil tilføje, at det samme også gælder for private borgere.

6.2.1. Borgere savner hjælp

Hvis en borger bliver udsat for en sikkerhedshændelse, kan vedkommende melde det til politiet – forudsat, at det er en forbrydelse, og der er sket påviselig skade.

Desværre savner politiet ressourcer og kompetencer på it-siden. NC3 har dygtige folk, men det er en specialenhed uden selvstændig jurisdiktion. Den må ikke efterforske sager, det skal ske ude i politikredsene. Og de har behov for efteruddannelse.

Hvor går borgeren hen, hvis en sikkerhedshændelse ikke ligner en forbrydelse, men der stadig er brug for hjælp? Det spørgsmål mangler vi at få afklaret.

Noget af ansvaret for borgernes informationssikkerhed ligger hos Digitaliseringsstyrelsen, der blandt andet udarbejder awareness-kampagner.

Det er en god indsats, men styrelsen kan ikke behandle massevis af henvendelser fra borgerne.

Og der kan blive tale om masser af henvendelser. Det fremgik af et indlæg fra Anja Philip, formand for Forbrugerrådet Tænk. Hun fortalte, at rådets app "Mit digitale selvsvar" er hentet næsten 30.000 gange. Appen advarer brugerne om aktuelle trusler.

Som en del af appen kan brugerne indsende trusler, de selv er blevet udsat for. Det kan for eksempel være phishing-mails.

Siden premieren i april har brugerne indsendt næsten 1.000 tips om trusler. Forbrugerrådet Tænk har tre medarbejdere på deltid til at undersøge henvendelserne.

DKCERT har tidligere meldt ud, at vi er klar til at påtage os opgaven med at håndtere henvendelser fra borgerne. Erfaringen fra appen viser, at der ligger en stor arbejdsbyrde i at behandle den slags henvendelser.

Uanset om opgaven lander hos DKCERT, Forbrugerrådet Tænk, Digitaliseringsstyrelsen eller et helt fjerde sted, skal der afsættes de nødvendige midler til at løse opgaven.

6.2.2. Paraply efterlyses

En mulig løsning på behovet for koordinering er at oprette en paraplyorganisation, der sikrer, at indsatsen for informationssikkerhed koordineres på tværs af sektorer.

Sådan en enhed kan sørge for, at de forskellige organisationer samarbejder og udveksler information. Og den kan sikre, at der oprettes de funktioner, der mangler i dag – for eksempel når det gælder borgerne.

Oprindelig offentliggjort den 30. juni 2017

6.3. OPDATER TRÅDLØST UDSTYR, MEN LIG IKKE VÅGEN AF FRYGT FOR SÅRBARHEDS-PROBLEMET KRACK

Truslen fra en udbredt samling sårbarheder i trådløse netværk er reel, men næppe alvorlig for langt de fleste. Men vær forberedt, for KRACK kan blive en større trussel, end den er i dag. "Næsten alle Wi-Fi-net i verden er blevet hacket," lød en overskrift fra avisen The Independent den 16. oktober.

Nej, det er de ikke.

Derimod er der opdaget en samling sårbarheder, der findes i stort set alt moderne Wi-Fi-udstyr.

Som enhver sårbarhed med respekt for sig selv har den naturligvis både navn, logo og eget websted. Den hedder KRACK (Key Reinstallation Attacks) og er opdaget af den belgiske sikkerhedsforsker Mathy Vanhoef.

Sårbarheder, der gør det muligt at aflytte krypteret kommunikation på trådløse netværk, lyder umiddelbart alvorlige.

Men en række faktorer gør, at jeg vurderer risikoen til et sted mellem lav og medium.

6.3.1. Skal være i nærheden

Sårbarhederne findes i protokollen WPA2 (Wi-Fi Protected Access), som bruges til at kryptere kommunikationen på Wi-Fi-netværk. Problemet opstår i udvekslingen af krypteringsoplysninger mellem en klient og et trådløst adgangspunkt.

Dermed skal en angriber være inden for radioafstand for at kunne udnytte sårbarheden.

Vi taler altså ikke om en sårbarhed, der kan udnyttes over internettet. Kinesiske eller russiske hackere kommer næppe til at bruge KRACK til at få fat i vores forretningshemmeligheder.

