DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

DKCERT Trendrapport 2017

Redaktion: Henrik Larsen og Torben B. Sørensen

Tak til vore øvrige bidragydere:

Tonny Bjørn, DKCERT,

Bjarne Mathiesen Schacht, DKCERT,

Shehzad Ahmad, Nets A/S,

Christian Wernberg-Tougaard, IT-Branchen,

Christian Ehlers Mikkelsen, Implement A/S og

Christian Damsgaard Jensen, DTU Compute.

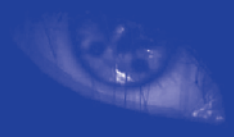
Design og layout: Kiberg Gormsen

DeiC-journalnummer: DeiC JS 2017-02

DKCERT, 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 afdeling 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 er oprettet i 1991 og 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

Uddannelse er afgørende i en verden med stigende udfordringer for informationssikkerheden.

Databeskyttelsesforordningen. ISO 27001. Internet of Things.

Der er nok at tage fat på for sikkerhedsfolkene. Og vi får brug for flere af dem: Medarbejdere med faglig viden om informationssikkerhed og hvordan vi sikrer den.

Dette års trendrapport har Internet of Things (IoT) i fokus. Det er et eksempel på et område, vi ikke kendte for ti år siden: Alskens apparater udstyres med en IP-adresse og en indbygget webserver, så vi kan bruge og konfigurere dem fra vores smartphones og pc'er. Men hvad betyder det for sikkerheden? Det giver nogle fagfolk deres bud på i kapitlet Det eksterne perspektiv.

Også EU's databeskyttelsesforordning medfører nye opgaver til sikkerhedsfolkene. Nogle af reglerne får konsekvenser for den tekniske opsætning af systemerne, andre handler om organisation og procedurer. Det samme gælder for de organisationer, der indfører styring af deres informationssikkerhedsarbejde ud fra reglerne i ISO 27001.

De nye opgaver kræver nye kompetencer. Vi får brug for medarbejdere, der er uddannet i databeskyttelsesforordningen og dens praktiske konsekvenser. Forordningen stiller krav om, at visse organisationer skal udpege en datarådgiver. Men der skal bruges mange andre kompetencer. Det gælder både sikkerhedsteknikere og folk, der kan håndtere den organisatoriske side af sikkerheden. Her tænker jeg på det, man internationalt betegner som GRC (Governance, Risk, and Compliance).

Der er gode muligheder for at blive uddannet på både den tekniske og organisatoriske side. De danske universiteter tilbyder en bred vifte af uddannelser – både komplette uddannelser og efteruddannelseskurser.

En række foreninger og private organisationer tilbyder også relevante kurser og certificeringer.

Desværre er det op ad bakke med at få virksomheder og organisationer til at erkende, at der er behov for mere uddannelse. En del har ganske vist uddannet deres folk, men der er brug for flere.

Med veluddannede medarbejdere bliver det lettere for både virksomheder og andre organisationer at efterleve kravene i databeskyttelsesforordningen. Og det, der fra starten kan se ud som endnu en besværlig omgang bureaukrati, kan ende med at blive en værdifuld del af informationssikkerhedsarbejdet.

God fornøjelse med læsningen af dette års DKCERT Trendrapport!

Henrik Larsen

chef for DKCERT

2. Resumé

DKCERT behandlede færre sikkerhedshændelser i 2016 end året før. Det kan skyldes bedre sikkerhed hos institutionerne på forskningsnettet.

DKCERT behandlede 95.597 sikkerhedshændelser i 2016. 86.993 var advarsler fra tredjepart om potentielle sikkerhedsrisici. Dermed var antallet af egentlige sikkerhedshændelser på 8.604. Både mængden af advarsler og egentlige hændelser faldt i forhold til året før.

Halvdelen af advarslerne handlede om systemer, der potentielt havde POODLE-sårbarheden (Padding Oracle On Downgraded Legacy Encryption).

81 procent af de egentlige hændelser var klager over misbrug af ophavsbeskyttet materiale.

DKCERTs sårbarhedsscanninger fandt sårbarheder på 27,7 procent af de IP-adresser, der blev undersøgt. I gennemsnit blev der fundet 7,6 sårbarheder på hver af de sårbare IP-adresser. Fire procent af sårbarhederne var alvorlige, to procent kritiske.

Mængden af modtagere af DKCERTs ugentlige nyhedsbreve steg 11 procent til 1.348 abonnenter. Antallet af følgere på Twitter steg 45 procent til 1.575 personer.

2.1. TENDENSER FRA ÅRET DER GIK

It-kriminelle stod bag flere store DDoS-angreb (Distributed Denial of Service). Nogle af dem udnyttede sårbare apparater (Internet of Things, IoT), som blev samlet i botnet. Nogle angreb var koblet til afpresningsforsøg, hvor offeret kunne slippe for at blive angrebet mod at betale en sum penge.

Angreb med ransomware var udbredte: Skadelig software krypterer offerets data og kræver løsepenge for at frigive den nøgle, der kan dekryptere dem. Europol har sammen med sikkerhedsfirmaer lanceret en webportal, der hjælper ofre.

Store mængder af persondata blev sat til salg på nettet. Mange af dem stammede fra flere år gamle hackerangreb.

Politisk motiveret hacking var i fokus under den amerikanske præsidentvalgkamp, hvor demokraternes valgorganisation blev hacket.

3. 2016 – året i tal

DKCERT behandlede 95.597 sikkerhedshændelser i 2016. 86.993 var advarsler fra tredjepart.

3.1. ÅRETS SIKKERHEDSHÆNDELSER

I alt modtog DKCERT henvendelse om 95.758 sikkerhedshændelser i 2016. 161 af dem blev afvist, det var fx spam eller mail sendt til en forkert adresse. Dermed behandlede DKCERT 95.597 hændelser i løbet af året.

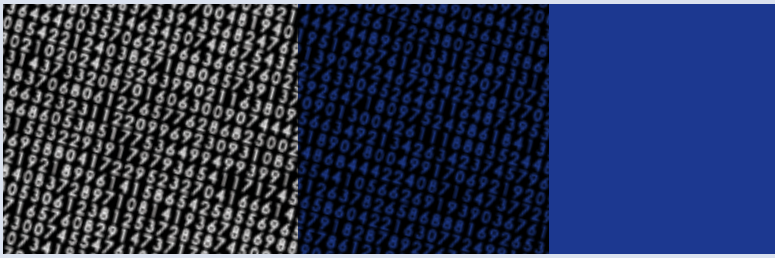
Langt de fleste hændelser var registreringer af advarsler fra tredjeparter. Denne service, som blev introduceret i 2015, giver institutionerne på forskningsnettet advarsler om potentielt sårbare systemer hos dem. Advarslerne kommer fra tredjeparter, der løbende scanner internettet for kendte sårbarheder, 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.

I alt var der 86.993 af disse advarsler fra tredjeparter. Dermed var antallet af egentlige sikkerhedshændelser på 8.604 (se Figur 1).

Vi har ikke nøjagtige tal for antallet af advarsler i forhold til sikkerhedshændelser i 2015, men anslår dem til knap 141.000 ud af de godt 160.000 hændelser, vi behandlede i 2015.

Dermed var der et fald på 44 procent i behandlede sikkerhedshændelser fra 2015 til 2016 (se Figur 2).



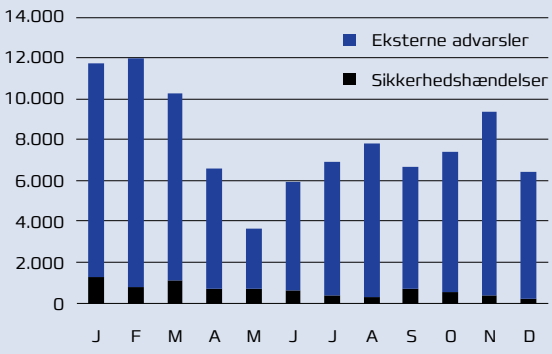
Mængden af advarsler fra tredjepart faldt 38 procent, mens øvrige hændelser faldt 55 procent.

DKCERT mener

Når mængden af advarsler falder, er det tegn på, at der findes færre sårbare systemer. Dermed ser advarslerne ud til at virke: Institutionerne får lukket sikkerhedshullerne, så scanningerne finder færre sårbarheder. Færre sikkerhedshuller kan også medvirke til faldet i egentlige sikkerhedshændelser.

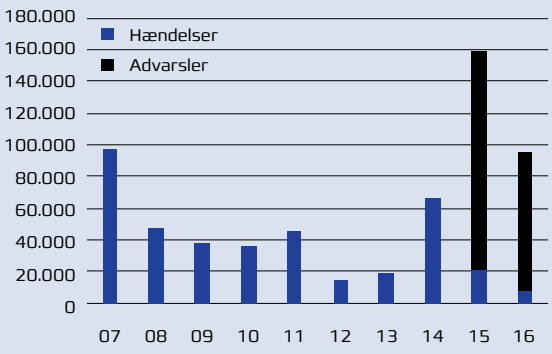
Figur 1: Hændelser pr. måned

En leverandør af advarsler havde tekniske problemer i maj, hvor der derfor blev udsendt færre advarsler.



Figur 2: Sikkerhedshændelser behandlet af DKCERT 2007-2016

Udvikling i antallet af sikkerhedshændelser, DKCERT behandler. Tallene er ikke sammenlignelige på tværs af årene grundet ændringer i registreringsmetoder.



3.2. SIKKERHEDSHÆNDELSER FORDELT PÅ TYPER

8.244 af de egentlige sikkerhedshændelser, DKCERT behandlede, er udstyret med en kategori. Her gennemgår vi de mest fremtrædende typer af sager.

3.2.1. Piratkopiering

Klager over piratkopier udgjorde langt den største andel af de sikkerhedshændelser, DKCERT behandlede i 2016: 81 procent af hændelserne bestod af henvendelser fra indehavere af ophavsretten, der klagede over misbrug (se Figur 3). Det handler typisk om kopiering af spillefilm og episoder fra populære tv-serier.

3.2.2. Spam

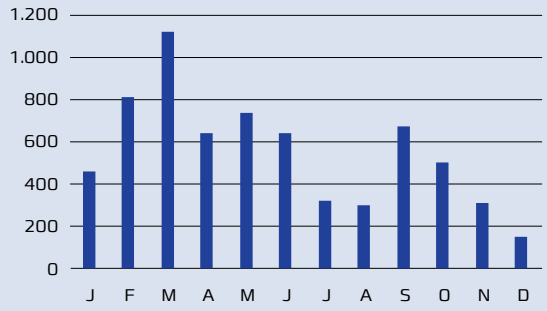
Klager over spam var de næstmest udbredte, de udgjorde 13 procent af klagerne. DKCERT tager kun imod klager over e-mails med uønskede reklamer, hvis de er udsendt via servere på forskningsnettet. Størstedelen af klagerne kom på to dage i januar, hvor en enkelt kompromitteret server havde udsendt en stor mængde spam. 780 ud af årets samlede mængde på 1.085 klager kom i de to dage (se Figur 4).

3.2.3. Portscanninger

Portscanninger er forsøg på at opdage, om en computer svarer på opkald fra internettet. Dermed er de ikke i sig selv skadelige, men de kan indgå i forberedelsen af et angreb. Portscanninger og lignende rekognosceringsforsøg udgjorde tre procent af de anmeldte hændelser (se Figur 5).

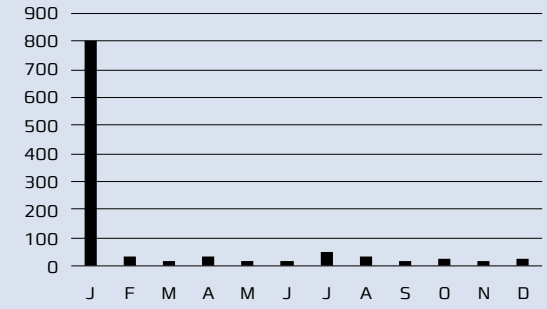
Figur 3: Download af piratkopier

Mængden af klager over piratkopiering er lavest i sommerferien og juleferien.



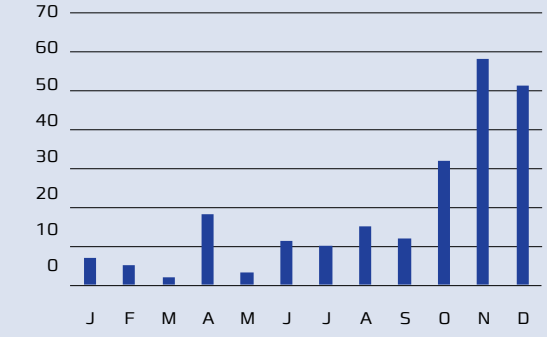
Figur 4: Spam

Hovedparten af klagerne over spam kom i løbet af to dage i januar.



Figur 5: Portscanninger

Mængden af portscanninger steg i sidste kvartal



3.2.4. Uautoriseret adgang

DKCERT opdeler hændelser om uautoriseret adgang til it-systemer i tre undertyper: Forsøg på at få adgang, kompromitterede systemer og systemer, der potentielt kan overtages, fordi de er sårbare.

Der var 110 sager om forsøg på adgang, 82 om sårbare systemer, og kun 17 sager med kompromitterede systemer (se Figur 6).

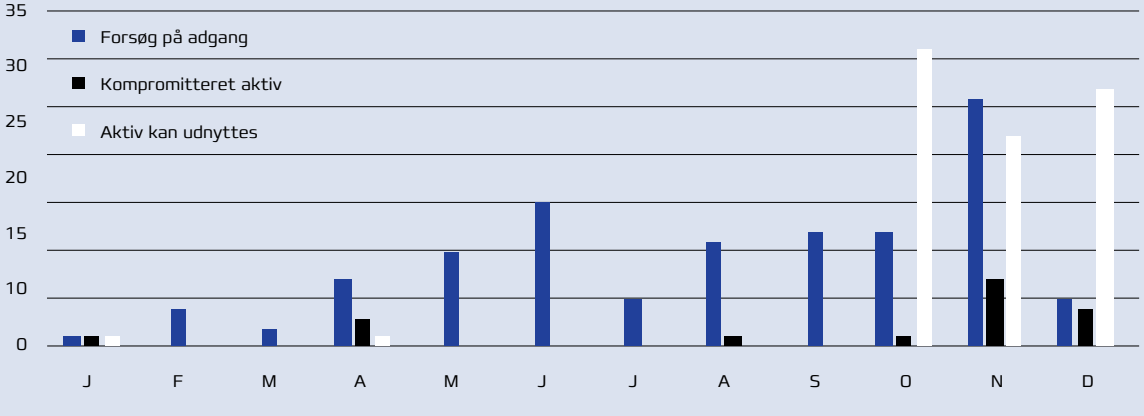
Tallene er næppe repræsentative. I langt de fleste tilfælde, hvor et it-system bliver overtaget, tager it-afdelingen på den pågældende institution sig af sagen uden at involvere DKCERT. Typisk hører DKCERT kun om sager, hvor en kompromitteret maskine bruges til at angribe andre computere på nettet.

