T R E N D R A P P O R T

16

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC DANISH e-INFRASTRUCTURE COOPERATION

DKCERT Trendrapport 2016

Redaktion: Henrik Larsen og Torben B. Sørensen

Tak til vore øvrige bidragydere: Tonny Bjørn, DKCERT, Bjarne Mathiesen Schacht, DKCERT, Edilbert Cajucom, F-Secure, Marie Albæk Jacobsen, Bech-Bruun, Henrik Rask, Aalborg Universitet, René Hedegaard Hansen, Terma, og Anette Høyrup, Forbrugerrådet Tænk

Design: Kiberg & Gormsen

Tryk: GraphicCo

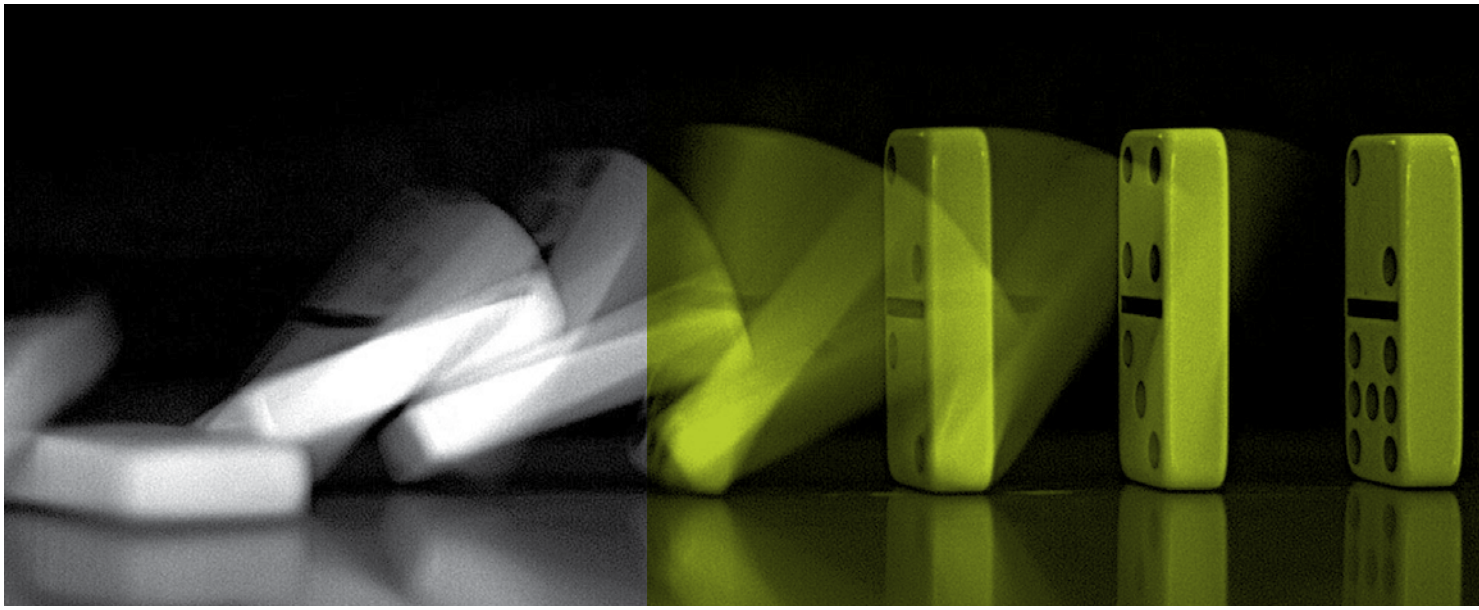
DeIC-journalnummer: DeIC JS 2016-2

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 blev oprettet i 1991 som en afdeling af UNI-C (forløberen for Styrelsen for It og Læring).

I dag hører DKCERT under DeIC, Danish e-Infrastructure Cooperation. DeIC har til formål at understøtte Danmark som e-science-nation gennem levering af e-infrastruktur (computing, datalagring og netværk) til forskning og forskningsbaseret undervisning. DeIC er etableret under Uddannelses- og Forskningsministeriet og hører organisatorisk under Styrelsen for Forskning og Innovation.

Fysisk er DKCERT placeret på DTU's campus nord for København.

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

Indholdsfortegnelse

1. Velkomst

Velkommen til DKCERT Trendrapport 2016! Dette års trendrapport markerer DKCERTs 25 års jubilæum: DKCERT blev oprettet i 1991.

Hvornår UNI-C helt nøjagtigt oprettede DKCERT, er svært at afgøre. Men det skete i forlængelse af den første store danske hackersag: Sagen mod de to hackere, der gik under navnene JubJub Bird og Sprocket. De blev anholdt den 14. januar 1991.

CERT, som organisationen dengang hed, blev oprettet med inspiration fra USA's CERT/CC (Computer Emergency Response Team Coordination Center). Det amerikanske center blev oprettet efter det første angreb med en orm på internettet, den såkaldte Morris-orm.

Dengang var der ikke mange centre til håndtering af sikkerhedshændelser. De fleste fandtes på amerikanske universiteter og var oprettet som konsekvens af Morris-ormen. Den danske CERT var blandt de første internationale CERT'er. Siden blev CERT et varemærke, som Carnegie Mellon-universitetet ejer. Den danske organisation skiftede navn til først DK-CERT, siden DKCERT.

Uanset navnet opstod DKCERT på grund af et behov: En sikkerhedshændelse i form af et hackerangreb skulle behandles. Siden da er behovet kun vokset.

Fra begyndelsen havde DKCERT et bredt udsyn. Det primære fokus var på sikkerheden på forskningsnettet, men der var også plads til at behandle it-sikkerhed i bredere forstand. Virksomheder og private borgere kunne henvende sig og få et godt råd, hvis de havde været udsat for en sikkerhedshændelse.