Desuden er den ikke helt ligetil at udnytte. En angriber skal aflytte kommunikationen, indsætte sine egne datapakker i den, og derefter regne sig frem til krypteringsnøglen. I øvrigt medfører angrebet ikke, at angriberen får fat i kodeordet til det trådløse net.

6.3.2. Android er udfordret

Det mest bemærkelsesværdige ved sårbarheden er, at den findes i selve WPA2-standarden, ikke i en bestemt implementering af den. Derfor bør alt WPA2-udstyr som udgangspunkt regnes for sårbart.

Sårbarheden er værst på klientsiden. Derfor er det vigtigst at opdatere klient-software.

Microsoft har allerede lukket sikkerhedshullet. Det samme gælder en række Linux- og Unix-varianter. Apple er på vej med rettelser.

Alvorligst står det til med Android. Her forværres sårbarheden af en fejl i implementeringen, der nulstiller en krypteringsnøgle. Så bliver det let at dekryptere kommunikationen. Fejlen findes i Android fra version 6 og op. Det er særlig uheldigt, fordi mange Android-enheder ikke modtager sikkerhedsopdateringer.

Her kan det vise sig at være en fordel, at nyere versioner er sårbare – de har trods alt større chance for at blive opdateret end ældre Android-versioner.

Enheder på det såkaldte Internet of Things (IoT) kan også blive en udfordring. Erfaringen viser, at de ofte ikke modtager softwareopdateringer. Så webkameraer, højttalersystemer og anden elektronik med indbygget internet-adgang kan være i risikozonen. Spørgsmålet er så, hvor interessant det er at aflytte deres kommunikation.

6.3.3. En mindre trussel

Hvor alvorlig truslen fra KRACK er, må i det hele taget komme an på en individuel risikovurdering. Men for langt de fleste er det næppe en realistisk trussel, at angribere vil placere sig inden for radiorækkevidde for at forsøge at dekryptere kommunikation.

Ofte vil der i øvrigt være flere lag af kryptering. Når vi bruger netbank og andre følsomme tjenester, krypteres kommunikationen med TLS (Transport Layer Security).

Så her får angriberen ikke noget ud af at knække WPA2-krypteringen – derefter skal TLS-kodningen også knækkes.

6.3.4. Resultat af lukkethed

KRACK-sårbarhederne har eksisteret siden 2004, da IEEE 802.11i-standarden blev indført.

Hvordan går det til, at så væsentlige fejl i en standardprotokol kan eksistere? En årsag kan være, at der er tale om en standard udviklet under IEEE (Institute of Electrical and Electronics Engineers). Disse standarder er ikke frit offentligt tilgængelige. Interesserede skal købe dokumenterne.

Der er ganske vist en mulighed for, at akademikere kan få adgang til standarderne. Men det sker først et halvt år efter, standarden er publiceret. På det tidspunkt er producenterne for længst gået i gang med at implementere dem i deres produkter.

Hvis WPA2-standarden havde været lettere at få fat i, er der større chance for, at sikkerhedsforskere havde kigget på den og opdaget KRACK, inden der var gået 13 år.

6.3.5. Ingen panik

Min konklusion: Truslens alvor har været overdrevet. Der er ingen grund til panik.

Tidligere sårbarheder har dog vist sig at være mere alvorlige end først antaget. Det sker, efterhånden som sikkerhedsforskere og angribere graver sig dybere ned i detaljerne. Så vær forberedt på, at KRACK kan blive en større trussel, end den er i dag.

Indtil da gælder det om at beskytte sig bedst muligt:

- Sørg for at opdatere først klienter, siden routere og adgangspunkter.
- Hvis I bruger 802.11r, bør I slå det fra, indtil udstyret er opdateret.
- Benyt flere lag af sikkerhed på trådløse netværk, for eksempel ved hjælp af VPN og anden kryptering.

Oprindelig offentliggjort den 27. oktober 2017

6.4. DERFOR ER DEN SVENSKE IT-SKANDALE IKKE EN IT-SKANDALE - OG DATABESKYTTELSE MÅ ALDRIG BLIVE EN SPAREØVELSE

Det er ikke en it-skandale. Det er en sag om myndigheder, der alvorligt svigter offentlighedens tillid.

Jeg tænker på den aktuelle sag fra Sverige, hvor en række følsomme data kan være kommet i uvedkommendes hænder.

En myndighed outsourcede it-systemer og undlod at følge kravene om, at data kun måtte behandles af personer med sikkerhedsgodkendelse.