3.2.5. Øvrige typer

Foruden de nævnte typer af sikkerhedshændelser har DKCERT behandlet nogle få sager om phishing, virusinfektioner og overtrædelse af regler. Der var også 19 sager om computere, der indgik i DDoS-angreb.

Figur 6: Uatoriseret adgang

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



3.3. ADVARSLER FORDELT PÅ TYPER

DKCERTs samarbejdspartnere scanner løbende internettet for potentielt sårbare systemer. DKCERT modtager advarsler om de systemer, der findes på forskningsnettet, og sender dem videre til de ansvarlige for de pågældende dele af netværket.

Mængden af advarsler svarer ikke til mængden af sårbare systemer. Hvis en scanning finder et sårbart system, og systemet ikke bliver opdateret i de følgende to uger, vil det optræde ti gange i statistikken.

En institution kan vælge ikke at få advarsler om et bestemt system. Det kan fx ske, hvis man ved, at et system er sårbart, men at det først kan blive opdateret efter en måned.

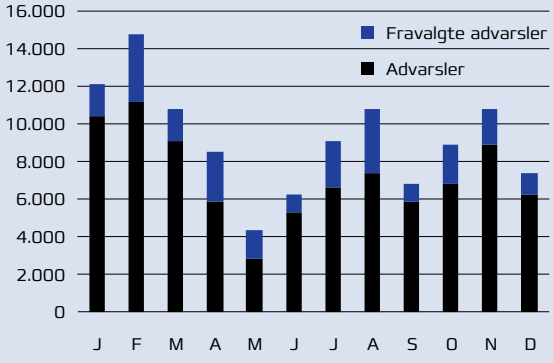
I alt udsendte DKCERT 86.993 advarsler i 2016. Hertil kommer 23.749 advarsler, som ikke blev udsendt, fordi institutionerne havde fravalgt dem. Potentielt kunne der altså være udsendt 110.742 advarsler (se Figur 7).

I det følgende gennemgår vi de typer advarsler, der har været flest af. En leverandør af advarsler havde tekniske problemer i maj, så derfor er der generelt få advarsler i den måned.

Tre sårbarhedstyper tegnede sig for tre ud af fire advarsler, DKCERT udsendte: POODLE, NTP og MDNS (se Figur 8).

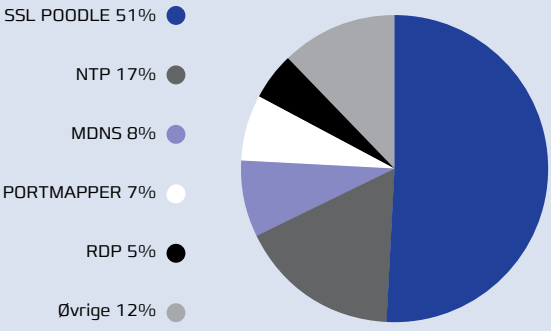
Figur 7: Advarsler om sårbare systemer

DKCERT kunne have udsendt 110.742 advarsler om sårbare systemer, men 23.749 advarsler blev fravalgt af institutionerne.



Figur 8: Advarsler

Tre advarselstyper står for tre fjerdedele af alle udsendte advarsler.



3.3.1. POODLE-sårbarhed

Godt halvdelen af alle advarsler handlede om systemer, der havde sårbarheden POODLE (Padding Oracle On Downgraded Legacy Encryption). Det er en sårbarhed i behandlingen af SSL-kryptering (se Figur 9). Der blev udsendt flest advarsler i første kvartal og færre sidst på året.

DKCERT mener

Udviklingen hen over året tyder på, at de systemansvarlige har opdateret en række systemer, der havde POODLE-sårbarheden.

3.3.2. NTP (Network Time Protocol)

Advarsler om åbne NTP-servere udgjorde 17 procent. NTP-servere bruges til at indstille tiden på computere. Nogle NTP-servere er indstillet til at svare på alle opkald, de modtager. Det kan angribere udnytte til DDoS-angreb: De sender en mængde forespørgsler med forfalsket afsenderadresse. NTP-serverne sender svar til afsenderadressen, der bliver overbelastet af de mange svar, den ikke har bedt om.

Også her var der flest advarsler i første kvartal, hvorefter mængden faldt væsentligt (se Figur 10).

3.3.3. MDNS (Multicast DNS)

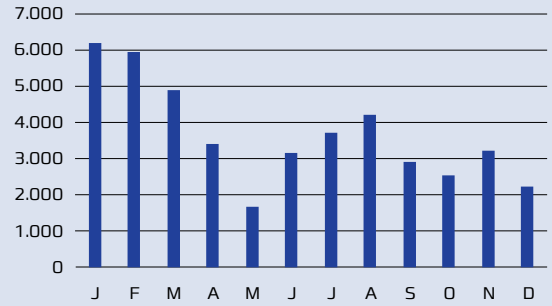
MDNS (Multicast DNS) gør det enkelt at lade enheder på et netværk opdage hinanden. Det fungerer i princippet ligesom DNS (Domain Name System), men uden en central server. I stedet sendes forespørgsler om et domænenavn ud til alle på det lokale netværk.

Teknologien indebærer samme sikkerhedsproblem som åbne NTP-servere: Hvis en computer svarer på mDNS-forespørgsler ude fra internettet i stedet for kun det lokale net, kan det misbruges til DDoS-angreb. Angriberen forfalsker afsenderadressen, der modtager en række uønskede svar på spørgsmål, den ikke har stillet.

Vi begyndte først at modtage advarsler om åbne mDNS-enheder i februar, derfor blev der ikke udsendt advarsler i januar. På en typisk måned udsendte vi 600 advarsler, mængden var konstant i årets løb (se Figur 11).

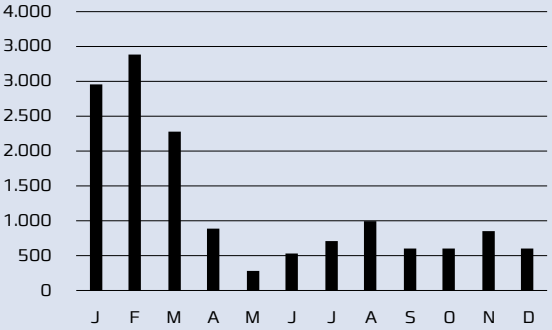
Figur 9: SSL POODLE

Halvdelen af advarslerne handlede om POODLE-sårbarheden.



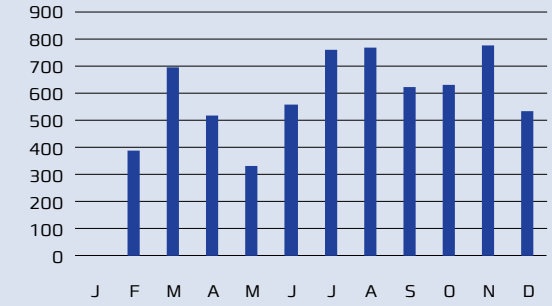
Figur 10: NTP

Der var flest åbne NTP-servere i første kvartal.



Figur 11: MDNS

Advarsler om åbne mDNS-enheder lå stabilt i sidste halvdel af 2016.



3.3.4. Portmapper

RPC Portmapper er en opslagstjeneste, der bruges i forbindelse med RPC (Remote Procedure Call). Den kan misbruges til DDoS-angreb med forfalsket afsenderadresse.

I første kvartal udsendte DKCERT 1.810 advarsler om åbne Portmapper-tjenester, i fjerde kvartal faldt mængden til 1.387 advarsler (se Figur 12).

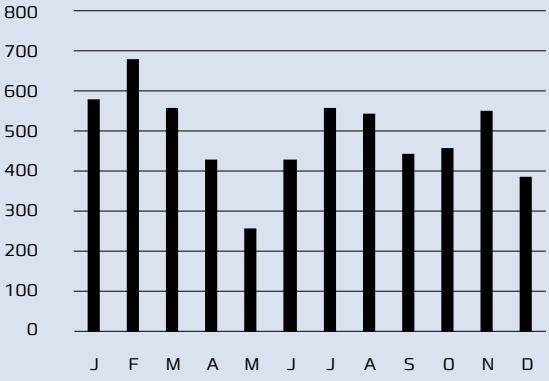
3.3.5. RDP (Remote Desktop Protocol)

RDP gør det muligt at koble sig til en Windows-computer og fjernstyre den over nettet. Dermed udgør protokollen en sikkerhedsrisiko, hvis den bruges over internettet: En angriber skal kun gætte et brugernavn og password for at få adgang til en computer. Endvidere blev der i 2012 opdaget en alvorlig sårbarhed i RDP under Windows, som kan bruges til at angribe computere der ikke er opdateret.

DKCERT begyndte først at modtage advarsler om RDP-servere, der stod åbne mod internettet, i september (se Figur 13). Hvis der havde været lige så mange advarsler i de øvrige kvartaler som i fjerde kvartal, ville RDP være den næstmest udbredte sårbarhedstype efter POODLE. Til gengæld faldt mængden hurtigt med en halvering fra oktober til december.

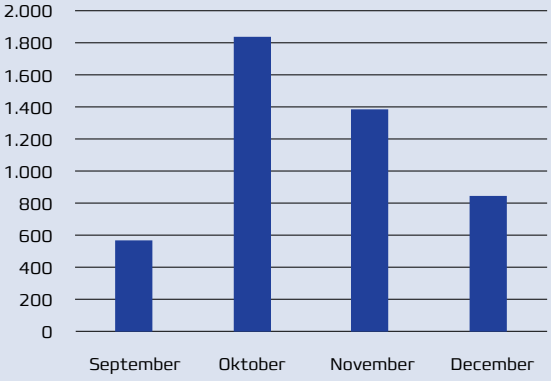
Figur 12: Portmapper

Advarsler om åbne Portmapper-systemer faldt fra første til fjerde kvartal.



Figur 13: RDP

Mængden af åbne RDP-servere faldt i løbet af fjerde kvartal.



3.4. MALWARE-UDVIKLINGEN

Langt de fleste skadelige programmer er fortsat trojanske heste. Det fremgår af statistikker fra sikkerhedsfirmaet F-Secure over de trusler, firmaets produkter har standset hos danske kunder.

89 procent af truslerne var trojanske heste (se Figur 14). I 2015 var andelen 84 procent. På andenpladsen kom exploits – det er programmer, der udnytter kendte sårbarheder. De udgjorde seks procent mod 11 procent året før.

Den mest udbredte trussel i Danmark i 2016 kalder F-Secure 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. Kavala blev i snit fundet hos 37 ud af 10.000 brugere.

Nummer to på topti-listen er Trojan:W97M/MaliciousMacro. Navnet dækker over flere forskellige trusler, der spredes via Microsoft Word-dokumenter. Den skadelige kode har form af en makro.

På tredjepladsen ligger Locky, der er et ransomware-program.

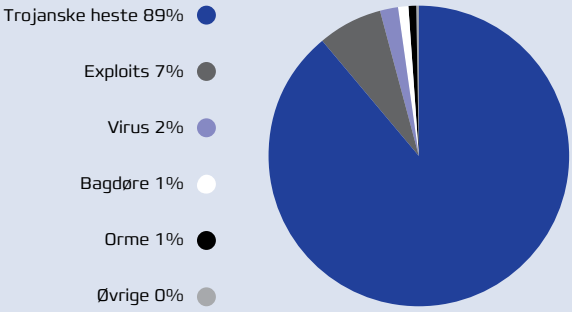
3.5. DEFACEMENTS

Ved et defacement-angreb overtager en hacker et websted og placerer sit eget indhold på det. Mange angreb er masseangreb, hvor flere websteder på det samme webhotel bliver overtaget i et hug.

Frem til 2011 blev danske domæner ofte angrebet. Siden er mængden faldt til mellem 3.000 og 6.000 om året. I 2016 var der således 3.585 angreb ifølge statistikwebstedet Zone-H (se Figur 16).

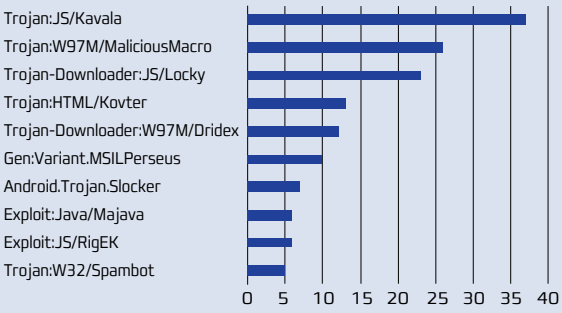
Figur 14: Malware i Danmark

Skadelig software fordelt på trusselstyper.
Kilde: F-Secure.



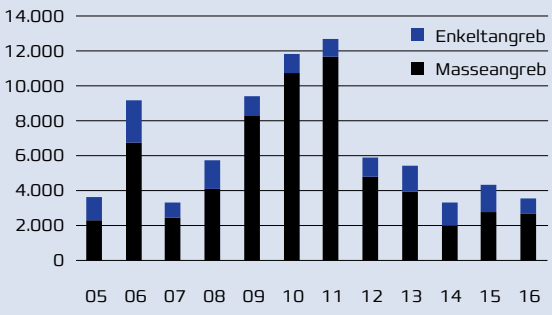
Figur15: Top ti over trusler

Top ti over de mest udbredte skadelige programmer.
Kilde: F-Secure.



Figur 16: Defacements på dk-domæner

Defacements på dk-domæner 2005-2016.
Kilde: Zone-H.



3.6. BORGERES OG MEDARBEJDERES INFORMATIONSSIKKERHED

På vegne af Digitaliseringsstyrelsen gennemførte DKCERT i efteråret en undersøgelse af informationssikkerheden hos tre befolkningsgrupper: Offentligt ansatte, medarbejdere i det private erhvervsliv og private borgere. Resultatet blev offentliggjort i rapporten "Danskernes informationssikkerhed 2016" i foråret 2017[1]. DKCERT har siden 2013 udført lignende undersøgelser, men de tidligere så kun på forholdene for private borgere.

Undersøgelsen viser, at danskerne er blevet lidt bedre til at tage sikkerhedskopi af data på deres pc'er: 40 procent gør det jævnligt, hvor tallet tidligere lå på 38-39 procent. Kun 30 procent tager backup af data på deres smartphone eller tablet-computer, det er lidt færre end året før (se Figur 17).

Dermed risikerer over halvdelen af danskerne at miste deres personlige dokumenter, feriebilleder og andre data, der ligger på deres pc eller telefon.

Otte procent af medarbejderne i undersøgelsen har oplevet at miste data som følge af manglende backup. Dermed ser manglende sikkerhedskopiering ud til også at være et problem i det offentlige og i det private erhvervsliv.

En sikkerhedskopi er uundværlig, hvis man bliver udsat for en af de mest ubehagelige trusler mod informationssikkerheden: Ransomware. Disse skadelige programmer krypterer offerets data og kræver løsepenge for at frigive den nøgle, der skal bruges til at dekryptere dem. Otte procent af de private borgere og seks procent af medarbejderne har været ramt af ransomware (se Figur 18).