Det arbejde har DKCERT ikke længere ressourcer til at påtage sig. I dag er vi en rendyrket akademisk CSIRT (Computer Security Incident Response Team).

Det medfører et problem: I dag er der ingen uafhængige instanser, der tager sig af it-sikkerhedshændelser hos private borgere eller virksomheder. Sikkerheden i staten er i gode hænder hos vores kolleger i Center for Cybersikkerhed under Forsvarets Efterretningstjeneste. Virksomheder, der driver kritisk infrastruktur, kan også få hjælp der. Erhvervs- og Vækstministeriet har netop oprettet Virksomhedsrådet for IT-sikkerhed, og Digitaliseringsstyrelsen har et Dialogforum for Informationssikkerhed.

Det er gode initiativer. Men vi mener, at borgerne og de mindre virksomheder mangler et sted at få konkrete råd og vejledninger, når de støder på sikkerhedsproblemer. Det kunne være i stil med, hvad Center for Cybersikkerhed tilbyder statens institutioner, og hvad DKCERT tilbyder den akademiske verden.

Den opgave vil vi gerne påtage os igen, hvis den nødvendige finansiering kan fremskaffes. Ikke som en konkurrent til de private virksomheder i sikkerhedsbranchen, men som en offentlig tjeneste, der er uafhængig af kommercielle interesser.

Hvad der foregår af sikkerhedshændelser i Danmark og internationalt, fremgår af de følgende sider. God fornøjelse med læsningen af dette års trendrapport!

Henrik Larsen
chef for DKCERT

2. Resumé

DKCERT behandlede en rekordstor mængde sikkerhedshændelser og fandt sårbarheder på 26 procent af de scannede systemer.

DKCERT behandlede over 160.000 sikkerhedshændelser i 2015. Det er en stigning på 145 procent, men tallene fra 2014 og 2015 er ikke umiddelbart sammenlignelige. For eksempel handlede næsten hver tredje hændelse i 2015 om advarsler mod systemer, der potentielt kan udnyttes til overbelastningsangreb. Den type hændelser registrerede vi ikke i 2014.

Godt 1.000 sager handlede om it-systemer, hvis sikkerhed var kompromitteret. I andet halvår var der 819 hændelser med klager over brud på ophavsretten. Det var typisk piratkopiering af film og tv-serier.

Trojanske heste var den mest udbredte form for skadelig software på danskernes pc'er. Den hyppigste trussel var JavaScript-programmer, der sendte besøgende videre til en anden computer med skadeligt indhold.

Mængden af defacements på danske websteder steg 29 procent. Det skyldes primært nogle få store angreb, hvor mange domæner på den samme IP-adresse blev overtaget i ét hug.

For tredje år i træk gennemførte DKCERT undersøgelsen "Borgernes informationssikkerhed" for Digitaliseringsstyrelsen. Den viste, at 61 procent af deltagerne ikke tager sikkerhedskopi af data på deres computer. 57 procent bruger samme adgangskode til flere onlinetjenester.

På verdensplan blev der fundet 6.488 nye sårbarheder i it-systemer i 2015. Det er 18 procent færre end i 2014.

DKCERT foretog sårbarhedsscanninger af de danske universiteters it-systemer i 2015. Scanningerne fandt sårbarheder på 26 procent af de IP-adresser, der svarede på scanningen. Da der senest blev scannet i 2013, var tallet 21,2 procent.

Kun to procent af de sårbarheder, scanningerne afslørede, er klassificeret som kritiske.

Sikkerhedsteknologien SSL (Secure Sockets Layer) og dens efterfølger TLS (Transport Layer Security) giver også problemer med sikkerheden. Halvdelen af de sårbarheder, scanningerne afdækkede, havde relation til SSL/TLS. Det kan fx være forældede versioner af softwaren, udløbne certifikater eller fejl i konfigurationen.

2.1. > TENDENSER FRA ÅRET DER GIK

Afpresning optrådte på mindst to måder i 2015: Ransomware og DDoS-angreb. Ransomware er skadelige programmer, der fjerner adgangen til data. Det sker typisk ved at kryptere dem, så brugeren ikke kan læse dem. Bagmændene kræver løsepenge for den nøgle, der kan fjerne kodningen. Syv procent af deltagerne i undersøgelsen "Borgernes informationssikkerhed" havde været udsat for ransomware. Ingen af dem fik data tilbage ved at betale løsesummen.

It-kriminelle truer med at udsætte websteder for overbelastningsangreb, såkaldte DDoS-angreb (Distributed Denial of Service). Efter at have demonstreret, at de kan sætte webstedet ud af drift, standser de angrebet og kræver betaling for ikke at starte det igen.

En række internationale sikkerhedshændelser handlede om persondata, der kom i de forkerte hænder. Den mest omtalte var hackerangrebet på Ashley Madison, en tjeneste for personer i et fast forhold, der er interesseret i at have en affære.

Sikkerhedsforskere demonstrerede for første gang, at de kunne hacke sig ind på en kørende bil og styre rat og bremser. Kommunikationen foregik over mobilnettet gennem underholdningssystemet i bilen. Det er et eksempel på de sikkerhedsproblemer, det såkaldte Internet of Things (IOT) kan medføre.

Mod slutningen af året opnåede EU-institutionerne enhed om den kommende persondataforordning, der skal gælde for alle EU-lande. Læs mere om den i kapitel 5.

3. 2015 – året i tal

DKCERT behandlede over 160.000 sikkerhedshændelser i 2015.