Sagen er for mig et eksempel på, at vi tænker på data på en forkert måde. Når en offentlig myndighed eller en privat virksomhed behandler data om personer, har den fået dem betroet af de personer, dataene handler om. Derfor er det forkert, hvis man for at spare penge giver køb på sikkerheden.

Tænk tilbage på tiden før digitaliseringen.

6.4.1. Stålskabet

Dengang lå for eksempel kommunerne også inde med fortrolige data om borgerne. Disse data stod på papirer, der blev opbevaret i hængemapper i aflåste arkivskabe. Ingen kommunal embedsmand kunne finde på at overlade nøglen til stålskabet til uvedkommende.

Den tankegang skal vi tilbage til.

Når data er digitale, er det utrolig nemt at kopiere, flytte og behandle dem. Men fordi noget er nemt, er det ikke nødvendigvis rigtigt. Vi skal igen til at opfatte data som betroet gods. Noget, som borgerne eller kunderne har givet os lov til at bruge på betingelse af, at vi passer godt på det.

I praksis betyder det, at vi skal være meget omhyggelige, når vi udarbejder databehandleraftaler. Vi skal skrive helt klart, hvem der må behandle data og under hvilke betingelser.

6.4.2. Lovforslag er i høring

At beskytte persondata effektivt er grundtanken bag den databeskyttelsesforordning, som EU har vedtaget. Forordningen gælder automatisk som lov i Danmark fra maj næste år.

Men der er områder, som forordningen overlader det til medlemslandene at tage stilling til. Derfor har justitsministeriet nu udarbejdet et forslag til dansk lov, der indfører de dele, som forordningen ikke dækker. Lovforslaget er i offentlig høring, du kan finde det på Høringsportalen.

En god ting ved forordningen er, at den gør det dyrt at sløse med persondata.

Hvis en virksomhed ikke beskytter data ordentligt, så de bliver lækket, kan den straffes med bøde eller ligefrem fængsel. Straframmen går op til 20 millioner euro eller fire procent af virksomhedens årlige omsætning. I praksis venter jeg dog, at de reelle bøder vil blive lavere.

6.4.3. Straf til det offentlige

Hvad så med offentlige myndigheder? Skal de også kunne idømmes straf? Det spørgsmål har været udestående, siden forordningen blev vedtaget. Det er nemlig op til de enkelte medlemslande.

Derfor var jeg spændt på at se, hvad lovforslaget siger om det. Her er ordlyden af §41 stk. 5:

"[stillingtagen til sanktionsspørgsmålet i forhold til offentlige myndigheder udestår]"

Så det må blive op til folketingets partier at afgøre.

Personlig er jeg i tvivl.

Et argument for en strafmulighed er, at det giver en klar motivation for at overholde loven. Endvidere har vi et princip om lighed for loven – hvorfor skal private virksomheder kunne idømmes bøder, mens offentlige myndigheder kan gå fri?

Imod taler, at der i sidste ende kun er et sted at hente de penge, en offentlig myndighed skal betale: Hos borgerne. Det kan ske i form af højere skatter eller forringet service. Vil vi acceptere længere ventetider på hospitalet, fordi det skal bruge penge på en bøde?

I dag har Datatilsynet meget begrænsede sanktionsmuligheder. Hvert år besøger tilsynet en række myndigheder. Og hvert år finder det tilfælde, hvor persondataloven ikke er overholdt.

Det medfører aldrig bøder – de er kun i få tilfælde givet til private virksomheder. Over for offentlige instanser er sanktionen kun, at Datatilsynet offentliggør kritik af myndigheden på sin webside.

Så erfaringen tyder på, at kritik ikke er tilstrækkeligt. En form for skrappere sanktion er nok nødvendig. Men om det skal være straffe i samme omfang som dem til de private aktører, er jeg i tvivl om. Måske skal det – som i det svenske tilfælde – være en personlig bøde til den ansvarlige chef.

Jeg kan anbefale at tage et kig på lovforslaget. Hvis du får lyst til at kommentere det, kan du sende et høringssvar. Sidste frist er den 22. august.

Oprindelig offentliggjort den 28. juli 2017

6.5. HVAD GØR DU MED DE DATA, SOM DIN APP INDSAMLER? DU SKAL VÆRE KLAR MED ET SVAR INDEN LÆNGE

En Android-app giver "hurtigt og nemt overblik over spændende kulturelle oplevelser, arrangementer og steder" i en kommune.