Ud af de ramte fik mellem seks og otte procent ikke deres data tilbage. Ingen af de ansatte betalte løsesum. Det gjorde nogle borgere: Tre procent af de ramte betalte løsesummen og fik data tilbage, mens knap en procent betalte uden at få noget ud af det.

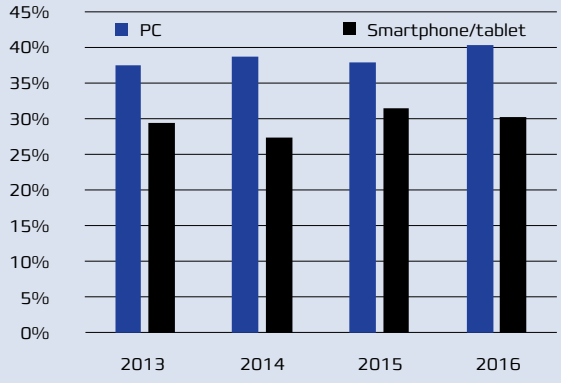
Vi spurgte medarbejderne i undersøgelsen om deres kendskab til arbejdspladsens it-sikkerhedspolitik. 48 procent af de offentligt ansatte og 57 procent af de privatansatte har sat sig ind i sikkerhedspolitikken. Men seks procent af de offentligt ansatte og ni procent af de privatansatte undlader indimellem at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet.

Ud af dem, der indimellem undlod at overholde reglerne, gjorde tre procent af de offentligt ansatte og 13 procent af de privatansatte det hver dag. For de fleste sker det sjældnere end en gang om måneden.

[1] DKCERT/Digitaliseringsstyrelsen: Danskernes informationssikkerhed 2016, https://www.cert.dk/information/borgernes_informationssikkerhed

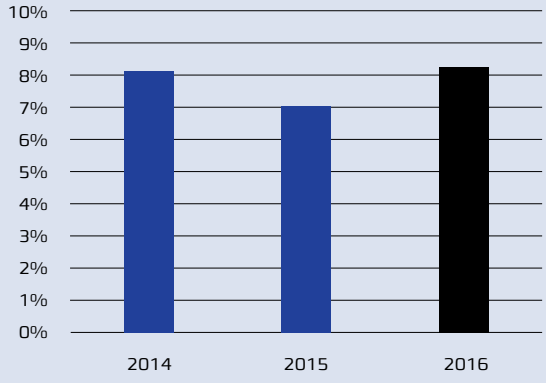
Figur 17: Sikkerhedskopiering af enheder

40 procent tager sikkerhedskopi af data på deres pc og 30 procent af data på smartphone eller tablet-computer.



Figur 18: Ofre for ransomware

Otte procent af borgerne har været ramt af ransomware.



3.7. ÅRETS SÅRBARHEDER

USA's National Vulnerability Database registrerede 6.449 nye sårbarheder i 2016. Det er en smule færre end i 2015.

Fordelingen ud fra risiko var stort set som i 2015: 10 procent udgjorde en lav risiko, 52 procent lå i midten, mens 38 procent udgjorde en høj risiko (se Figur 19).

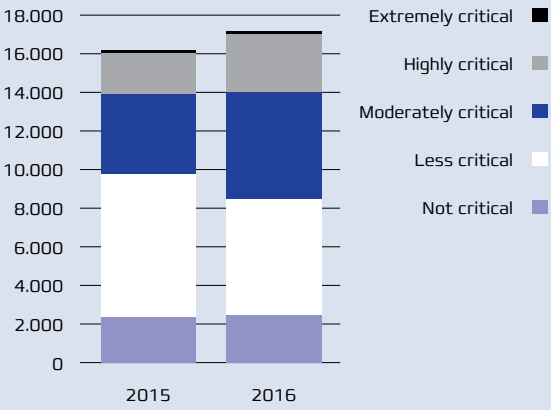
Tallene er ikke nødvendigvis udtryk for, at mængden af sårbarheder har stabiliseret sig. Firmaet MITRE, der driver National Vulnerability Database, blev i foråret 2016 kritiseret for ikke at kunne følge med, når det gælder udstedelse af CVE-numre. Et alternativt system ved navn Distributed Weakness Filing (DWF) System blev sat i drift.

Sårbarhedslaboratoriet Secunia Research fra firmaet Flexera Software følger også med i sårbarheder. Her talte man antallet af nye sårbarheder i 2016 til 17.147[2]. Det er seks procent flere end i 2015 (se Figur 20). Sårbarhederne var fordelt på 2.136 applikationer fra 246 producenter. Også her kan det reelle antal sårbarheder være højere, idet firmaet koncentrerer sig om de produkter, dets kunder bruger.

[2] Flexera Software: Vulnerability Review 2017, ret link til https://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/

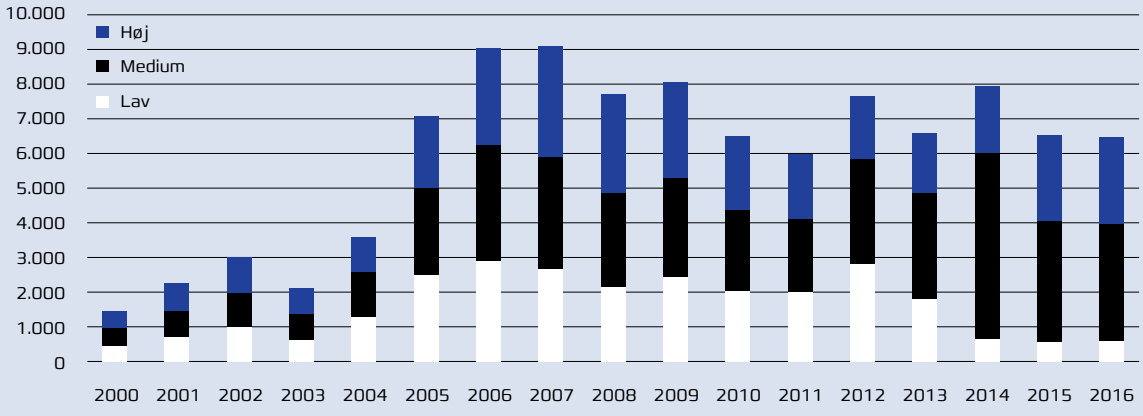
Figur 20: Sårbarheder efter risikovurdering

Sårbarheder registreret af Flexera Software.



Figur 19: Sårbarheder i NVD

Sårbarheder pr. år registreret i USA's National Vulnerability Database.



3.8. SÅRBARHEDSSCANNINGER

DKCERT scannede over en halv million IP-adresser i årets løb. Det er 162 procent flere end i 2015. Mange adresser blev scannet flere gange. 7.093 adresser svarede på scanningen og blev undersøgt for sårbarheder (se Figur 21).

Vi fandt sårbarheder på 1.964 adresser eller 27,7 procent af de adresser, der svarede. I 2015 var der sårbarheder på 26 procent af de adresser, der svarede. En sårbarhed kan være talt med flere gange, hvis IP-adressen blev scannet flere gange, uden at sårbarheden var blevet fjernet mellem scanningerne.

I gennemsnit blev der fundet 7,6 sårbarheder på hver af de sårbare IP-adresser. I 2015 var tallet 8,4.

Langt de fleste sårbarheder udgjorde en mindre alvorlig risiko. 25 procent var risikovurderet til lav, 69 procent til middel. Kun fire procent udgjorde høj risiko, mens to procent var kritiske (se Figur 22).

Antallet af forskellige sårbarheder blev halveret: Scanningerne afdækkede 267 forskellige CVE-numre (Common Vulnerabilities and Exposures) mod 542 i 2015.

En stor del af sårbarhederne handlede om problemer med kryptering. Det fremgår også af toptilisten over de kritiske sårbarheder (se Tabel 1), hvor SSH (Secure Shell) og SSL (Secure Sockets Layer) eller TLS (Transport Layer Security) optræder flere gange.

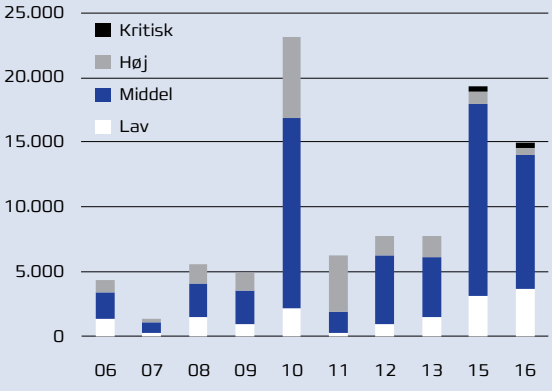
Tabel 1: Kritiske sårbarheder

Topti over de mest kritiske sårbarheder, som DKCERTs scanninger fandt.

1. SSH Server CBC Mode Ciphers Enabled
2. SSH Weak MAC Algorithms Enabled
3. SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
4. SSL RC4 Cipher Suites Supported (Bar Mitzvah)
5. Web Server Transmits Cleartext Credentials
6. Web Server Uses Basic Authentication Without HTTPS
7. OpenSSL AES-NI Padding Oracle MitM Information Disclosure
8. SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
9. FTP Supports Cleartext Authentication
10. SSL Anonymous Cipher Suites Supported

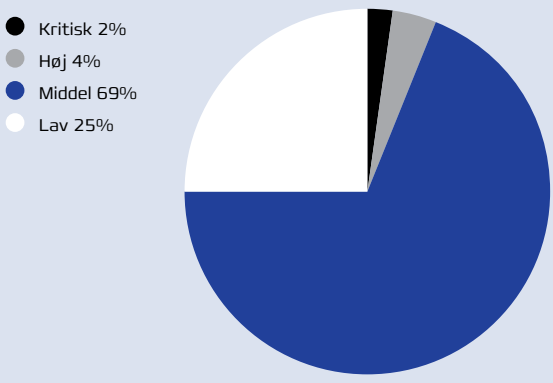
Figur 21: Sårbarheder efter risikovurdering

DKCERT fandt 23 procent færre sårbarheder i 2016 end i 2015.



Figur 22: Risikovurdering 2016

De fleste sårbarheder var mindre alvorlige.



4. 2016 – året i ord

DKCERT forberedte en tjeneste med dataanalyse i et år med store datalækager og DDoS-angreb.

4.1. DKCERTS AKTIVITETER I ÅRETS LØB

4.1.1. Information om sikkerhed

DKCERTs websted blev opdateret med nyheder om informationssikkerhed næsten dagligt. Mængden af modtagere af DKCERTs ugentlige nyhedsbreve steg 11 procent til 1.348 abonnenter. Antallet af følgere på Twitter steg 45 procent til 1.575 personer.

Henrik Larsen optrådte jævnligt i medierne som ekspertkilde inden for informationssikkerhed. Computerworld bringer hver måned en klumme af Henrik Larsen om aktuelle emner inden for sikkerhedsområdet.

På vegne af Digitaliseringsstyrelsen udarbejdede DKCERT i efteråret en undersøgelse af kendskabet til informationssikkerhed hos offentligt ansatte, privatansatte og borgere. DKCERT udarbejdede en række spørgsmål, som Danmarks Statistik stillede til et repræsentativt udvalg af befolkningen. Rapporten udkom i foråret 2017 (se afsnit 3.6).

4.1.2. DKCERT-CAB

DKCERT-CAB (Change Advisory Board), der giver råd og indstillinger til DeiCs bestyrelse vedrørende udvikling og drift af DKCERT, holdt fire møder i 2016. I årets løb udtrådte Henrik Rask fra Aalborg Universitet på grund af jobskifte. Nyt medlem blev informationssikkerhedschef Poul Halkjær Nielsen, Københavns Universitet (indstillet af CISO-forum).

4.1.3. Dataanalyse

DKCERT-CAB har anbefalet, at DKCERT udvikler nye tjenester. En af dem bliver en tjeneste til analyse af netværksdata med henblik på at afdække nye angrebsmønstre og opdage angreb, der ellers ikke ville blive registreret.

Projektet blev igangsat som pilotprojekt med en diplomingeniørpraktikant i fem måneder. Praktikperioden var meget succesfuld og førte til gode erfaringer, der danner grundlaget for at sætte en tjeneste i produktion. Praktikanten er fortsat som timelønnet studentermedhjælp og arbejder videre med projektet.

4.1.4. Fremtidige tjenester

Andre planlagte tjenester omfatter konsulentbistand i forbindelse med EU's databeskyttelsesforordning. Tjenesten planlægges at omfatte koordinering af institutionernes arbejde med overholdelse af forordningen, oplysning om behandling af persondata i forskningen, deponering af krypteringsnøgler ved pseudonymisering af personhenførbare forskningsdata, samt facilitering af netværk for institutionernes databeskyttelsesrådgivere (DPO'er). Endvidere vil tjenesten kunne indeholde en datarådgivertjeneste, som institutionerne vil kunne abonnere på, i det omfang de ikke ønsker at udpege deres egen datarådgiver. Der er bevilget midler til igangsætning af denne tjeneste, som efterfølgende vil blive tilbudt som en ekstra tjeneste mod betaling.

En anden mulig tjeneste i fremtiden kunne være konsulentbistand ved indføring af styring af sikkerhedsarbejdet efter ISO 27001-standarden.

4.1.5. Internationalt samarbejde

DKCERT deltager i jævnlige videomøder med de øvrige nordiske forskningsnet-CERT'er samt NORDUnet-CERT. Henrik Larsen deltager i GÉANT's SIG-ISM (Special Interest Group – Information Security Management). Sammen med en repræsentant for UNINETT (Norge) og en for SURFNET (Holland) holdt han et fælles indlæg på NORDUnet-konferencen i september om arbejdet i SIG-ISM. Henrik Larsens indlæg handlede om erfaringerne fra DeiCs igangværende ISO 27001-projekt.

DKCERT er siden 2002 akkrediteret medlem af den europæiske sammenslutning af sikkerhedsteams, Trusted Introducer/TF-CSIRT. DKCERT-medarbejderne Bjarne Schacht, Tonny Bjørn og Henrik Larsen har deltaget i sammenslutningens møder i årets løb. Endvidere er DKCERT fuldt medlem af FIRST (Forum of Incident Response and Security Teams), en international organisation for sikkerhedsteams. Henrik Larsen deltog i FIRST's konference i Seoul, Sydkorea.

Bjarne Schacht har taget TF-CSIRT's Transits II-uddannelse for CERT-medarbejdere. Han og Henrik Larsen deltog sammen med diplomingeniørpraktikant Simon Nexø Jensen i et seminar i Prag om dataanalyse arrangeret af den tjekkiske forskningsnet-CERT. Viden herfra indgik i udformningen af DKCERTs kommende dataanalysetjeneste.

På vegne af Danske Universiteters CISO-forum (Chief Information Security Officer) arrangerede DKCERT en rundtur til EU's databeskyttelseskontor i Generaldirektoratet for Retsvæsen og Forbrugerforhold, Bruxelles, samt til europæiske CERT-organisationer og informationssikkerhedschefer fra universiteterne i de respektive lande. Turens tema var databeskyttelsesforordningen.