3.1. > ÅRETS SIKKERHEDSHÆNDELSER

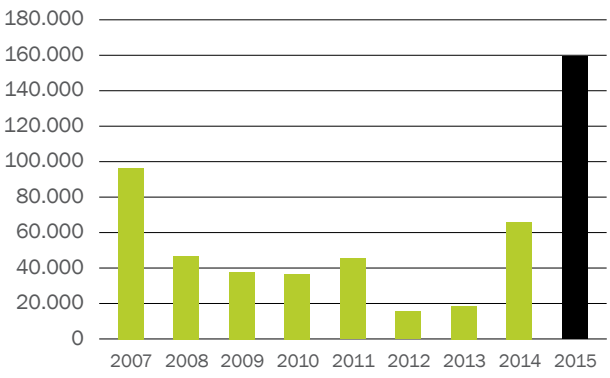
DKCERT behandlede 160.214 sikkerhedshændelser i 2015. Det er en stigning på 145 procent i forhold til 2014 (se Figur 1). Tallene er dog ikke direkte sammenlignelige. Det skyldes to forhold: Dels indførte DKCERT et nyt sagsbehandlingssystem i sommeren 2015, dels er der kommet nye eksterne kilder til.

De eksterne kilder leverer oplysninger om sikkerhedshændelser og potentielt sårbare systemer. DKCERT kan for eksempel modtage en advarsel om, at en bestemt IP-adresse har en computer med Heartbleed-sårbarheden. Det registreres som en hændelse i sagsbehandlingssystemet.

Hvis vi to dage senere får en advarsel om, at samme IP-adresse har en Heartbleed-sårbarhed, tæller det som en ny hændelse. Det er muligt, at der er tale om den samme sårbare computer. Men bag en IP-adresse vil der ofte gemme sig flere forskellige maskiner. Vi kan derfor ikke vide, om det drejer sig om den samme computer. Det kan være, at den oprindelige computer har fået fjernet sårbarheden, men at der siden er tilføjet en ny sårbar computer bag samme IP-adresse. På den baggrund kan der være gengangere i registreringerne.

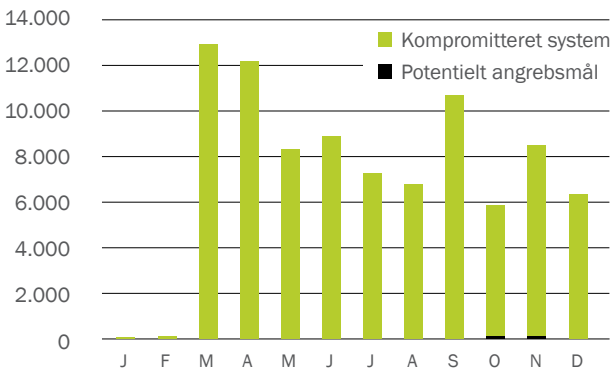
FIGUR 1

Sikkerhedshændelser håndteret af DKCERT 2007-2015



FIGUR 2

Hovedparten af sagerne om uautoriseret adgang handlede om potentielle mål for angreb



3.2. > FORDELING PÅ TYPER AF HÆNDELSER

Ved overgangen til det nye sagsbehandlingssystem indførte DKCERT også nye klassificeringer af sikkerhedshændelser. Derfor har det ikke været muligt at sammenligne typerne af hændelser med tidligere år. Af samme grund har vi ikke data for hele året, når det gælder nogle af sagstyperne.

3.3. > UAUTORISERET ADGANG

DKCERT registrerede 88.503 sikkerhedshændelser, der handlede om uautoriseret adgang til it-systemer. Langt hovedparten var af typen, hvor der blev opdaget et system, som kunne kompromitteres – for eksempel fordi det havde en kendt sårbarhed. Kun godt 1.000 sager handlede om systemer, der rent faktisk var kompromitteret (se Figur 2).

Anmeldelserne om potentielt sårbare systemer kommer typisk fra automatiserede systemer, der løbende scanner nettet. DKCERT behandler dem ligeledes automatiseret, idet en advarsel automatisk sendes videre til de ansvarlige for den IP-adresse, den handler om.

3.4. > BRUD PÅ OPHAVSRETTEN

Klager over brud på ophavsretten tegnede sig i perioden fra 15. juli til udgangen af året for 819 hændelser. Det er som regel repræsentanter for rettighedshavere, der har registreret, at et værk er blevet hentet af en bestemt IP-adresse. Værkerne er typisk film og tv-serier (se Figur 3).

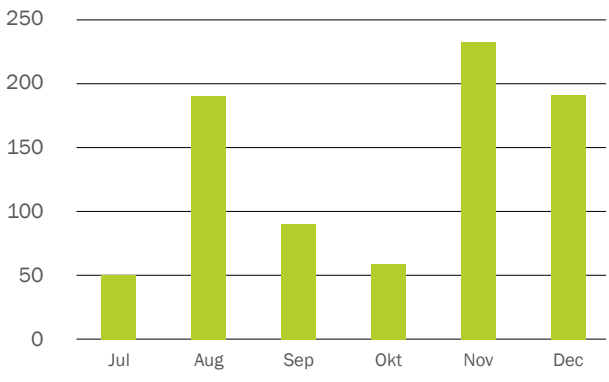
3.5. > DENIAL OF SERVICE

Godt 53.000 sager handlede om overbelastningsangreb, såkaldt denial of service. Stort set alle var af typen, hvor DKCERT blev opmærksom på en server, der kunne misbruges i et DDoS-angreb (Distributed Denial of Service). Tallet angiver altså ikke mængden af angreb, men omfatter især de tilfælde, hvor DKCERT advarede en institution om, at dens it-systemer kunne misbruges til at angribe andre med. I en række tilfælde var sagen dog, at tjenester på forskningsnetadresser havde været udnyttet til angreb på tredjepart.