Meget fint. Men hvorfor har appen brug for at få adgang til følgende data på telefonen?

- Identitet.
- Kontaktpersoner.
- Præcis placering.
- Opkald.
- Billeder/medier/filer – læse, ændre eller slette indhold på USB-lageret.
- Lagerplads.
- Kamera – tage billeder og optage video.
- Oplysninger om Wi-Fi-forbindelse.
- Enheds-id og opkaldsoplysninger.

Appen er udviklet af et firma, der udbyder den i samarbejde med den pågældende kommune.

6.5.1. Husk samtykke

Lad os tage databeskyttelsesbrillerne på og se nærmere på den type app. Som bekendt træder databeskyttelsesforordningen i kraft 25. maj næste år. Hvad vil den betyde for sådan en app?

Først må vi afgøre, hvem der er dataansvarlig. Er det kommunen eller samarbejdspartneren, der leverer indhold til den?

Den dataansvarlige er altid den, der bruger dataene, og hvis jeg installerer appen, skal jeg ifølge databeskyttelsesforordningen give mit samtykke til, at den indsamler data. Mit samtykke skal være frivilligt, specifikt, informeret og utvetydigt.

Jeg synes, appen har et problem med, at samtykket skal være informeret. Som bruger vil jeg gerne vide, hvilke data den indsamler med hvilket formål.

Ja, jeg får at vide, at appen får adgang til mine kontaktpersoner og filer på enheden. Men hvilke data bruger den? Hvad bruger den data til? Hvor bliver de lagret? Hvordan kan jeg få indsigt i, hvilke data appen har indsamlet?

Og hvordan kan jeg rette fejl i data eller få dem slettet?

Disse spørgsmål finder jeg ikke svar på i standardbeskrivelsen af appens tilladelser i Play Store.

6.5.2. Luskede apps

Spørgsmålet om samtykke bliver endnu mere presserende, når det gælder apps, der snyder brugeren. Jeg tænker på øjensynligt uskyldige apps, der for eksempel udstyrer smartphonen med en lommelygte.

Nogle af den slags apps har et skjult formål. For eksempel kan de lytte efter bestemte lydsignaler, der udsendes sammen med tv-reklamer. På den måde kan de rapportere, at brugeren har været i et lokale, hvor reklamen blev vist.

Udviklerne af den type apps må forudse store problemer, når databeskyttelsesforordningen træder i kraft.

6.5.3. Vær klar til at svare

Hvis I udvikler eller udbyder apps, bør I overveje, hvordan I vil besvare ovenstående spørgsmål. For det skal I kunne, når forordningen træder i kraft. Og dataansvarlige må forvente mange henvendelser mandag 28. maj 2018.

På den første arbejdsdag efter, at forordningen er trådt i kraft, kan der komme en strøm af forespørgsler fra registrerede personer.

I første omgang handler det næppe om at rette eller slette data. Personerne vil sandsynligvis begynde med at få et overblik over, hvad der overhovedet er registreret om dem.

Hvis ideen om at få indsigt går viralt, må virksomheder forudse en strøm af henvendelser. Måske kommer der ligefrem en app, der på enkel vis gør det nemt at sende forespørgsler til en række organisationer, der kan tænkes at ligge inde med data.

Er I forberedt på at besvare adskillige henvendelser om, hvad I har registreret om brugerne af jeres apps?

Og er I i stand til at slette eller rette i data, når den registrerede person ønsker det?

Husker I at slette data, når I ikke længere har brug for dem?

6.5.4. Kan du besvare disse spørgsmål?

Databeskyttelsesforordningen medfører, at man risikerer bødestraf, hvis man ikke overholder reglerne. Derfor kan det blive dyrt for virksomheder, hvis de ikke har styr på forordningen.

Det er mit indtryk, at mange dataansvarlige er famlende over for, hvordan de skal håndtere databeskyttelsesforordningen. Det gælder ikke kun data, der indsamles via apps, men helt generelt. Vi har ellers kendt til indholdet i forordningen i mindst halvandet år.

Alligevel kan mange organisationer ikke besvare disse spørgsmål:

- Hvilke data om personer registrerer I?
- Hvor ligger data?
- Hvordan kan I udlevere data til de registrerede personer?
- Hvor har I dokumenteret, at I har indhentet samtykke til registreringen?
- Hvordan kan registrerede personer få rettet eller slettet data?