Gruppen besøgte blandt andre det belgiske forskningsnet Belnet, Luxembourgs GovCERT og forskningsnet-CERT, RESTENA-CERT, samt det tyske forskningsnets DFN-CERT. Her hørte deltagerne blandt andet om erfaringerne med at lade flere universiteter deles om en databeskyttelsesansvarlig. Erfaringerne herfra indgår i planlægningen af en kommende DKCERT-tjeneste med konsulentydelser vedrørende databeskyttelsesforordningen.

4.2. TENDENSER OG TRUSLER

4.2.1. Truslen fra IoT blev virkelig

Mirai-botnettet er et netværk af digitale videooptagere og overvågningskameraer. Bagmændene udnytter netværket til DDoS-angreb (Distributed Denial of Service), hvor tusindvis af apparater på samme tid sender angrebspakker mod offeret. I efteråret blev Mirai anvendt i et angreb på sikkerhedsreporter Brian Krebs' websted[3]. Angrebet nåede en båndbredde på 620 Gbit/s, hvilket var rekord for DDoS-angreb på det tidspunkt. Mirai menes også at have indgået i et stort angreb på DNS-udbyderen Dyn[4].

Med angrebene fra Mirai blev truslen fra Internet of Things (IoT) konkret. Sikkerhedseksperter har i årevis advaret om risikoen ved, at meget internet-opkoblet udstyr har for dårlig sikkerhed. For eksempel kan apparaterne være udstyret med standardbrugernavn og -password, så det er let for angribere at hacke sig ind på dem. Den indbyggede software kan være sårbar, og det er vanskeligt for forbrugerne at opdatere den.

DKCERT mener

Angreb på og ved hjælp af IoT-udstyr viser, at truslen er reel. Der er brug for større fokus på sikkerheden hos både producenter, forhandlere og brugere.

4.2.2. Afpresning på mange måder

Pengeafpresning er fortsat en populær metode hos de it-kriminelle. I 2016 har vi især set det på to fronter: Ransomware og DDoS-afpresning. Ransomware er en afart af skadelig software. Tidligere tiders virus ødelagde data uden noget økonomisk motiv. Ransomware krypterer brugerens data og kræver en løsesum for at frigive nøglen, der bringer data tilbage.

Det er blevet let at udgive ransomware. Selv kriminelle uden større teknisk indsigt kan købe gør-det-selv-sæt på nettet, der gør det let at fremstille og udsende ransomware.

I juli lancerede Europol webportalen NoMoreRansom.org, der har til formål at hjælpe ofre for ransomware[5]. Siden har sikkerhedsfirmaer løbende lagt værktøjer ud på portalen, som ofre kan bruge til at dekryptere data med.

Afpresning med trusler om at lægge et websted ned har været kendt i flere år. Også her er det blevet enklere at være kriminel: Man behøver ikke længere selv udvikle et botnet-program og distribuere det. I stedet kan man købe adgang til et botnet og starte angreb efter behov.

I foråret kom der en række trusler om DDoS-angreb. Afsenderen var angiveligt Armada Collective, der stod bag angreb i 2015. Der kan dog være tale om andre, der efterligner dem. Blandt ofrene var en række schweiziske banker og pengeinstitutter[6].

DKCERT mener

Truslen fra ransomware illustrerer behovet for sikkerhedskopiering: Har man en sikkerhedskopi, kan man gendanne data fra den i stedet for at betale løsesummen. Især private borgere er imidlertid ikke gode til at tage backup.

4.2.3. Lækager af persondata

Lækager af gigantiske mængder persondata var i overskrifterne flere gange i 2016. De største stammede fra angreb, der foregik flere år tidligere, men hvor omfanget først blev offentligt kendt i 2016. Det hang typisk sammen med, at kriminelle satte dataene til salg.

Yahoo mistede således data om en halv million brugere i 2014. Senere kom det frem, at et angreb i 2013 førte til data om over en milliard brugere af tjenesten.

Data om 117 millioner brugere af LinkedIn blev sat til salg i maj. De stammede fra et angreb i 2012.

[3] Brian Krebs: KrebsOnSecurity Hit With Record DDoS, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[4] Flashpoint: Mirai Botnet Linked to Dyn DNS DDoS Attacks, https://www.flashpoint-intel.com/mirai-botnet-linked-dyn-dns-ddos-attacks/

[5] Europol: No More Ransom: law enforcement and IT security companies join forces to fight ransomware, https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware.

[6] GovCERT.ch: Armada Collective is back, extorting Financial Institutions in Switzerland, https://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland.

Knap 360 millioner data om MySpace-brugere menes at stamme fra 2008 eller 2009. De blev også sat til salg i 2016.

Også det russiske sociale netværk VK, der tidligere hed Vkontakte, blev ramt. Brugernavne og passwords for 100 millioner brugere kunne købes på nettet. En analyse viste, at over 700.000 af passwordene var "123456".

DKCERT mener

Flere af lækagerne er flere år gamle. I de tilfælde hvor tjenesterne kendte til angrebene, har de sørget for at nulstille brugernes passwords. Dermed er der kun lille risiko for, at et gammelt password kan bruges på den tjeneste, det hører til.

Men hvis brugeren har brugt samme password sammen med samme brugernavn på andre tjenester, er risikoen større. Så kan angribere gå i gang med at afprøve kombinationerne fra lækagerne på andre tjenester, indtil der er gevinst.

Derfor anbefaler DKCERT, at man ikke genbruger passwords på tværs af tjenester.

4.2.4. Politisk hacking

Valgkampen i USA var præget af hackerangreb. En hacker, der kaldte sig Guccifer 2.0, tog ansvaret for et angreb, der fik fat i godt 19.000 e-mails fra Democratic National Committee, der er den øverste ledelse af det demokratiske parti[7]. Wikileaks offentliggjorde i juli meddelelserne, der blandt andet afslørede interne detaljer om behandlingen af kandidaterne Hillary Clinton og Bernie Sanders. Senere på året offentliggjorde Wikileaks også e-mails fra John Podesta, der var formand for Hillary Clintons kampagne[8]. De menes at være hacket af gruppen Fancy Bear, der er tilknyttet en russisk efterretningstjeneste.

Amerikanske efterretningstjenester er overbevist om, at Rusland står bag angrebene. Formålet skulle være at påvirke folkestemningen op til præsidentvalget, så Ruslands foretrukne kandidat, Donald Trump, skulle få bedre chancer for at vinde.

DKCERT mener

Hackerangrebene under den amerikanske præsidentvalgkamp illustrerer, at it-kriminalitet kan indgå aktivt i en politisk kamp. Det stiller øgede krav til sikkerheden hos personer og organisationer, der er involveret i det politiske liv: De skal være opmærksomme på truslen og træffe de nødvendige forholdsregler.

[7] Wikipedia: 2016 Democratic National Committee email leak, https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak.
[8] Wikipedia: Podesta emails, https://en.wikipedia.org/wiki/Podesta_emails.

5. Det eksterne perspektiv

Fire bidragydere uden for DKCERT giver her deres syn på sikkerhedsproblematikker i forbindelse med Internet of Things (IoT).

Internet of Things (IoT) er fællesbetegnelsen for alle de apparater på internettet, der ikke er traditionelle computere. Det kan være overvågningskameraer, routere, alarmsystemer og andet udstyr, der er forsynet med en IP-adresse.

Apparaterne udgør ofte et sikkerhedsproblem. Det skyldes flere faktorer:

- Brugerne ved ikke, hvordan de skal opdatere den indbyggede software, når der kommer sikkerhedsrettelser.
- Producenterne udstyrer ofte apparaterne med usikker eller fejlbehæftet software. Mange producenter udsender ikke sikkerhedsopdateringer.
- Det kan være fysisk vanskeligt at komme til apparaterne, når de først er sat i drift.

DKCERT har bedt fire bidragydere give deres bud på, hvordan vi får styr på sikkerheden både i og med IoT-apparaterne. Shehzad Ahmad fra Nets skriver om IoT i fremtidens betalinger, Christian Wernberg-Tougaard skriver som formand for brancheforeningen IT-Branchens IT-sikkerhedsudvalg om IoT set med producentbriller, Christian Ehlers Mikkelsen fra Dansk IT's netværk om informationssikkerhed behandler skismaet mellem innovation og sikkerhed, og endelig fortæller lektor Christian Damsgaard Jensen, DTU Compute, hvordan IoT kan bruges til at øge informationssikkerheden.

5.1. IOT OG FREMTIDENS BETALINGER

AF INFORMATIONSSIKKERHEDSCHEF SHEHZAD AHMAD, NETS

Internet of Things: Alle taler om det, men færre ved, hvad det dækker over. De fleste ved dog, at i takt med digitaliseringen bliver alle de ting, vi omgiver os med, i større grad koblet sammen og integreret via internettet. Det giver os som forbrugere en masse fordele og muligheder, men i lige så stor udstrækning også en række udfordringer, som vi løbende skal forholde os til.

Nogle af disse fordele er nemlig kun fordele, hvis de kan individualiseres. Og derfor er det nødvendigt at afgive informationer, der adskiller os fra andre individer. F.eks. i form af betalinger. IoT-udviklingen stiller derfor også stigende krav til håndtering af disse informationer på en sikker måde. Det er komplekst, og der findes ikke en "silver bullet," der løser alle udfordringerne, uanset om man er forbruger, leverandør eller serviceudbyder.

5.1.1. Betalinger med smartphones er bare starten

Finanssektoren var en af de første brancher til at se mulighederne i digitalisering. Som årene er gået, er sektorens modenhed med hensyn til teknologianvendelse steget. I Danmark samler flere og flere betalinger sig omkring mobiltelefonen. I en ikke så fjern fremtid vil betalinger formodentlig også blive foretaget med ure, køleskabe, tv og andre elektroniske redskaber, som vi bruger i dagligdagen.

Betalinger med mobiltelefonen bygger på kendte teknologier som Bluetooth, Near Field Communication (NFC) og QR-koder. Der eksperimenteres også med udvikling af nye typer betalinger, der bygger på blockchain-teknologi, som blandt andet mange digitale valutaer, herunder Bitcoin, bygger på. Blockchain-betalinger kan køre helt uden om bankerne og dermed også uden om det traditionelle sikkerhedssetup omkring betalinger. Blockchain har en anden indbygget sikkerhed, der gør det muligt at identificere alle betalinger, der er foretaget med den pågældende digitale valuta. Men det kræver et andet setup og nye foranstaltninger for at sikre betalingerne.

5.1.2. Skal køleskabsproducenten håndtere betalingsinformation?

IoT åbner for helt nye muligheder i forhold til betalinger. På nuværende tidspunkt er det kun muligt at gisne om, hvilken betydning det kommer til at have for fremtidens betalinger. Men hvis vi tager udgangspunkt i de muligheder, som den globale udbredelse af smartphones har givet for betalinger på relativt kort tid, så bliver de kommende år meget spændende at følge.

I den forbindelse bliver kryptering af data den helt afgørende teknologi, der skal sikre transaktionen og dens fortrolighed. Den er allerede etableret, når betalinger foregår med betalingskort, men nye betalingsløsninger kræver naturligvis også stærk sikkerhed og forbrugerbeskyttelse.

En ting er de fordele, den teknologiske udvikling giver os i forhold til at betale med vores smartphone. I forhold til IoT ligger det nye i introduktionen af smartphonen (eller køleskabet) som den enhed, der i sammenhæng med en anden enhed eller dedikeret terminal hos den detailhandlende kan initiere transaktionen og sikre den helt tilbage til bankens systemer. Dermed er der skabt en "forsyningskæde" med potentiale til at ændre hele brancher, og for den sags skyld hele verden, til noget andet end det, vi ser i dag.

5.1.3. Nye spilleregler må ikke gå ud over sikkerheden

Når man flytter hele processen fra et "dumt" betalingskort og over til en "smart" enhed, som jo har masser af regnekraft og utallige andre funktioner, er det indlysende, at man risikerer at introducere både sårbarheder og nye veje ind til brugerens data, som ikke tidligere har været mulige. Smartphonen er jo blot en computer, hvor producenten har stor magt over, hvad netop deres enhed skal kunne, ligesom de står for dens basale sikkerhed. Det kan give producenten en uforholdsmæssig stor magt, men på den anden side også et stort ansvar. Et ansvar, som betalingssektoren og bankerne gennem mere end 30 år har været vant til at løfte. Respekt for den enkeltes privatliv og pengeforbrug har været omdrejningspunktet for både drift og udvikling.

Der er som sådan ingen grund til at tro, at det vil ændre sig. Og dog. Ændret EU-lovgivning vil fra 2018 gøre det muligt for andre virksomheder som f.eks. Apple, Microsoft og særligt Google at komme ind på markedet for betalinger. Der er fortsat strenge krav til sikkerhed, men der kommer flere aktører ind i forsyningskæden. Og det kan tænkes, at de vil forsøge at ændre spilleregler og standarder for, hvad man må bruge data til.

5.1.4. Sikkerhed må ikke bero på det svageste led

I de seneste knap 10 år har vi set en eksplosion af IT-kriminalitet, samtidig med at al anden kriminalitet er faldende. En naturlig følge af digitaliseringen.

Tendensen har været, at nye teknologier konstant er blevet udfordret af meget kompetente og kreative kriminelle, ofte uden for politiets rækkevidde. Dette har udviklet sig til kattens leg med musen, som aldrig står stille, og det er der ikke nogen grund til at forestille sig vil ændres. I en verden hvor forsyningskæderne bliver mere komplekse og meget længere, bliver den store udfordring at bevare overblikket og sikre, at det ikke bliver det svageste led i kæden, der afgør niveauet. Derfor er det i dag vigtigere end nogensinde, at alle led i kæden påtager sig et ansvar for deres egne produkters sikkerhed. Frivilligt eller via lovgivning.

5.2. NÅR DEN FJERDE REVOLUTION RAMMER OS

AF CHRISTIAN WERNBERG-TOUGAARD, FUJITSU,
FORMAND FOR IT-BRANCHENS IT-SIKKERHEDSUDVALG

Der pågår en revolution for tiden. Det er måske ikke en der skaber overskrifter, men det burde den. I Statsministeriet, hos World Economic Forum og OECD er man opmærksom på de voldsomme forandringer, som vi som samfund står overfor. Det er ikke en væbnet revolution eller en revolution, som vi mærker på vores dagligdag – endnu. For den vil få en ganske omfattende indflydelse på vores allesammens dagligdag om blot få år.

Den fjerde industrielle revolution, eller kort #IR4, er sammenkoblingen af mange forskellige teknologiske fremskridt, som tilsammen automatiserer, digitaliserer og effektiviserer alle dele af vores samfund. Som altid kendetegnes det af en række buzzwords – nøgleord, som er forkortelser, som for eksempel:

- **IoT (Internet of Things)** er tingenes internet: det forhold at alle tænkelige og utænkelige dimser og dingenoter kan snakke sammen og udveksle data.
- **AI (Artificial Intelligence)**, kunstig intelligens, som vil muliggøre automatiserede beslutninger gennem intelligent analyse af data.
- **AR (augmented reality)**, som kobler den analoge verden sammen med den digitale ved at projicere data gennem briller eller tablets.