Det kan for eksempel være en tjeneste som DNS (Domain Name System). Hvis serveren tillader opslag fra alle på internettet, kan den misbruges. En angriber kan sende en forespørgsel med forfalsket afsender. DNS-serveren sender svaret til den forfalskede adresse. Hvis mange gør det på samme tid, overbelastes serveren hos offeret.

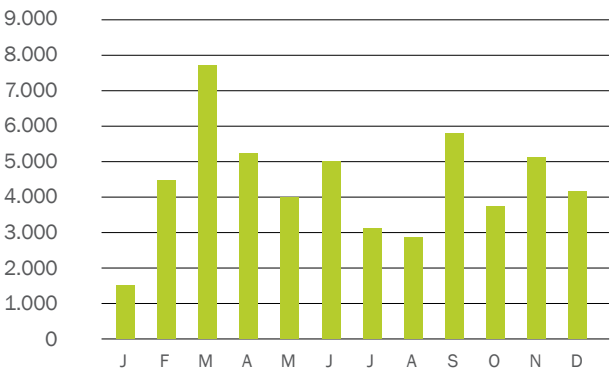
FIGUR 3

Hændelser om brud på ophavsretten



FIGUR 4

Sager om systemer, der potentielt kan misbruges til DDoS-angreb



3.6. > MALWARE-UDVIKLINGEN

Trojanske heste var igen i 2015 langt den hyppigste form for skadelig software (malware) på danskernes pc'er. Ifølge statistikker fra sikkerhedsfirmaet F-Secure udgjorde trojanske heste 84 procent af de skadelige programmer, firmaet fandt i Danmark (se Figur 5). En trojansk hest er et skadeligt program, der giver sig ud for at være ufarligt.

Exploits er angrebsprogrammer, der udnytter kendte sårbarheder til at få adgang til en computer. De tegnede sig for 11 procent af malware-angrebene i 2015.

Den mest udbredte trussel i 2015 kalder F-Secure Trojan:JS/Redirector (se Figur 6). Navnet dækker over en stor gruppe af programmer, der alle videresender besøgende på et websted til et andet. Formålet er som regel at forsøge at inficere den besøgende computer med flere skadelige programmer.

Det sker gerne via et såkaldt exploit kit, der kører på en webserver. Når en browser besøger et exploit kit, afprøver det en række velkendte angreb, der udnytter sårbarheder i browseren, plug-ins eller styresystemet. Har den besøgende computer blot én af sårbarhederne, bliver den inficeret. I 2015 blev danske computere især udsat for exploit kits af typen Angler og Nuclear.

Nummer to på topti-listen er forskellige former for malware, der spredes via Microsoft Office-dokumenter. Ofte er den skadelige kode makroer, der er indlejret i dokumentet. Når makroen kører, hentes og installeres yderligere skadelige programmer. I 2015 var det ofte Dridex, der indrullerer pc'en i et botnet. Formålet er at få fat i offerets adgangskode til netbank og andre tjenester. Skønt Dridex ikke er på topti-listen, så F-Secure den hyppigt på danske pc'er i 2015.

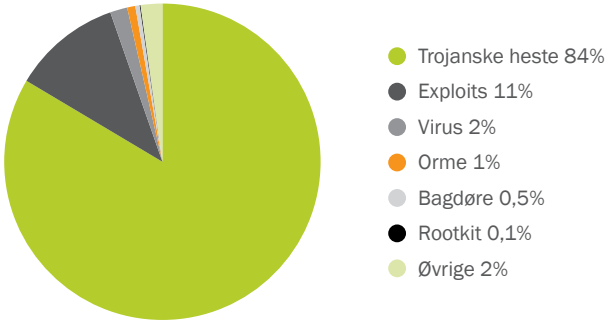
Tallene dækker både over computere, der blev renset for infektioner, og computere, hvor antivirusfirmaet forhindrede et forsøg på infektion.

DKCERT mener:

De it-kriminelle har fundet frem til den mest effektive metode til at inficere ofrenes computere med malware: Diverse afarter af trojanske heste. Det er positivt, at de fleste danskere er klar over truslen og anvender et antivirusprogram. Det fremgår af "Borgernes informationssikkerhed". Men antivirusprogrammer kan ikke fange alle trusler, så brugerne bør supplere dem med andre beskyttelsesmekanismer. Det kan fx være filtre til at beskytte mod skadeligt indhold på websider.

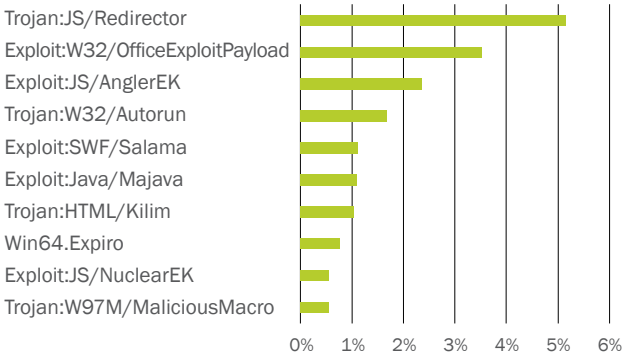
FIGUR 5

Fordeling af malware i Danmark 2015. Kilde: F-Secure



FIGUR 6

De ti mest udbredte skadelige programmer i Danmark. Kilde: F-Secure



3.7. > DEFACEMENTS

Defacement-angreb er en trussel mod websteder. En angriber hacker sig ind på webstedet og placerer sine egne websider på det. Formålet kan være at sprede politisk propaganda eller at prale over for andre hackere.

I 2015 var der en stigning på 29 procent i antallet af defacements af danske websteder i forhold til 2014: 4.304 danske domæner blev overtaget mod 3.345 året før[1]. Der er dog stadig langt op til rekorden i 2011, hvor 11.662 websteder blev ramt (se Figur 7).