Få nu styr på det. I har otte måneder.

Oprindelig offentliggjort den 29. september 2017

7. Fremtidens trusler og trends

It-kriminelle bliver stadig mere professionelle. Beskyttelsen af personlige data kommer i centrum i år.

Enten går de efter penge, eller også arbejder de for efterretningstjenester. Det er den korte beskrivelse af de typiske it-kriminelle i dag. I nogle tilfælde kan det være begge dele – et angreb kan ligne ransomware, men reelt være et forsøg på at sætte en infrastruktur ud af drift.

7.1. TRUSLER MOD INFORMATIONSSIKKERHEDEN I 2018

7.1.1. It-kriminalitet er blevet professionel

Forbrydelser som en tjenesteydelse har været en stigende tendens de senere år. En begynder inden for it-kriminalitet behøver ikke selv at skrive virus eller hacke sig ind på servere: Man kan købe sig ind på et botnet, få adgang til stjålne kreditkortnumre eller abonnere på andre lyssky tjenester.

Det er et resultat af den professionalisering, som den it-kriminelle underverden har gennemgået. I dag optræder dele af den som virksomheder med planer for markedsføring, rekruttering, salgskanaler og vidensdeling.

To teknologier er medvirkende til at gøre det muligt: TOR og kryptovalutaer.

TOR anonymiserer ens færden på nettet. De kriminelle opretter butikker på det såkaldte dark web, som man skal bruge TOR for at få adgang til.

Kryptovalutaer 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. Tøj kan også hackes

De senere år har vi set flere eksempler på angreb på Internet of Things-udstyr. Det vil fortsætte. Når genstande udstyres med en processor og netadgang, bliver de med det samme potentielle angrebsmål.

De næste på listen kan derfor blive smartwatches, kondimålere, smykker og tøj med indbygget netopkobling.

7.1.3. Enkle angreb får succes

Forholdsvis simple angreb må forventes fortsat at udgøre hovedparten af al it-kriminalitet. Og de vil fortsat have stor succes.

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

7.2. SIKKERHEDSTRENDS I 2018

7.2.1. Persondata kommer i centrum

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

På sikkerhedssiden taler forordningen om risikobaseret sikkerhed. Dermed bliver den en god anledning til at lære at tænke på risiko. For nogle organisationer vil det være en større omlægning af tilgangen til sikkerhed, for andre falder det naturligt.

7.2.2. Trådløs sikkerhed med WPA3

I 2017 afdækkede en sikkerhedsforsker sårbarhederne KRACK (Key Reinstallation Attacks) i WPA2, som er standarden for sikkerhed på trådløse netværk. I 2018 kan vi vente version 3 af WPA (Wi-Fi Protected Access), og måske også de første produkter baseret på den. Den ventes både at løse problemerne med KRACK og indføre yderligere forbedringer af sikkerheden[14].

[14] WPA3 skal øge sikkerheden for trådløse netværk, DKCERT, 16-1-2018, https://www.cert.dk/da/news/2018-01-16/WPA3

7.2.3. To-faktor-autentificering og password managers

Passwords er ikke den bedste sikring mod uønsket adgang. Men ofte er det den, det er teknisk muligt at indføre. Til gengæld udvikles der løbende metoder til at supplere sikkerheden. DKCERT venter, at de vil blive brugt mere.

En metode er to-faktor-autentifikation. Her suppleres passwordet med noget andet, fx en engangskode fra et nøglekort (NemID), en kode sendt via sms eller en kode fra en autentifikations-app. Det beskytter mod angreb, hvor en hacker kun har fået fat i brugernavnet og passwordet.

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 passwordet til password manager-programmet er meget sikkert.

I takt med, at vi anvender stadig flere tjenester, der er beskyttet med password, venter 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 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.
3. Forbered overholdelse af databeskyttelsesforordningen.
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.
14. Indfør tiltag mod misbrug via gæstenetværk.
15. Anvend single sign-on suppleret med to-faktor-autentifikation.
16. 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 persondatalovgivningen, 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. Kortlæg flowet af persondata i organisationen med henblik på at leve op til databeskyttelsesforordningen.
5. Hold de ansatte, studerende og gæster informeret om informationssikkerhedspolitikken og aktuelle problemer.
6. Etabler et beredskab og udarbejd en beredskabsplan for kritiske hændelser.
7. Prioriter og synliggør risikostyring.
8. Foretag løbende risikovurderinger af forretningskritiske systemer.
9. Afsæt ressourcer til uddannelse og kompetenceudvikling 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.