Set fra IT-branchen er digital omstilling godt, men samtidig er vi meget bevidste om, at der er en række nye som gamle data- og it-sikkerhedsudfordringer, som vi bliver nødt til at tage medansvar for at løse. Fremtidens CPS (cyber-physical systems, cyber-fysiske systemer) vil gøre rigtig mange ting nemmere, enklere og hurtigere. Men – for der er et stort men – vi bliver nødt til i dag at tænke over, hvordan vi beskytter den komplekse, digitale infrastruktur, da vi vil være langt mere afhængige af det digitale i morgen end i dag.

I IT-branchens IT-sikkerhedsudvalg har vi derfor som ét af tre fokusområder valgt at sætte #IR4 på dagsorden. Vi vil sammen med andre gode udvalg i IT-branchen kigge på teknologiernes brug i specifikke sektorer, og de mulige problemstillinger som teknologierne skaber både etisk og data- og it-sikkerhedsmæssigt. Et par af de områder som personligt optager mig meget er, hvordan vi kan bruge fremtidens teknologier til at skabe mere velfærd i vores ældreomsorg, og hvordan vi kan bruge teknologi til at personalisere vores sundhedssektor.

Hvordan skal man for eksempel implementere RPA (Robot Process Automation) så man ikke kompromitterer de systemer, som softwarerobotten varetager? Og hvem holder øje med, hvem der kan ændre robottens algoritmer?

Hvordan sikrer man, at IoT-enheder, som er afgørende for fx rigtigheden af videnskabelige måledata, ikke kompromitteres eller forstyrres? Hvem har adgang til data fra fx en ældre medborgers wearables, som fortæller om puls, blodtryk, blodsukker, gangrytme og hvor vedkommende befinder sig?

Der er brug for, at de bedste tænkere – på tværs af industrier, offentlig sektor og faglige områder – overvejer, hvordan vi kan bygge et samfund, som udnytter de digitale muligheder fuldt ud uden at blive udsat for mere digital svindel, manipulation og udnyttelse. Der er ikke nogen nem vej – vi bliver nødt til at bruge alle de forskellige værktøjer i værktøjskassen; fra folkeoplysning og digitalt medborgerskab til uddannelse i folkeskolen og standardisering, til indlejring af privacy i de fremtidige digitale løsninger.

I IT-branchen er det vores ambition, at vi senere på året kan invitere til en åben debat om, hvordan vi som samfund i dag kan medvirke til, at vi får et mere sikkert "i morgen". Det er afgørende, at alle trækker på samme hammel for at skabe en effektiv og fornuftsbaseret tilgang til balance mellem digital innovation og beskyttelse af data og personlig information.

Fremtiden kræver, at vi handler nu. Kun gennem tvær-sektoral debat og med politisk mod til at understøtte forandringerne agilt kan vi skabe et trygt og data-sikkert samfund til glæde og gavn for alle borgere og virksomheder.

5.3. INNOVATION OG SIKKERHED – ET NØDVENDIGT SKISMA?

CHRISTIAN EHLERS MIKKELSEN, IMPLEMENT CONSULTING GROUP, MODERATOR FOR DANSK IT'S KOMPETENCENETVÆRK OM INFORMATIONSSIKKERHED

Internet of things - IoT - Internet of insecure things - industrial Internet of Things. Kært barn har mange navne, men uanset betegnelsen var 2016 endnu et år med en hastig vækst i udbredelsen af internetopkoblede enheder i form af sensorer og styringsenheder med og uden batterier, med direkte internetopkobling eller indirekte internetopkobling over forskellige netværk via forskellige producenters gateways ind i cloud-baserede tjenester.

Fælles for dem alle er, at producenter, serviceudbydere og brugere efter bedste evne forsøger at skabe værdi, ofte inden for et eller flere af områderne:

> Nye og forbedrede bruger- eller kundeoplevelser
  Eksempelvis styring af lamper og enheder i hjemmene, fjernaŰæsning af forbrugsmålere, styring og overvågning af alarmsystemer mv.
> Nye tjenester og forretningsmodeller
  Eksempelvis knapper til online genbestilling af forbrugsvarer, lærende legetøj, online sensorbaseret energimærkning af ejendomme, forebyggende vedligehold af vindmølleturbiner, biler mv.
> Effektivisering af eksisterende forretningsmodeller
  For eksempel sensorer der registrerer forbipasserendes smarte telefoner for at optimere vareudbud/tilbud, digitale prisskilte, måling af skraldespandes fyldningsgrad for at optimere tømning, smarte fugtsensorer i bygninger, dokumentation af buskørselsmønstre og rettidighed, Űådestyring osv.

IoT og sikkerhed er samtidig et fortræffeligt eksempel på, at historien gentager sig selv.

IoT er i fuld gang med en udvikling, som på mange måder ligner den, vi så for pc'er i starten af 1990'erne – det hele foregår nu bare i et voldsomt accelereret tempo.

Egentlig var det slet ikke nogen dårlig udvikling med pc'erne. Men der var nogle væsentlige faldgruber med globale vira, usikker softwareudvikling, opdateringsregimer mv.

De værste, som kostede menneskeliv og store nationale ressourcer, kunne måske være undgået eller kan nu forhåbentlig tjene som erfaring og inspiration til eftertiden. Et oplevet behov for innovation, vækst og forretningsudvikling friholder hverken producenter, politikere, løsningsleverandører eller forbrugere fra at udvise ansvarlighed.

Helt analogt til pc-verdenen halter sikkerheden for IoT-enheder på rigtig mange områder. I værste fald med direkte usikre standardopsætninger og i andre tilfælde "blot" med små detaljer som det, at producenten ikke understøtter en effektiv opgradering af softwaren i enhederne i takt med, at sikkerhedshuller opdages og publiceres.

Selv med mærkningskrav og standarder vil der være alvorlige svigt. Den næste front for dette er godt på vej til at blive batterilevetid og opgraderbarhed.

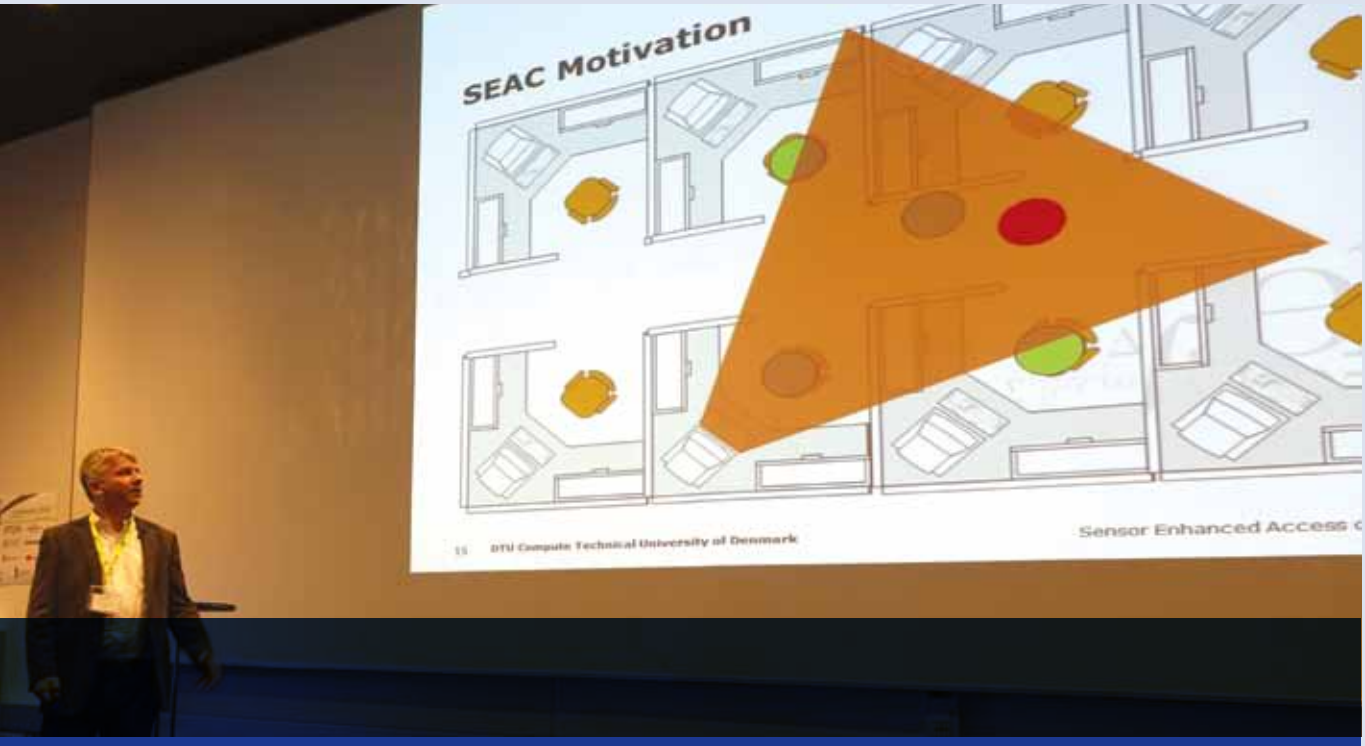
I øjeblikket baserer mange virksomheder sig på producenters løfter om, at deres produkter er fortræffeligt sikre. De indkøber i 100.000-vis af strøm-, vand- og varmemålere til installation i danske hjem. Samtidig skulle disse enheders levetid og batterilevetid angiveligvis være mere end 13 år.

Mange har oplevet skuffelsen med en "certificeret" fin ny el-sparepære, som skulle have holdt i mindst otte år, men endte med at holde 14 måneder – fordi producenten måske ikke lige havde kommunikeret, at levetiden forudsatte et dagligt forbrugsmønster med et begrænset antal tænd- og slukhændelser. Tilsvarende udfordringer ser vi allerede nu med batterier i flowmålere, termostater, nærværs-sensorer mv.

Når man anskaffer IoT-enheder, bør man afveje gevinster og risici nøje – og med afsæt i nedenstående liste gøre sig klart, hvad konsekvensen er hvis

- der ikke er en effektiv måde til regelmæssigt eller i nødsfald at softwareopdatere enhederne.
- (når) batterilevetiden viser sig at være det halve af det speciůcerede.
- en softwareopdatering forårsager en kraftig reduktion i batterilevetiden.
- alle fra nettet uhindret kan aŰæse eller modiůcere data fra en eller Űere sensorer.
- enheden kan kompromittere det netværk, den sidder på.
- brugere går sammen for at gøre ansvar gældende.
- enhederne ikke har den forventede levetid – hvad betyder det for business casen?
- fortsæt selv…

IoT, innovation og sikkerhed er ikke modsætninger, husk blot den sunde fornuft!



Christian Damsgaard Jensen demonstrerede ideen bag Persistent Authentication på DeiC konference 2016. På skærmen markerer de grønne cirkler godkendte personer, mens den røde cirkel er en uautoriseret person. Når den røde cirkel nærmer sig skærmen med fortrolig information, opdager sensorerne det, og skærmen går i sort.

5.4. KOBLING AF LOGISK OG FYSISK SIKKERHED MED SENSORER

AF LEKTOR CHRISTIAN DAMSGAARD JENSEN, DTU COMPUTE

"Internet of Things" eller IoT betegner en klasse af systemer, hvor sensorer, aktuatorer og beregningsenheder bygges ind i hverdagsobjekter, der kan kommunikere gennem internettet. Disse hverdagsobjekter er underlagt markedets krav om høj funktionalitet og lav pris, så sikkerhed har sjældent optrådt højt i kravspecifikationen, hvilket de mange historier om manglende sikkerhed i IoT-systemer i pressen gennem de senere år bevidner.

I det efterfølgende undersøger vi ikke sikkerhed i IoT, men i stedet den øgede sikkerhed vi kan opnå med IoT, det vil sige ved at indlejre små kommunikerende sensorer og aktuatorer i vore omgivelser.

Ved at indlejre forskellige sensorer i vore omgivelser eller interagere med sensorer folk normalt har med sig, f.eks. det arsenal af sensorer der er indbygget i moderne smartphones, kan man opbygge et situationsoverblik, der tillader et it-system at håndhæve sikkerhedspolitikker som vi mennesker, som sociale væsener, har svært ved at håndhæve. Eksempler på sådan maskinel håndhævelse af sikkerhedspolitikker er en elektronisk dørlås, der ikke låser op, før alle personer i den umiddelbare nærhed er autentificeret. Det forhindrer "tailgating," hvor uvedkommende følger med ind, når en ansat åbner døren). Et andet eksempel er et system, der ikke viser en login-boks, før der ikke er andre personer i den umiddelbare nærhed. Det forhindrer "shoulder surfing," hvor uvedkommende kigger folk over skulderen og ser fortrolig information på skærmen. Samme mekanisme kunne i øvrigt benyttes på dankortterminaler.

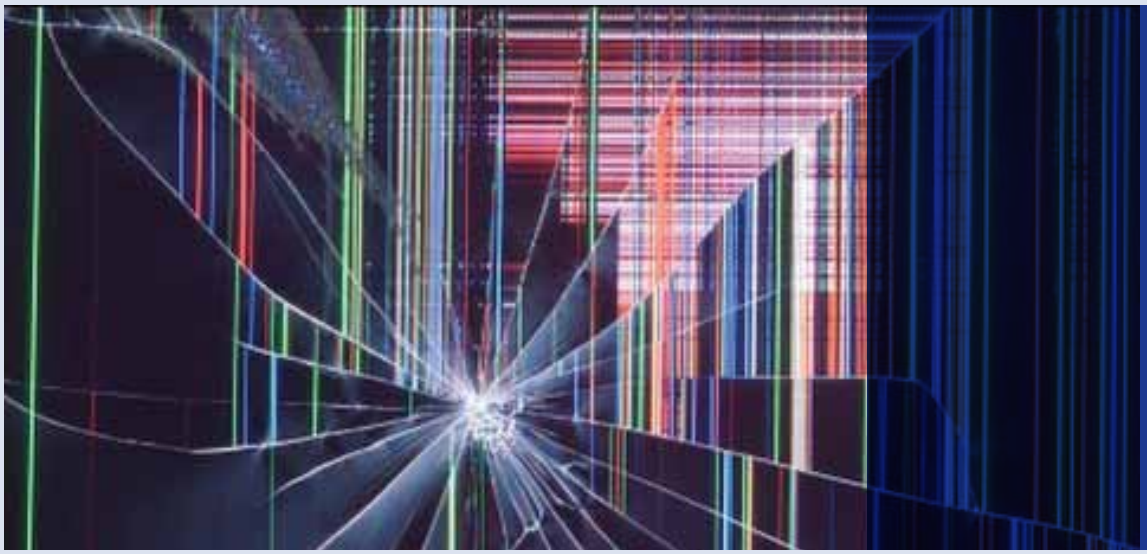
På DTU Compute arbejder vi blandt andet med "Persistent Authentication" (PA). Her følges allerede autentificerede personer med sensorer, f.eks. overvågningskameraer, så systemet til enhver tid ved, hvem der er hvor. Hvis denne information ikke lagres, får det begrænsede konsekvenser for per-

sonernes privathed. Det bagvedliggende system kan hermed automatisk autentificere personer i forhold til lokationsbestemte tjenester. For eksempel kan computerens loginmekanisme ændres, så brugeren automatisk logges på, når hun sætter sig foran den.