Årsagen kan være, at defacements er blevet en specialitet, som en lille skare af hackere foretager. Det fremgår også af, at nogle defacements holdes skjult: I stedet for at overtage webstedets indgangsside placerer hackerne deres sider på undersider, som der ikke er links til. Man skal derfor kende den nøjagtige adresse for at se siden. Dermed er det muligt, at ejeren af webstedet ikke opdager, det er hacket. Årsagen kan være, at hackerne ikke er interesserede i, at den brede befolkning ser siderne – de udfører kun angrebene for at vise sig over for andre hackere.

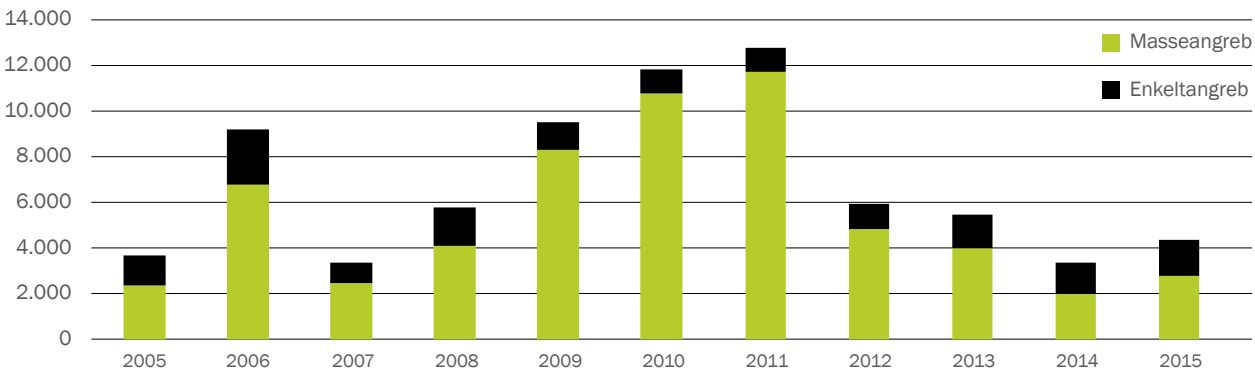
De fleste angreb var masseangreb, hvor flere domæner på samme IP-adresse blev overtaget i ét hug. Den type angreb kan typisk lade sig gøre på webhoteller, der ikke har gennemført en sikkerhedsmæssig opdeling af de forskellige kunders websteder.

DKCERT mener:

Det er positivt, at mængden af defacements fortsat er på et lavt niveau. Men overgangen til skjulte defacements medfører en risiko for, at nogle angreb ikke bliver opdaget.

FIGUR 7

Defacements på dk-domæner 2005-2015. Kilde: Zone-H



3.8. > BORGERNES INFORMATIONSSIKKERHED

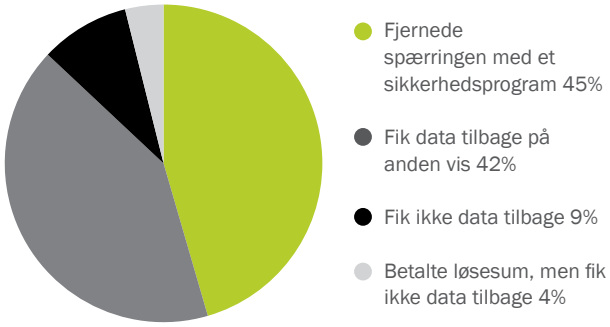
DKCERT gennemførte for Digitaliseringsstyrelsen undersøgelsen "Borgernes informationssikkerhed 2015"[2]. Her spurgte vi blandt andet om udbredelsen af ransomware; det vil sige skadelig software, der spærrer for adgangen til data. Syv procent af deltagerne havde været udsat for ransomware. 45 procent af dem angav at have brugt et sikkerhedsprogram til at fjerne spærringen. 42 procent fik deres data tilbage på anden vis. Ingen fik data tilbage ved at betale løsesum (se Figur 8).

61 procent af de adspurgte tager ikke sikkerhedskopi af data på deres pc med jævne mellemrum (se Figur 9). For data på smartphone eller tablet er tallet 68 procent.

Undersøgelsen viste også, at 57 procent bruger den samme adgangskode til flere tjenester på nettet (se Figur 10).

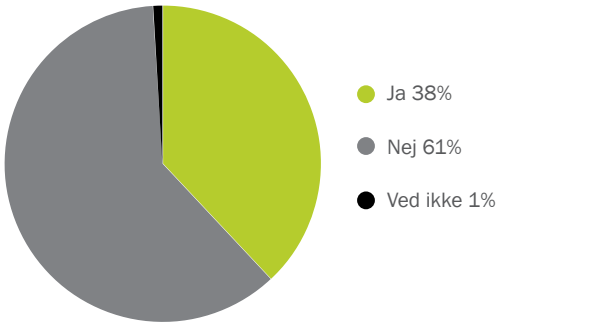
FIGUR 8

Fire procent af ofrene for ransomware betalte løsesummen, men fik ikke deres data tilbage



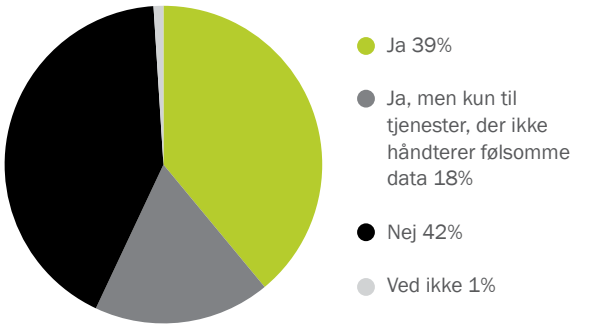
FIGUR 9

61 procent tager ikke jævnligt sikkerhedskopi af data på deres pc



FIGUR 10

57 procent bruger den samme adgangskode til flere onlinetjenester



3.9. > ÅRETS SÅRBARHEDER

National Vulnerability Database registrerede i 2015 i alt 6.488 nye sårbarheder[3]. Det er et fald på 18 procent i forhold til 2014, der satte rekord med 7.937 sårbarheder (se Figur 11). En større andel af sårbarhederne var vurderet til at være alvorlige end i 2014. Alvorlige sårbarheder er her defineret som dem, der har en CVSS-værdi på 7 eller derover.