Cloud computing
Services distribueret i en sky af primært virtuelle ressourcer. Skyen giver mulighed for, at man får adgang til ressourcer efter behov. Skalerbarhed og pris er ofte de væsentligste argumenter for at lade sine services outsource til skyen. Overordnet skelnes mellem tre forskellige typer af cloud-services: Software as a Service (SaaS), Platform as a Service (PaaS) og Infrastructure as a Service (IaaS).

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 request forgery (CSRF)
En metode, der muliggør at uautoriserede parametre og kommandoer eksekveres på serveren gennem henvendelser fra en bruger, som websitet har tillid til. Metoden kan for eksempel medføre overtagelse af brugerens session.

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

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

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

Defacement
Web defacement er et angreb på et websted, hvor websider overskrives med angriberens signatur og ofte et politisk budskab.

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, der vil blive håndhævet fra 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 27002
En vejledning til, hvordan en organisation kan opfylde kravene i ISO/IEC 27001.

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-browser
Et angreb relateret til man-in-the-middle-angreb, hvor en trojansk hest kan modificere websider og indhold af transaktioner uden brugerens vidende. Dermed kan kriminelle fx overtage sessionen til netbanken, overføre penge fra brugerens konto og herefter ændre indholdet i browseren, således at overførslen ikke fremgår af kontooversigten.

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

MDM
Mobile Device Management er software, der benyttes til central administration og sikkerhed på enhedsniveau af mobile enheder.

NemID
NemID er en fælles certifikatbaseret dansk loginløsning til netbanker og offentlige hjemmesider, der baserer sig på den offentlige digitale signatur. Løsningen består af en personlig adgangskode og et nøglekort. NemID blev sat i drift 1. juli 2010 og bliver drevet af firmaet Nets DanID.

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.

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.

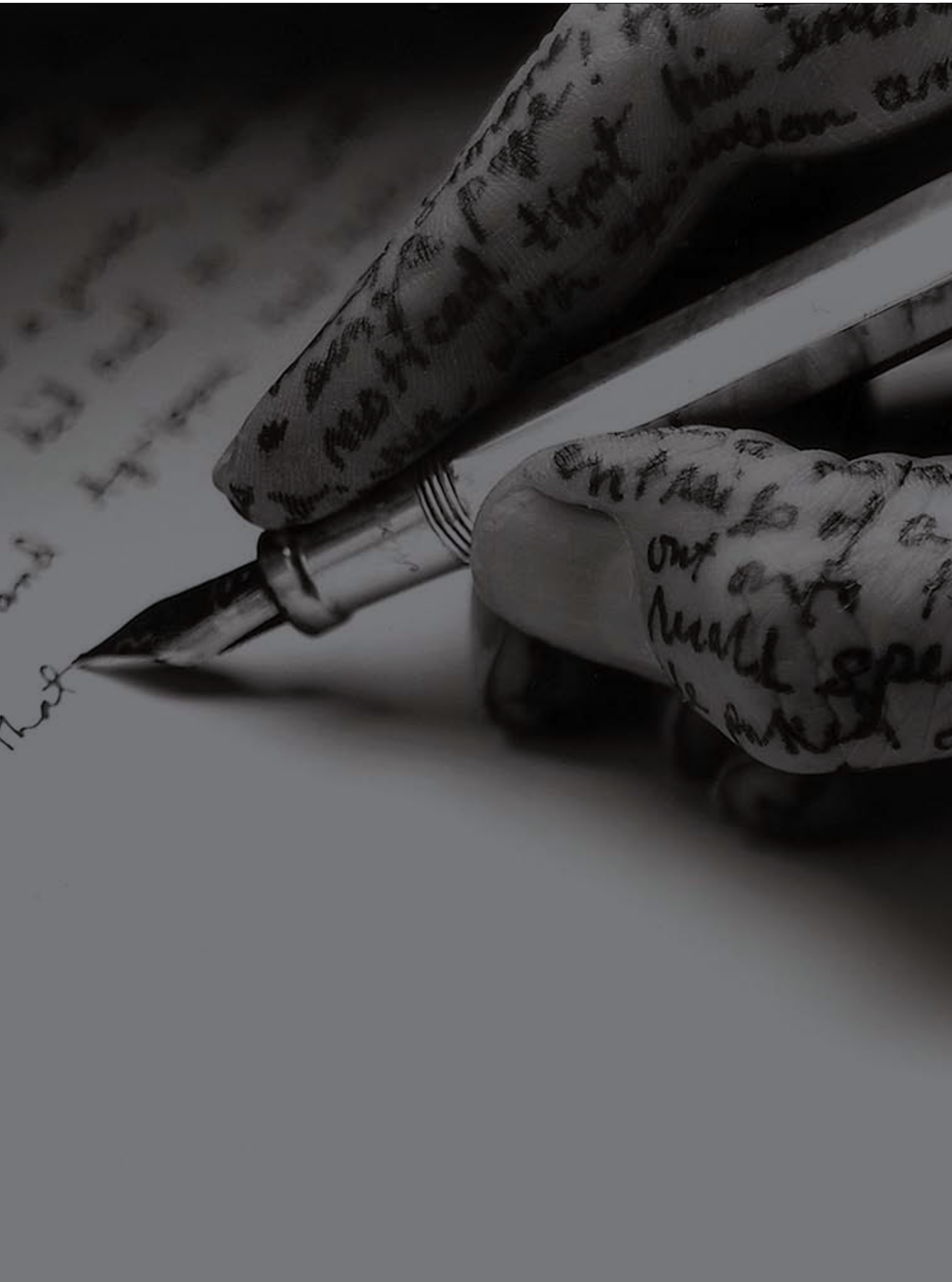
To-faktor-autentifikation
Autentifikation, der supplerer brugernavn og password med en yderligere faktor, som brugeren skal angive for at få adgang. Det kan være en engangskode, der sendes til brugerens mobiltelefon som sms, et fingeraftryk, der angives via en fingeraftrykslæser, en kode fra et papirkort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