Systemet kan også integreres med bygningers øvrige sikkerhedssystem, der styrer alarmer eller elektroniske dørlåse, således at alle døre normalt altid er låst, men åbnes, når autoriserede personer nærmer sig. På den måde vil personer, der kun går gennem tilladte døre, opleve bygningen som ulåst, mens andre vil finde dørene låst, når de forsøger at gøre noget forkert. Det forhindrer samtidig personer, der har snydt sig ind i en bygning gennem "tailgating" eller "social engineering," i at bevæge sig frit rundt i bygningen. Det ville være umuligt med traditionel skalsikring.

Et fuldstændigt situationsoverblik og PA kan også benyttes i åbne kontorlandskaber eller lignende steder, hvor nogle medarbejdere behandler fortrolige oplysninger på deres computerskærm. Andre medarbejdere eller gæster vil normalt kunne læse disse fortrolige oplysninger over skulderen på medarbejderen, når denne sidder og arbejder. Det er en overtrædelse af adgangskontrolpolitikken, der ikke kan forhindres af normale computeres adgangskontrolmekanismer. Ved at integrere PA med computerens adgangskontrolmekanisme har vi udviklet et system, der skjuler vinduer med fortrolig information, når der er uautoriserede personer inden for skærmens synsfelt. Når vinduet skjules, kan medarbejderen selvfølgelig ikke fortsætte med at arbejde, så vi arbejder nu på at udvikle en række alternative mekanismer, f.eks. blot at advare computerbrugeren om at en uautoriseret person har skærmen i sit synsfelt eller at reducere kontrasten mellem vinduets forgrundsfarve og baggrundsfarve efterhånden som den uautoriserede person nærmer sig. Ved at indlejre relativt billige IoT-enheder i omgivelserne og integrere dem med computerens sikkerhedsmekanismer kan vi således udvide disse sikkerhedsmekanismers virkefelt til også at omfatte omgivelserne.

Sådanne mekanismer kan selvfølgelig kun realiseres gennem sikre IoT-systemer. Men de viser, hvordan vi kan håndhæve intentionerne i sikkerhedspolitikkerne bedre, når vi inkluderer information fra de omgivelser, hvor computersystemerne findes og benyttes. De beskrevne sikkerhedsmekanismer er alle prototyper og der resterer en del arbejde, før de kan anvendes i praksis. Men de illustrerer, hvordan sikkerhed og bekvemmelighed kan gå op i en højere enhed, hvis vi anvender den ny IoT-teknologi rigtigt.



6. Klummer af Henrik Larsen

Hver måned kommenterer Henrik Larsen, chef for DKCERT, aktuelle problemstillinger inden for informationssikkerhed i magasinet Computerworld. Her bringer vi et udvalg.

6.1. SÅDAN KAN VI FÅ STYR PÅ DE EKSTREME IT-SIKKERHEDS-RISICI I INTERNET OF THINGS

Hvem er du, kære maskine?

Det spørgsmål skal de intelligente dimser i vores liv fremover kunne besvare. For at få et sikkert Internet of Things (IoT) har vi brug for Identity of Things.

Internet of Things vokser hurtigt. Stadig flere elementer i vores hverdag kan gå på nettet og dermed betjene os mere intelligent.

Vi kan tænde for varmen i sommerhuset hjemmefra via en app, så huset er varmt, når vi ankommer. Lægen kan fjernstyre patientens pacemaker, så dens indstillinger kan ændres, uden at det kræver en operation. Bilen kan hente trafikinformation over nettet og lede os uden om trafikpropper.

Men de smarte dimser medfører nye sikkerhedsrisici.

For eksempel skal der være styr på, hvem der ændrer på opsætningen af pacemakeren. Hvordan ved pacemakeren, at en kommando kommer fra patientens læge?

I sikkerhedskredse er man begyndt at tale om Identity of Things. Det handler om metoder til at identificere vores dimser. Eksemplet med den hackede pacemaker er ekstremt. Men behovet viser sig også i mere dagligdags teknologier.

For nylig er websteder blevet ramt af overbelastningsangreb fra botnettet Mirai. Computerne i Mirai er ikke pc'er eller servere. I stedet er de typisk digitale videooptagere. Mirai-programmet har let ved at inficere apparaterne. De har nemlig en standardbrugerkonto med tilhørende standardpassword.

6.1.1. Sikker opdatering

Mirai-botnettet demonstrerer behovet for stærkere identitet for apparater. Ligesom vi styrer menneskelige brugeres adgang til it-systemer med autentifikation, skal vi gøre det for apparaterne.

En af de store udfordringer ved Internet of Things er vedligeholdelse af firmware.

Når sikkerhedsforskere finder et sikkerhedshul, skal det lukkes. Producenten kan som regel forholdsvis hurtigt skrive en ny version af firmwaren. Problemet kommer, når den nye version skal ud til apparaterne.

Vores dimser kører ikke et tjek for nye opdateringer en gang om måneden. Derfor skal brugerne selv aktivt opdage, at der er kommet en ny version af firmwaren. De skal finde ud af, hvordan de opdaterer deres dimser. Og de skal gøre det, hver gang der kommer en ny version.

Det er ikke praktisk muligt. Selv med de gode systemer til opdatering, Windows og MacOS tilbyder i dag, kører mange med forældede softwareversioner på deres pc. Hvordan skal vi så forvente, at forbrugerne kan holde deres apparater opdateret?

Et led i Identity of Things er derfor også at etablere en sikker metode til at opdatere udstyret. Måske kan PKI (Public Key Infrastructure) blive en del af løsningen. Ved hjælp af digitale certifikater kan et apparat sikre sig, at det kun modtager opdateringer og kommandoer fra autoriserede kilder.

6.1.2. Mit personlige apparat

Et andet element i Identity of Things er forbindelsen mellem apparat og menneske.

I nogle tilfælde er der brug for at koble apparatets og dets brugers identitet sammen. For eksempel kan en pacemaker vide, at den er indopereret i en bestemt person.

Når min bil kører ud af et parkeringshus, skal afregningssystemet være sikker på, at jeg kun bliver opkrævet for min egen parkering - ikke for andre biler, der har været parkeret der.

6.1.3. Mangler vi et CDR?

I USA er myndighederne opmærksomme på problemet med usikre dimser på nettet. Department of Homeland Security har for nylig udgivet en samling strategiske principper for at sikre Internet of Things. Et grundlæggende princip er, at sikkerheden skal ind i produkterne allerede i designfasen.

I Danmark holder centrale systemer som CPR og CVR styr på identiteten af henholdsvis borgere og virksomheder. Måske er det på tide med et CDR - Centralt Dimse-Register?

Det kunne give apparaterne sikkerhed for, at de kommunikerer med den rigtige tjeneste. Men hvis det laves forkert, åbner sådan et register for problemer med privatlivsbeskyttelsen.

Ovenstående ideer til løsninger er kun løse tanker fra min side.

Dimsernes identitetsproblem må løses i et samarbejde mellem producenter, brugere og myndigheder.

Oprindelig offentliggjort den 25. november 2016

6.2. HAR DU HUSKET DENNE VIGTIGE DETALJE I DIN BACKUP?

Har du indlæst din sikkerhedskopi i dag? Inden for den sidste uge? Måned?

Vi sikkerhedsfolk understreger gerne, hvor vigtigt det er at tage backup. Desværre glemmer vi tit at nævne, at det også er vigtigt at kunne gendanne data.

En sikkerhedskopi er intet værd, hvis dataene i den ikke kan gendannes og bruges. Og det skal kunne lade sig gøre på rimelig tid.

Har I tid til at vente to dage på at få indlæst dataene fra jeres webshop?

6.2.1. Bedste middel mod ransomware

De senere år er flere organisationer blevet ramt af ransomware. Programmerne krypterer store dele af organisationens data. Bagmændene kræver løsepenge for den nøgle, der kan dekryptere dem.

Hvis virksomheden har en sikkerhedskopi, kan den glemme alt om løsepengene. I stedet indlæser den data fra sikkerhedskopien. I praksis stiller det nogle særlige krav til sikkerhedskopien.

For eksempel er det blevet udbredt at tage backup over internettet. Data lagres i cloud-systemer, hvorfra man kan tilgå dem via web eller med særlig klient-software. Fordelen er, at backuppen altid er opdateret. Filer kopieres over i cloud-systemet, så snart de oprettes eller ændres.

Men det er samtidig akilleshælen ved online backup: Når ransomwaren krypterer filerne, bliver de krypterede versioner gemt i skyen.

Derfor skal man stille krav til udbyderen af cloud backup: Det skal være muligt at gå tilbage og gendanne tidligere versioner af filerne.

For at undgå det problem anbefaler jeg, at I ikke nøjes med online backup. I bør også have en offline backup, der for eksempel bliver taget en gang i døgnet.

6.2.2. Backup som bevismateriale

Beskyttelse mod ransomware er én ting. Men sikkerhedskopier kan også bruges til andet.

En virksomhed kan blive ramt af et hackerangreb. En medarbejder kan misbruge sin position til at overføre penge eller stjæle fortrolige data. Når

den slags bliver opdaget, skal sagen efterforskes. Og her kan sikkerhedskopier spille en vigtig rolle.

En intern bedrager er måske dygtig til at slette sine spor. Filer bliver slettet, også logfiler. Men ofte glemmer bedrageren sikkerhedskopien. Eller forhåbentlig har vedkommende slet ikke fysisk eller logisk adgang til de bånd eller diske, den ligger på.

Her kan en sikkerhedskopi vise, hvordan de ændrede filer oprindelig så ud. Måske er der ligefrem en kopi af den logfil, bedrageren har slettet.

På den måde kan en sikkerhedskopi fungere som en bagdør til data, der ellers ikke er til at få fat i.

Den metode har vi imidlertid også set misbrugt.

6.2.3. Berømthedernes iPhone-fotos

I de sager, hvor berømtheder har fået stjålet private billeder fra deres iPhones, har hackerne ikke haft adgang til den fysiske smartphone. I stedet hackede de sig ind på den backup, der ligger i Apples cloud-system.

Eksemplet understreger, at backupdata er værdifulde. De skal beskyttes på linje med andre informationsaktiver.

6.2.4. Test jævnligt

Backup beskytter mod følgerne af fysisk nedbrud. Af ransomware. Af sabotage. Jeres backupsystem er uundværligt til at beskytte jeres data. Men som sagt er det alt sammen ligegyldigt, hvis sikkerhedskopien ikke kan indlæses.

Derfor anbefaler jeg, at I med jævne mellemrum tester, at I kan indlæse jeres sikkerhedskopier.

Det kræver is i maven at gøre det på et produktionssystem. Det vil jeg ikke anbefale. Opbyg i stedet et testsystem, der er en kopi af produktionssystemet. Brug det til at teste, at det er muligt at indlæse sikkerhedskopien og få systemet op at køre igen.

Backup handler foruden teknologi i høj grad om procedurer. Hvem tager backup, hvor tit sker det - og hvor ofte tester I, at I kan gendanne data?

Det skal alt sammen fremgå af jeres informationssikkerhedspolitik.

Oprindelig offentliggjort den 26. februar 2016

6.3. NY TENDENS I SIKKERHEDS-VERDENEN: MARKEDSFØRTE SÅRBARHEDER

Når en enkelt sårbarhed får uforholdsmæssigt stor opmærksomhed, ødelægger det prioriteringen af opdateringer.

I marts måned blev webstedet Badlock.org oprettet. Sikkerhedsforskerne bag siden oplyste, at de havde fundet en meget alvorlig sårbarhed - som de ville fortælle nærmere om 12. april, hvor rettelser også ville blive udsendt.

Det medførte en masse snak på Twitter og blandt sikkerhedsfolk i øvrigt. Hvad var sårbarheden? Hvor alvorlig var den? Vi vidste, at den fandtes i både Samba og Windows. Det tydede på, at den havde forbindelse til Windows fildeling.

Badlock var udstyret med både sit eget domænenavn og et ikon, der mindede om det, man brugte om sårbarheden Heartbleed.

I DKCERT udsendte vi en advarsel til de sikkerhedsansvarlige på universiteterne.

Vi foretog også en scanning efter IP-adresser på forskningsnettet, der havde åbent for Windows-fildeling.

6.3.1. Katastrofen udeblev

Tirsdag 12. april var vi mange, der ventede med spænding. Jeg fik en opringning fra en it-afdeling omkring klokken 16:00 - den kunne ikke forstå, hvor Badlock-rettelsen blev af. Jeg kunne berolige dem med, at Microsoft normalt udsender rettelser omkring kl. 19:00 dansk tid.

Så kom den endelig. Microsofts sikkerhedsbulletin MS16-047. Risikovurdering: Important.

Ja, important. Ikke critical.

Ingen mulighed for at afvikle programkode over netværk. Dommedag var aflyst.

Sårbarheden viste sig kun at kunne udnyttes via et man-in-the-middle-angreb. Angriberen skal altså befinde sig på offerets netværk i forvejen. Er det tilfældet, kan Badlock til gengæld udnyttes til at få øgede privilegier, læse password-databasen og i det hele taget misbruge adgangen til Active Directory.

6.3.2. Badlock er alvorlig

Som det fremgår, er Badlock altså alvorlig nok.

Hvis en angriber udnytter den i kombination med en anden sårbarhed, der giver adgang til offerets netværk, kan den bringe fortroligheden og integriteten i fare. Men for at kunne bruge den direkte ude fra internettet skal angriberen finde et offer, der har åbnet for Windows fildeling.

Sikkerhedseksperter har i mange år anbefalet at lukke af for den slags i firewallen.

Som forberedelse til Badlock gennemførte vi som nævnt en scanning af forskningsnettet efter IP-adresser med åben Windows-fildeling. Vi fandt under en tiendedel promille.

Så min konklusion er: Ja, Badlock er en vigtig sårbarhed. Sørg for at opdatere Windows og Samba.

Men den var langt fra den alvorligste sårbarhed, der blev lukket den dag.

12. april udsendte Microsoft 12 andre sikkerhedsrettelser. Fem af dem fik vurderingen Critical - Microsofts højeste risikovurdering.

6.3.3. Risiko for forkert prioritering

Hvilken opdatering prioriterede mine utålmodige venner, der ringede for at høre om Badlock, højest?