3.10. > SÅRBARHEDSSCANNINGER

Efter et års pause genoptog DKCERT i 2015 de regelmæssige scanninger efter sårbarheder på it-systemer på forskningsnettet. Pausen i 2014 blev benyttet til at sætte et nyt scanningssystem i drift. Vi har udbygget med ny hardware, software og kompetencer, så scanningerne kan blive mere præcise og brugbare for institutionerne.

I 2015 scannede DKCERT 192.573 IP-adresser fordelt på alle landets universiteter samt visse andre institutioner på forskningsnettet. Der er ikke tale om unikke adresser, idet nogle af dem blev scannet flere gange. Derfor er det mere relevant at se på, hvor mange IP-adresser der svarede på vores scanning: 8.904. Det er dobbelt så mange, som der typisk svarede på scanningerne i de foregående år.

De adresser, der svarede, blev scannet for kendte sårbarheder med programmet Nessus Enterprise. Scanningerne fandt sårbarheder på 2.312 adresser. Med andre ord var der sårbarheder på 26 procent af de IP-adresser, vi var i kontakt med. Det er lidt flere end i 2013, hvor tallet var 21,2 procent.

Scanningerne afdækkede 542 forskellige sårbarheder. Den mest sårbare IP-adresse havde 183 sårbarheder. Dertil skal dog bemærkes, at det var en webserver, der svarede på 10 porte. Så det reelle antal sårbarheder på maskinen er væsentligt lavere.

3.10.1. > FÆRRE ER ALVORLIGE

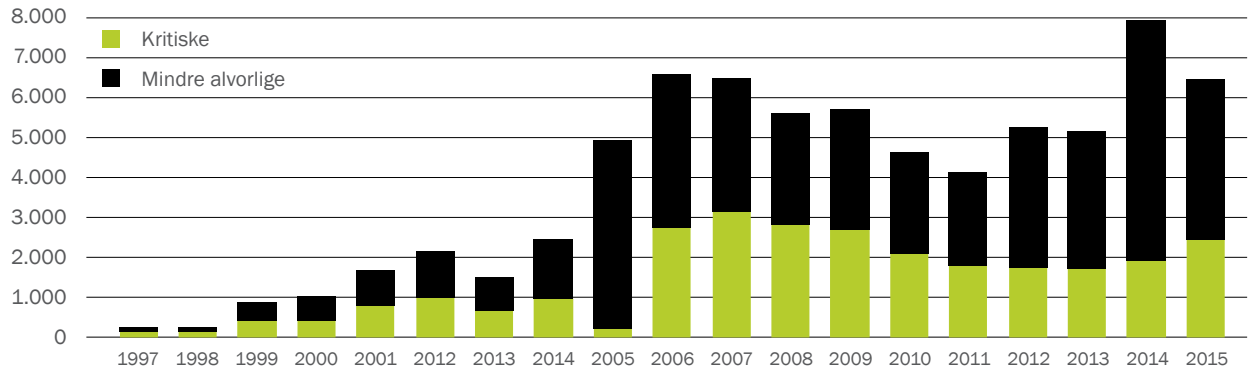
Alle sårbarheder er registreret med de CVE-numre (Common Vulnerabilities and Exposures), som de er opført under i National Vulnerability Database. Her er der også angivet en risikovurdering baseret på CVSS (Common Vulnerability Scoring System).

Tre ud af fire af de sårbarheder, vi fandt ved scanninger i 2015, er klassificeret som middelalvorlige. Fire procent udgør en høj risiko, og to procent regnes for kritiske (se Figur 12). I alt udgør 94 procent af de fundne sårbarheder enten en risiko vurderet lav eller middel.

Dermed fortsætter en tendens, hvor stadig færre af de fundne sårbarheder er alvorlige eller kritiske. I 2011 var hele 63 procent alvorlige (høj eller kritisk). I de følgende år var det 20 procent, og i 2015 var der altså kun seks procent, der var vurderet til høj eller kritisk risiko (se Figur 13).

FIGUR 11

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



3.10.2. > DE HYPPIGSTE SÅRBARHEDER

Den sårbarhed, som vi fandt flest gange, har betegnelsen "Web Application Potentially Vulnerable to Clickjacking". Den fandt vi 1.371 gange. Sårbarheden er risikovurderet til middel.

Vi har samlet en top fem over de mest kritiske sårbarheder (se Tabel 1).

TABEL 1

Top fem over kritiske sårbarheder

1. Operativsystemet er ikke længere understøttet.
2. PHP er ikke opdateret.
3. HTTP.sys er sårbar (MS15-304).
4. Schannel er sårbar (MS14-066).
5. OpenSSL er ikke opdateret.

Mange af sårbarhederne har relation til SSL (Secure Sockets Layer) og efterfølgeren TLS (Transport Layer Security). Det er teknologier, der bruges til at sikre kommunikationen mellem en browser og en webserver. Men denne sikkerhedsteknologi udgør paradoksalt nok også en trussel, når softwaren ikke holdes opdateret, eller der er fejl i opsætningen. Sårbarheder relateret til SSL/TLS udgjorde næsten halvdelen af alle de sårbarheder, scanningerne afdækkede.