Warez, piratsoftware
Begrebet dækker over computerprogrammer, musik, film og lignende, der distribueres illegalt og i strid med rettigheder og licensbetingelser. Warez er en sproglig forvanskning af ordet software.

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



10. Figurliste

11. Kilder og referencer

Tallene henviser til kildernes fodnotenumre.

1 Cloudflare har lækket fortrolige data, DKCERT, 24-2-2017, https://www.cert.dk/da/news/2017-02-24_Cloudflare

2 Ransomware-ormen WanaCrypt0r har ramt tusindvis af computere, DKCERT, 13-5-2017, https://www.cert.dk/da/news/2017-05-13/WanaCrypt0r

3 Angreb udnytter sårbarhed i Apache Struts, DKCERT, 10-3-2017, https://www.cert.dk/da/news/2017-03-10_Struts

4 Sårbarheder i Bluetooth gør angreb mulige, DKCERT, 13-9-2017, https://www.cert.dk/da/news/2017-09-13/BlueBorne

5 Kryptering af trådløse netværk har alvorligt sikkerhedshul, DKCERT, 16-10-2017, https://www.cert.dk/da/news/2017-10-16/KRACK

6 Intel lukker alvorlige huller i chipsæt, DKCERT, 23-11-2017, https://www.cert.dk/da/news/2017-11-23/Intel

7 Oracle lukker alvorlige huller i Tuxedo, DKCERT, 22-11-2017, https://www.cert.dk/da/news/2017-11-22/Oracle

8 Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes, Washington Post, 12-1-2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

9 2017: Poor Internal Security Practices Take a Toll, Gemalto, http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

10 Year in Review: Notable Data Breaches for 2017, Trend Micro, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017

11 Alla svenska körkortsfoton läckte till Tjeckien, SVT, https://www.svt.se/nyheter/inrikes/alla-svenska-korkortsfoton-lackte-till-tjeckien

12 "Databeskyttelse gennem design" i Revision og Regnskabsvæsen, https://www.karnovgroup.dk/artikler/rr-12-2017-databeskyttelse

13 Rådet for Digital Sikkerhed: Vejledning om Databeskyttelse gennem Design, https://www.digitalsikkerhed.dk/nyheder/2017/11/22/rdet-for-digital-sikkerhed-vejledning-om-databeskyttelsen-gennem-design

14 WPA3 skal øge sikkerheden for trådløse netværk, DKCERT, 16-1-2018, https://www.cert.dk/da/news/2018-01-16/WPA3

DKCERT/DeiC

DTU, Asmussens Allé
Bygning 305
2800 Kgs. Lyngby

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

Trendrapport