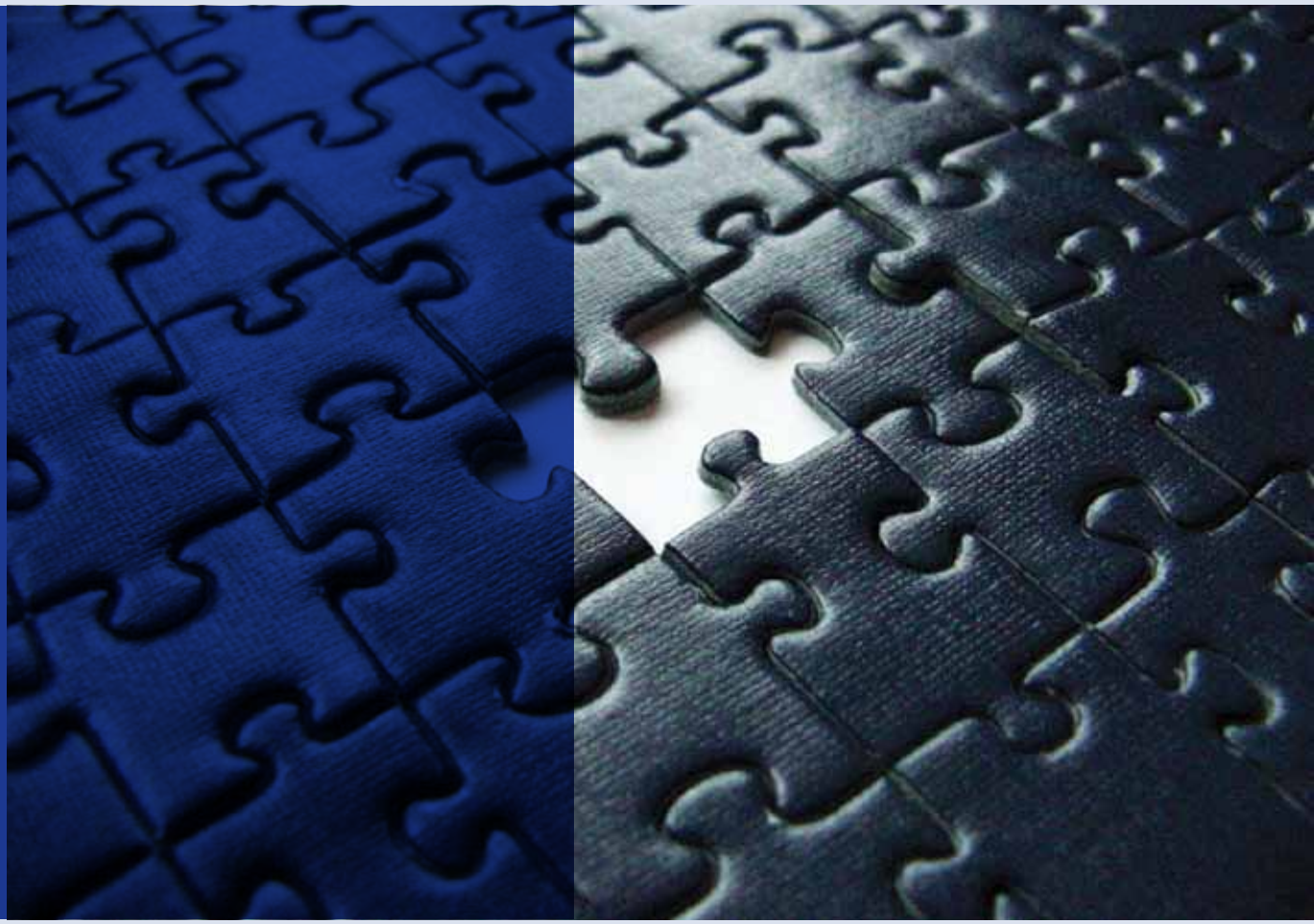
Jeg håber, at de læste beskrivelserne af sårbarhederne og foretog en risikovurdering af dem i forhold til deres eget it-miljø. Hvis de på den baggrund valgte at lukke Badlock-hullet først, er det fint. Men jeg er bange for, at mange har prioriteret Badlock højest uden at undersøge sagen nærmere.

Dermed kan vigtigere opdateringer være blevet sat bagest i køen.

6.3.4. Sårbarheder med navn og logo

Badlock skriver sig ind i en ret ny tradition i sikkerheds-verdenen: Markedsførte sårbarheder. I april 2014 blev en sårbarhed i OpenSSL kendt under navnet Heartbleed - komplet med eget domæne og logo.

Det var første gang, en sårbarhed blev markedsført på den måde. Tidligere har der været navne til



trusler og virus, men ikke til sårbarheder. Siden har vi hørt om POODLE, Shellshock, Ghost, FREAK og flere andre navngivne sårbarheder.

Der er flere fordele ved at give en sårbarhed et navn.

For det første er det nemmere at huske. Kun sikkerhedsfolk kan kende forskel på CVE-2014-0160 og CVE-2014-6271, mens det er let at huske Heartbleed og Shellshock.

For det andet sikrer det, at vi taler om den samme sårbarhed.

For det tredje er det lettere at gøre folk uden for sikkerhedsverdenen interesserede.

Ulempen er, at massivt markedsførte sårbarheder som Badlock kan få mere opmærksomhed, end de fortjener - og dermed fjerne opmærksomheden fra mere alvorlige sårbarheder.

6.3.5. Inflation i sårbarheder

Jeg håber, at sikkerhedsfolk fremover er mere forsigtige med at markedsføre sårbarheder med navn og logo. Ellers risikerer vi, at der går inflation i det, og der opstår en "Ulven kommer"-effekt.

I øvrigt medførte den almindelige skuffelse over Badlock, at nogen oprettede domænet Sadlock.org. Besøg det for et satirisk kig på sårbarhedsmarkedsføring.

Oprindelig offentliggjort den 29. april 2016

6.4. DERFOR SKAL DU FORTÆLLE ALLE OM ANGREB OG TRUSLER DER RAMMER DIG

Vi har været ramt af ransomware.

Nej, ikke DKCERT. Men DeiC (Danish e-Infrastructure Cooperation), som vi hører ind under. En medarbejder kom til at klikke på en vedhæftet fil, og hans dokumenter blev krypteret. Andre data blev ikke berørt.

Vi løste det ved at indlæse backuppen. Dermed mistede medarbejderen kun en halv dags arbejde.

Når jeg nu fortæller om vores ransomwareangreb, skyldes det, at jeg gerne vil slå et slag for åbenhed.

Vi i informationssikkerhedsbranchen skal blive bedre til at dele oplysninger om de angreb, vi bliver udsat for. Inspirationen til denne klumme kommer fra Tom Engly, der er sikkerhedschef i Tryg.

Han fortalte for nylig i Børsen om, hvordan forsikringsselskabet var blevet ramt af ransomware. I artiklen opfordrede han til større åbenhed og samarbejde om informationssikkerhed.

Jeg er helt enig. Samarbejde er nødvendigt. Kommunikation er en forudsætning for samarbejde. Og kommunikation kræver åbenhed.

6.4.1. Uheldig tradition

Vi har en uheldig tradition for lukkethed, når det gælder sikkerhedshændelser. De fleste virksomheder eller organisationer vil nødig fortælle, at de er blevet ramt af virus eller et hackerangreb.

Men er det pinligt at blive ramt af ransomware? Nej. Det kan ske for enhver organisation.

Årsagen kan være medarbejdere, der er lidt for hurtige, eller sårbarheder, der ikke er blevet fjernet med en softwareopdatering.

Jeg tror, der er mange angreb med ransomware i Danmark. Men jeg ved det ikke. Det er der heller ingen andre, der ved.

Der mangler simpelthen statistikker over, hvor mange pc'er der bliver inficeret med ransomware.

Et vigtigt element i informationssikkerhed er risikovurdering. Risiko er defineret som kombinationen af en sårbarhed og en trussel ganget med sandsynligheden for, at den bliver udnyttet.

For at anslå risikoen skal man altså kende sandsynligheden. Men det gør vi ikke, når ingen fortæller om de angreb, de bliver ramt af.

6.4.2. Derfor holder vi tæt

Traditionen for lukkethed er naturligvis ikke opstået ud af ingenting. Der er gode argumenter for at holde kortene tæt til kroppen.

Et argument kan være, at man ikke vil tiltrække sig uønsket opmærksomhed. Hvis angriberne ved,

at man en gang har været ramt, kan de opfatte en som et let mål og dermed sætte flere angreb ind.

Den bekymring er reel, når vi taler målrettede angreb som fx industrispionage.

Men langt det meste malware og ransomware er ikke målrettet. Bagmændene skyder med spredehagl i håbet om at ramme et eller andet. Derfor er jeg ikke bange for, at vi bliver udsat for øgede mængder ransomware ved at fortælle om et enkelt angreb - der i øvrigt ikke gav bagmændene nogen gevinst.

6.4.3. Forordning ændrer reglerne

En anden årsag til lukkethed kan være frygten for virksomhedens renommé. Tør kunderne handle med en virksomhed, der er blevet offer for et angreb?

Også her en relevant bekymring. Men i langt de fleste tilfælde har angreb med ransomware eller anden malware ingen konsekvenser for kunderne. Deres personlige data, herunder oplysninger om betalingskort, bliver kun sjældent berørt.

Og bliver personlige data ramt, er der slet ingen mulighed for at undgå åbenhed: Så skal man indberette det til Datatilsynet og informere alle berørte kunder.

Det er konsekvensen af EU's persondataforordning, som træder i kraft om et par år.

Forordningen gør det muligt at straffe virksomheder med bøder, hvis de ikke overholder reglerne. Og de ramte personer kan søge erstatning.

6.4.4. Kender du til angreb?

Jeg håber, at persondataforordningen kan være med til at ændre kulturen, så vi bliver mere åbne om at dele vores sikkerhedshændelser. Men det kræver, at vi kender til dem.

Åbenhed udadtil er kun mulig, hvis vi har den indadtil. Har du styr på, hvor mange medarbejdere, der bliver ramt af ransomware?

Jeg har indtryk af, at angreb efterhånden er så udbredte, at it-afdelingerne er blevet hurtige til at rense pc'erne og indlæse backup. Effektivitet er godt. Men bliver angrebene registreret?

Hvis I selv savner det overblik, vil jeg anbefale, at I gør noget ved det. Se fx på, om jeres system til servicedesken kan bruges til at føre statistik.

Endelig ville det være nyttigt, hvis der var en fælles instans, der opsamlede data om angreb.

I DKCERT har vi desværre ikke ressourcerne til at tilbyde at stå for det. Men hvis nogen kan finde midlerne, vil vi med glæde påtage os opgaven.

Oprindelig offentliggjort den 27. maj 2016

6.5. VI HAR KÆMPET FOR IT-SIKKERHED I 25 ÅR - I DAG HAR HVERKEN PRIVATE ELLER SMÅ VIRKSOMHEDER NOGET STED AT GÅ HEN

Nøjagtig hvornår DKCERT blev stiftet, ved vi ikke. Der er ikke bevaret skriftligt materiale. Alt tyder dog på, at det skete i sommeren 1991.

Dermed fylder DKCERT 25 år. Vi fejrede fødselsdagen på den årlige DeiC konference i Kolding tidligere på måneden. Ved den lejlighed fortalte jeg udpluk fra DKCERTs historie.

Oprettelsen af DKCERT var en direkte konsekvens af en af de første danske hackersager: Sagen mod Jub Jub Bird og Sprocket.

Det var to unge herrer, der bevæbnet med et par Amiga-computere og en pc hackede sig ind på UNI-C's netværk. UNI-C var det nationale center for it til forskning og uddannelse. Organisationen drev et landsdækkende ethernet-baseret netværk.

Hackerne benyttede modemer til at ringe op til computere hos UNI-C. De gættede sig til adgangskoder og kom på den måde på nettet.

Allerede i 1989 havde de held med at komme ind på computere i både Danmark og udlandet.

6.5.1. Angreb fra RUC mod NASA

Omkring årsskiftet 1990-91 var de to i gang igen. Denne gang forsøgte de at hacke sig ind på computere hos NASA via en computer på RUC.

En systemadministrator fra Nasa gav i januar 1991 UNI-C besked om, at nogen havde forsøgt at få fat i password-filen fra en af organisationens servere.

I 1988 var det meste af det daværende internet blevet lagt ned af den såkaldte Morris-orm. Det førte til dannelsen af CERT/CC (Computer Emergency Response Team Coordination Center) på Carnegie Mellon University.

CERT/CC stod for koordinering af indsatsen ved alvorlige sikkerhedsproblemer på nettet.

6.5.2. Kontakt til CERT/CC

CERT/CC fik en kopi af mailen fra NASA og hen-

vendte sig til UNI-C og fortalte, at man havde set flere andre forsøg på hacking fra RUC. UNI-C meldte sagen til politiet, og i fællesskab lykkedes det at finde frem til Jub Jub Bird og Sprocket. De blev anholdt og dømt.

Ligesom Morris-ormen førte til dannelsen af CERT/CC, førte den danske hackersag til, at UNI-C oprettede CERT. Efterhånden blev navnet udvidet til DKCERT for at markere forskellen til de CERT'er i andre lande, der begyndte at blive dannet.

I 1993 kom DKCERT på banen i den såkaldte Haslevsag. Igen blev UNI-C's netværk og modemer misbrugt til at give hackere adgang til en række computere på universiteter og andre steder.

6.5.3. Udvidede aktiviteter

Jørgen Bo Madsen var den første leder af CERT frem til 1997. Derefter blev CERT lagt ind under UNI-C's andre sikkerhedsaktiviteter.

I 2000 ansatte UNI-C den tidligere vicekriminalkommissær Preben Andersen som leder. I Preben Andersens tid blev staben udvidet. Samtidig udbyggede han det internationale samarbejde, der havde eksisteret fra begyndelsen.

Ligeledes optrådte han og DKCERT ofte i medierne, når der var nyheder om it-sikkerhed.

Den linje fortsatte under Shehzad Ahmad, der overtog chefposten i 2007. Samtidig gjorde han meget for at udbygge samarbejdet med de sikkerhedsansvarlige på universiteterne.

I kraft af min stilling som først driftsansvarlig og siden sikkerhedsansvarlig på Københavns Universitet lærte jeg DKCERT og Shehzad Ahmad at kende. Derfor var det nærliggende for mig at søge stillingen som chef, da Shehzad forlod den i 2015.

6.5.4. Fra akademikere til private

Siden begyndelsen har DKCERT været knyttet til det landsdækkende forskningsnet. Først via UNI-C, i dag som en del af DeiC (Danish e-Infrastructure Cooperation), der arbejder for at fremme eScience (brugen af it i forskningen) i Danmark.

Da vi begyndte, var internettet ikke noget for private brugere. Web var kun lige ved at blive opfundet. Siden er adgang til internettet fra vores hjem og mobiltelefoner blevet noget, vi tager for givet.

Det har medført, at sikkerhedstruslerne er mangedoblet i omfang: Hvor de it-kriminelle før kun kunne gå efter virksomheder og offentlige institutioner, retter de i dag også skytset mod private borgere.