DKCERT mener:

Det er positivt, at stadig færre af de fundne sårbarheder er alvorlige. Derimod er det ikke godt, at der findes sårbarheder på mere end hver fjerde adresse, vi scanner. En mulig forklaring kan være, at vi ikke scannede institutionerne i 2014. Derfor kan der være et efterslæb, som der først skal ryddes op i. Vi håber derfor at finde en mindre andel sårbare servere i scanningerne i 2016.

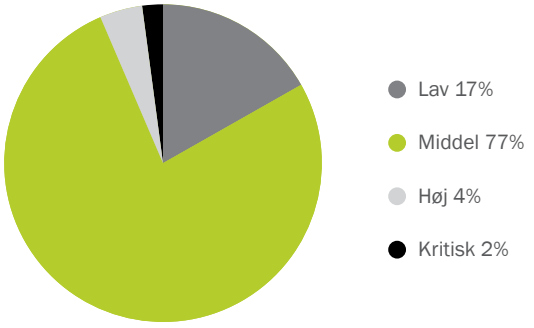
Forældede operativsystemer er den hyppigste af de kritiske sårbarheder. I sommeren 2015 holdt Microsoft op med at understøtte Windows Server 2003. Hvis institutionerne stadig har den i drift, er det på tide at finde en afløser.

TLS og forgængeren SSL er uundværlige teknologier til at beskytte kommunikationen på internettet. Men tallene viser, at der er store problemer med at implementere dem på en sikker måde. Her bør institutionerne sætte ind ved for eksempel at opdatere forældede versioner og certifikater. DKCERT anbefaler, at alle opgraderer til TLS 1.2 og får styr på certifikaterne.

For at understøtte institutionerne i arbejdet med at nedbringe antallet af sikkerhedshuller har DKCERT som mål at scanne alle IP-adresser på alle danske universiteter mindst to gange i 2016. Også de øvrige institutioner på forskningsnettet bør scannes.

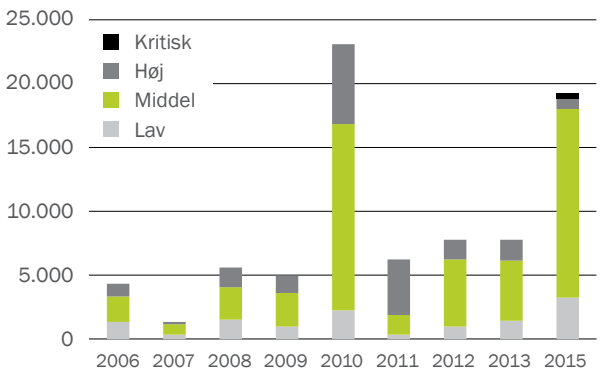
FIGUR 12

94 procent af sårbarheder fundet ved scanninger i 2015 var vurderet til lav eller middel risiko