DKCERT har ikke ressourcer til at behandle hændelser fra andre end forskningsnettet. Det ville vi ellers gerne. Og der er brug for det.

Private borgere og små og mellemstore virksomheder har ikke noget sted at gå hen, når de løber ind i sikkerhedsproblemer. Ingen offentlig instans tager sig af dem.

Det ville være en spændende opgave for DKCERT at påtage sig i de kommende 25 år. Vi er klar. Men i givet fald skal nogen finde finansieringen til det.

Oprindelig offentliggjort den 28. oktober 2016

7. Fremtidens trusler og trends

Afpresning i flere former og misbrug af persondata vil fortsat true informationssikkerheden. Organisationer får travlt med at forberede sig til databeskyttelsesforordningen.

De it-kriminelle går efter værdierne. Det gjorde de ikke, da DKCERT blev oprettet for 25 år siden. Dengang handlede hacking og virus mest om at demonstrere teknisk kunnen og udforske systemer. Men siden da har motivationen ændret sig.

7.1. TRUSLER MOD INFORMATIONSSIKKERHEDEN I 2017

Langt hovedparten af dagens it-kriminalitet forsøger at få fat i andres værdier. Det kan være værdier forstået som kolde kontanter. Det ser vi i ransomware, DDoS-afpresning og falske direktør-mails om pengeoverførsler.

Men værdier kan også være fortrolige oplysninger om et konkurrerende politisk partis strategi. Det så vi i 2016, hvor hackede oplysninger indgik i den amerikanske præsidentvalgkamp.

Begge motivationer vil fortsat være aktive i 2017. Derfor venter vi også at se en fortsættelse af de trusler, vi så i 2016. Det drejer sig blandt andet om:

- Ransomwareangreb.
- Afpresning med trusler om DDoS-angreb.
- Afpresning med trusler om at afsløre forretningshemmeligheder stjålet ved hacking eller gennem insidere.
- Misbrug af persondata fra store web-tjenester – enten fremskaffet via hacking eller på grund af fejl hos udbyderen.
- Svindel med klik på webannoncer.
- Misbrug af persondata fremskaffet via phishing.
- Direktørsvindel med falske bestillinger af pengeoverførsler.
- Industrispionage via hacking og spear phishing.
- Politisk spionage via hacking og spear phishing.
- Distribution af piratkopierede film og andre medier.

7.2. SIKKERHEDSTRENDS I 2017

7.2.1. Databeskyttelsesforordningen

Den største sikkerhedsopgave i 2017 bliver at forberede sig på EU's databeskyttelsesforordning. Den vil blive håndhævet fra den 25. maj 2018. Inden da skal myndigheder, institutioner, private virksomheder og andre, der behandler persondata, være klar til at leve op til kravene.

Visse organisationer skal tilknytte en databeskyttelsesrådgiver (DPO, Data Protection Officer). Kravet gælder alle offentlige myndigheder og institutioner. Endvidere gælder det også private virksomheder, der behandler store mængder persondata, eller hvis forretning bygger på registrering af data om fysiske personer.

I DKCERTs verden betyder det blandt andet, at universiteterne skal tilknytte databeskyttelsesrådgivere. De får til opgave at sikre, at organisationerne beskytter persondata i henhold til forordningens krav.

Men forordningen får også indflydelse på andre organisationer. Så snart man behandler en eller anden form for persondata, er man omfattet. Opbevarer I navne og mail-adresser på jeres kunder eller ansatte? Så er I omfattet.

7.2.2. ISO 27001

Forberedelserne til databeskyttelsesforordningen kan gå hånd i hånd med arbejdet med at indføre styring af informationssikkerhedsarbejdet ud fra ISO 27001-standarden. Statslige organisationer skal i forvejen følge ISO 27001. Derfor giver det god mening at tænke arbejdet med databeskyttelsesforordningen ind i det rammeværk, man opbygger ud fra ISO-standarden.

Også selvom der ikke er krav om, at ens organisation eller virksomhed skal indføre ISO 27001, kan det alligevel være en god ide at se nærmere på den.

7.2.3. Sikkerhed er ledelsens ansvar

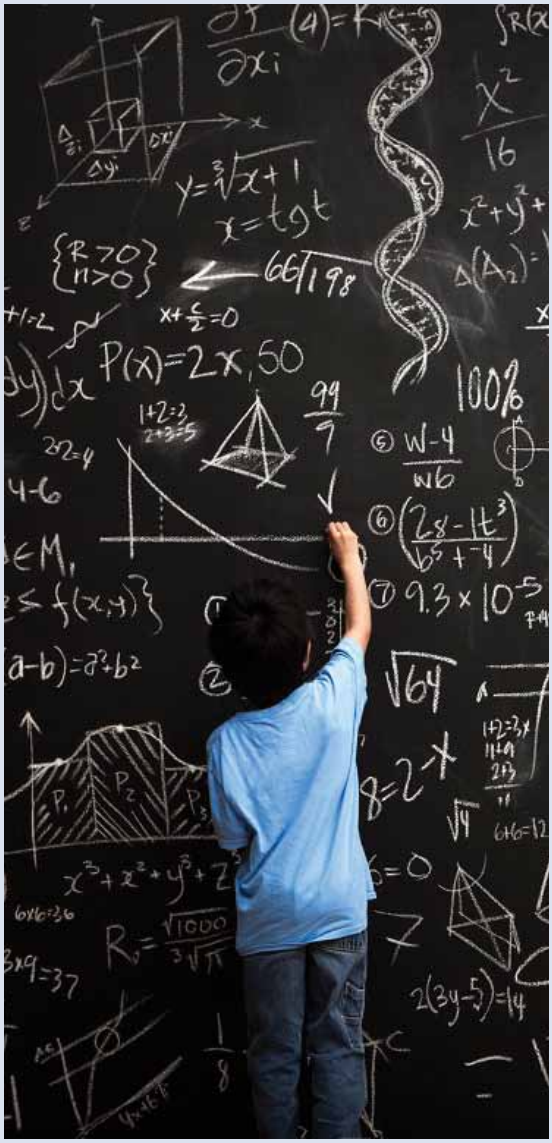
I dag gennemsyrer digitaliseringen hele vores liv – både for privatpersoner og virksomheder. Et brud på informationssikkerheden kan få alvorlige konsekvenser. Derfor er det nødvendigt, at ledelsen tager ansvaret for informationssikkerheden.

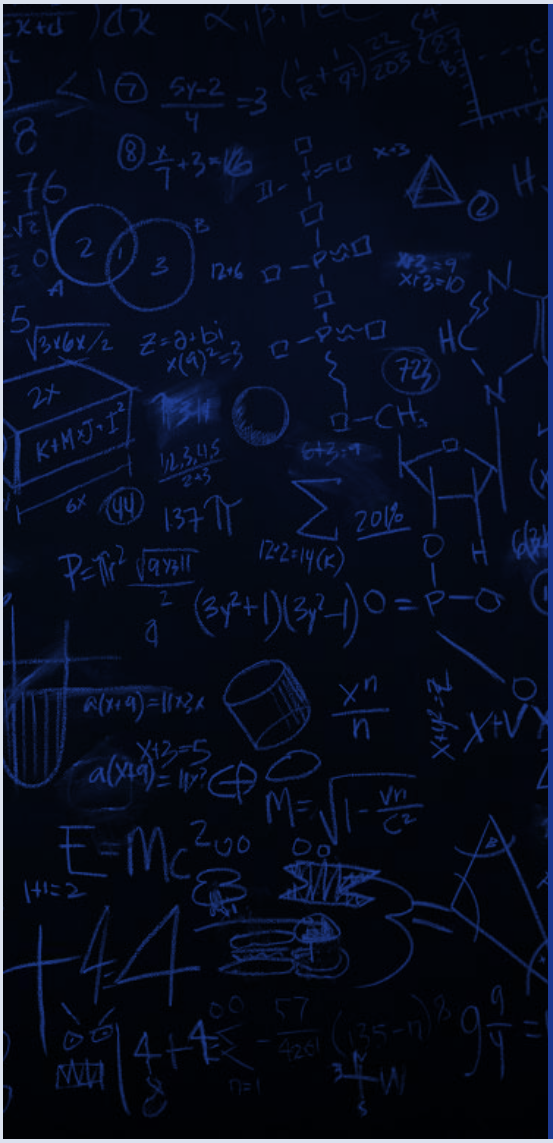
Det betyder ikke, at direktøren eller rektoren skal kunne konfigurere en firewall. Men ledelsen skal træffe de overordnede beslutninger om sikkerhed ud fra en risikovurdering. Og ledelsen skal sikre, at den overordnede strategi udmøntes i konkrete tiltag.

Den tanke går godt i tråd med både databeskyttelsesforordningen og ISO 27001.

DKCERT mener

Arbejdet med informationssikkerhed skal forankres i ledelsen. Udgangspunktet skal være en risikobaseret tilgang, hvor ledelsen ud fra en risikovurdering fastlægger organisationens sikkerhedsstrategi. Den skal udmøntes i konkrete sikkerhedstiltag. Hele arbejdet kan med fordel styres ud fra principperne i ISO 27001.





8. Anbefalinger

I dette kapitel kommer DKCERT med anbefalinger, der har til formål at øge informationssikkerheden i den akademiske verden.

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.

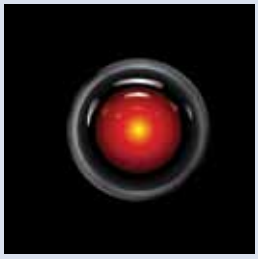
1. Forlang ledelsens aktive involvering i informationssikkerhedsarbejdet
2. Ajourfør og vedligehold informationssikkerhedspolitikken
3. Forbered overholdelse af databeskyttelsesforordningen
4. Hav fokus på sikkerheden ved udvikling af applikationer og tjenester samt tilretninger af eksisterende systemer.
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 Ůowet 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 tjeneste fra DeiC. Se 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.

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.

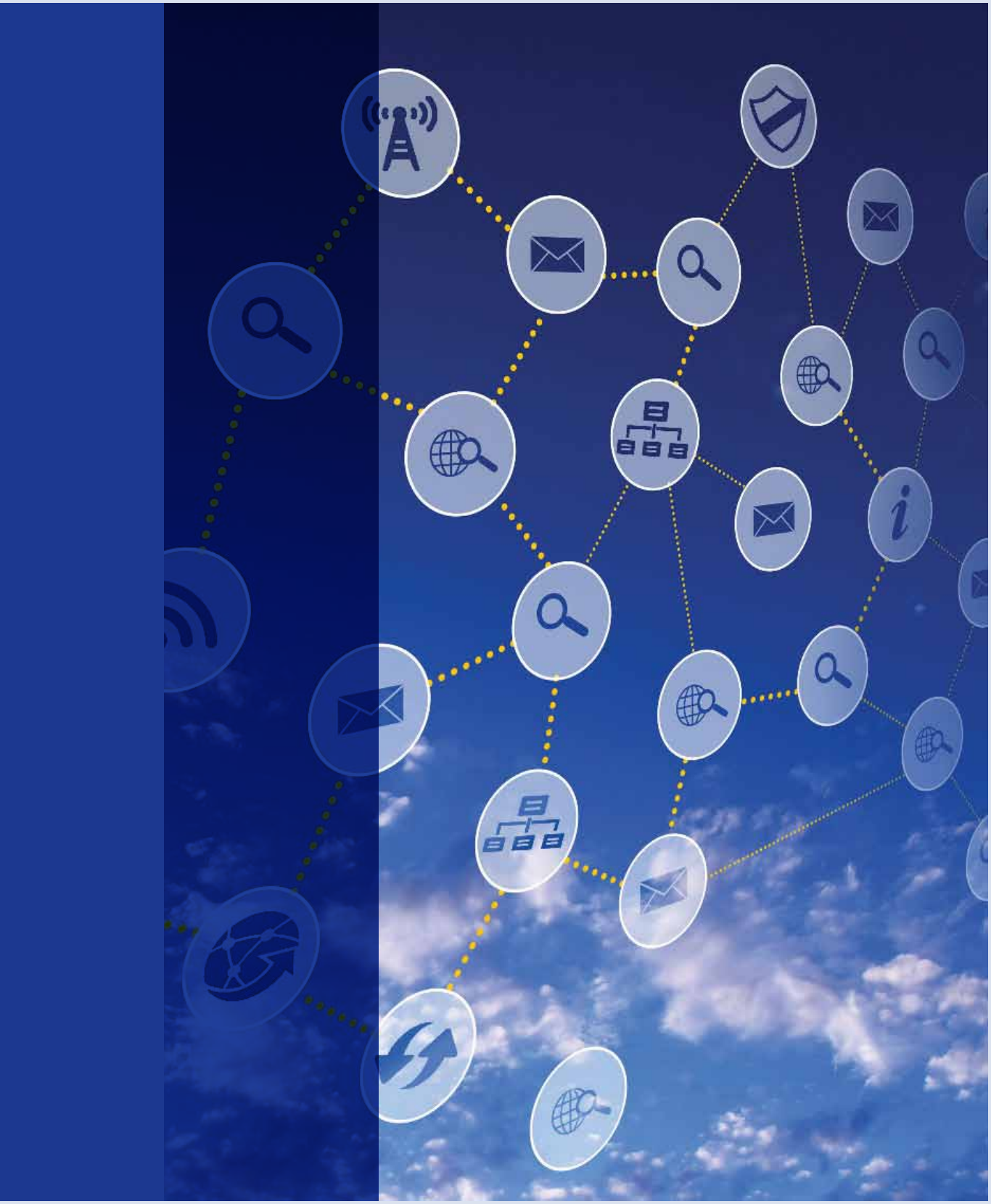
To-faktor-autentiûkation
Autentifikation, der supplerer brugernavn og password med en yderligere faktor, som brugeren skal angive for at få adgang. Det kan være en engangskode, der sendes til brugerens mobiltelefon som sms, et fingeraftryk, der angives via en fingeraftrykslæser, en kode fra et papirkort 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, botnetprogrammer 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. **DKCERT/Digitaliseringsstyrelsen:**
   Danskernes informationssikkerhed 2016,
   https://www.cert.dk/information/borgernes_informationssikkerhed

2. **Flexera Software:**
   Vulnerability Review 2017,
   https://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/

3. **Brian Krebs:**
   KrebsOnSecurity Hit With Record DDoS,
   https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

4. **Flashpoint:**
   Mirai Botnet Linked to Dyn DNS DDoS Attacks,
   https://www.flashpoint-intel.com/mirai-botnet-linked-dyn-dns-ddos-attacks/

5. **Europol:**
   No More Ransom: law enforcement and IT security companies join forces to fight ransomware,
   https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware

6. **GovCERT.ch:**
   Armada Collective is back, extorting Financial Institutions in Switzerland,
   https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware

7. **Wikipedia:**
   2016 Democratic National Committee email leak,
   https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak

8. **Wikipedia:**
   Podesta emails,
   https://en.wikipedia.org/wiki/Podesta_emails

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC

Trendrapport

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

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