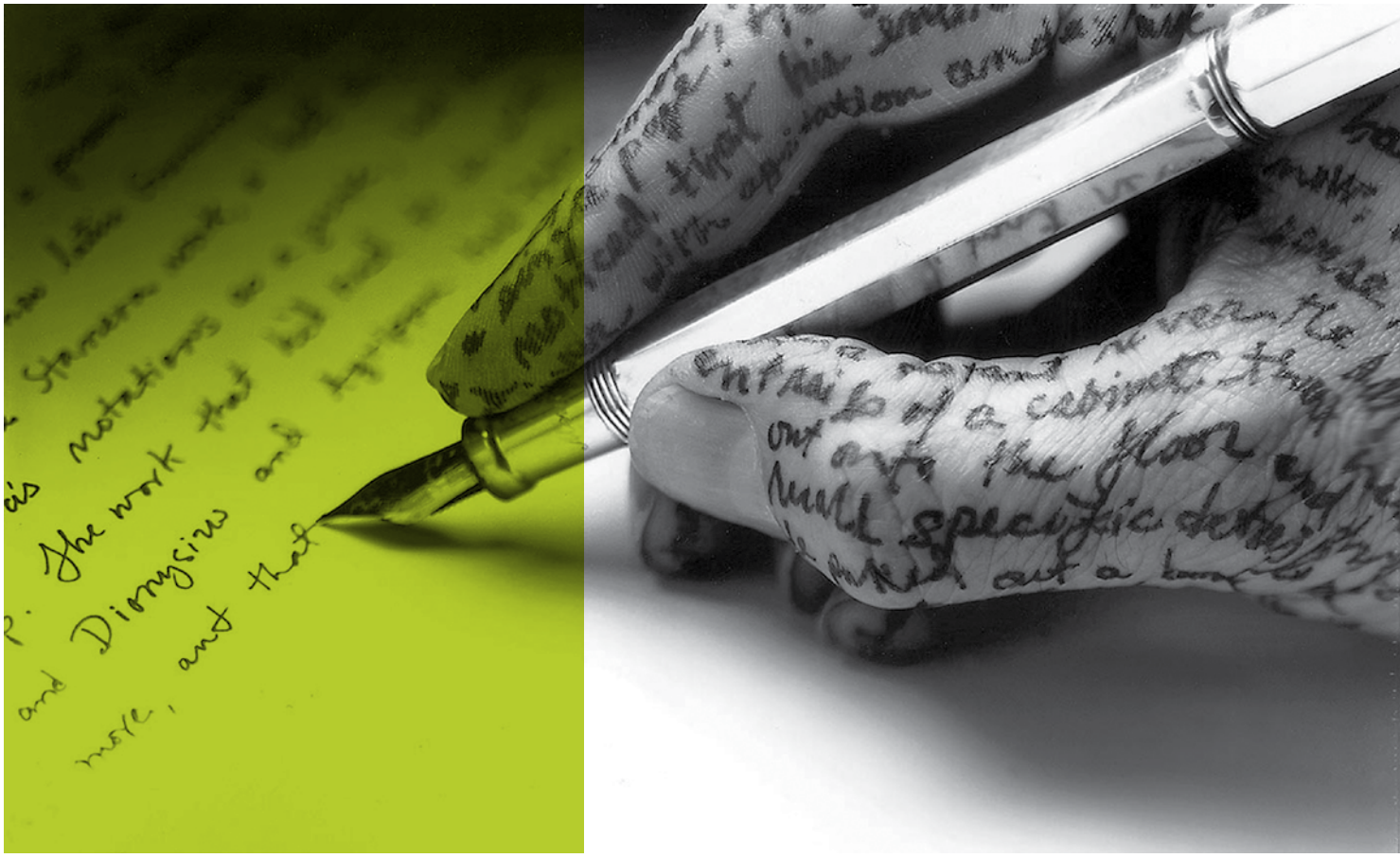


FIGUR 13

Scanningerne afslører flere sårbarheder, men en mindre andel er alvorlige. Årsagen kendes ikke til den store mængde sårbarheder i 2010



4. 2015 - året i ord



DKCERT fik ny chef og et rådgivende organ i form af DKCERT CAB. På sikkerhedsfronten gjorde flere former for digital afpresning sig bemærket.

Henrik Larsen afløste i marts 2015 Shehzad Ahmad som chef for DKCERT. Henrik Larsen kom fra en stilling som informationssikkerhedschef på koncernniveau ved Københavns Universitet. 2015 blev det første år, hvor DKCERT CAB gav strategisk rådgivning om udviklingen af tjenesten.

4.1. > DKCERTS AKTIVITETER I ÅRETS LØB

4.1.1. > DKCERT-CAB

Til at rådgive DKCERT om strategien er der udpeget et DKCERT CAB (Change Advisory Board). DKCERT CAB holdt sit første møde den 29. maj og nåede yderligere to møder i 2015. Som formand er informationssikkerhedschef Ole Boulund Knudsen, Aarhus Universitet, udpeget. De øvrige medlemmer er informationssikkerhedschef Henrik Rask, Aalborg Universitet, it-souschef Mads Sinkjær Kjærgaard, Roskilde Universitet og netværksadministrator Lasse Birnbaum Jensen, Syddansk Universitet.

4.1.2. > INFORMATION OG OPLYSNING

I 2015 fik DKCERT en fastansat kommunikationsmedarbejder, der opdaterer hjemmesiden og Twitter næsten dagligt med sikkerhedsnyheder. Der udsendes ugentlige nyhedsbreve om it-sikkerhed til universiteterne, borgerne og små og mellemstore virksomheder. Ved udgangen af året havde DKCERT 1.084 følgere på Twitter.

I årets løb blev chefen for DKCERT, Henrik Larsen, jævnligt interviewet af medierne om aktuelle sikkerhedsemner. Han holdt også flere indlæg på konferencer og andre møder. Hver måned bragte Computerworld en klumme af Henrik Larsen om informationssikkerhed.

DKCERT bidrog endvidere til planlægning og afvikling af DeIC konference 2015, hvor sikkerheds-temaet var bredt repræsenteret.

For tredje år i træk udarbejdede DKCERT undersøgelsen "Borgernes informationssikkerhed" for Digitaliseringsstyrelsen. Talmaterialet blev indsamlet af Danmarks Statistik i oktober. Rapporten blev offentliggjort i januar 2016.

4.1.3. > NY INFRASTRUKTUR

I juli afsluttede DKCERT et længere arbejde med at implementere en ny it-infrastruktur. Samtidig blev nye informationskilder føjet til sagsbehandlingssystemet. Det betyder, at flere advarsler om potentielt sårbare systemer og andre trusler mod sikkerheden behandles og udsendes automatisk.

4.1.4. > INTERNATIONALE AKTIVITETER

DKCERT er siden 1993 fuldt medlem af det globale netværk FIRST (Forum of Incident Response and Security Teams), der består af mere end 300 CERT/CSIRT-teams fra hele verden. DKCERT deltog i FIRST's europæiske workshop i januar og den globale konference i juni i Berlin.

I 2000 var DKCERT blandt initiativtagerne til grundlæggelsen af det europæiske fællesskab for Computer Incident Response Teams, Trusted Introducer. Vi har siden 2003 været akkrediteret medlem af denne organisation, som også kaldes TF-CSIRT (Task Force on Computer Security Incident Response Teams). TF-CSIRT er tilknyttet GÉANT, de europæiske forskningsnetværks samarbejdsorganisation. DKCERT har deltaget i to af TF-CSIRT's tre møder i 2015: I januar, hvor det blev afholdt sammen med FIRSTs workshop på Gran Canaria, og i september i Tallinn.

DKCERT har et nært samarbejde med NORDUnet CERT og de øvrige nordiske forskningsnet-CSIRT'er. Dette netværk har siden NORDUnets workshop i København i september 2015, hvor CERT/CSIRT'erne holdt et særskilt møde, holdt videomøder en gang om måneden.

Endelig deltog DKCERT-medarbejdere i BlackHat/DefCon-konferencen i Las Vegas i august og i ISACA's europæiske konference og workshops, "EuroCACS/ISRM" i december i København.

4.2. > TENDENSER OG TRUSLER

Afpresning var et nøgleord i 2015. Både internationalt og i Danmark blev ofre udsat for afpresning af it-kriminelle. Det skete primært på to måder: Via ransomware og DDoS-angreb.

4.2.1. > RANSOMWARE

Ransomware er skadelige programmer, der lukker for offerets adgang til data eller programmer. Tidligere var programmerne ofte ret enkle: De viste et skærmbillede, der hævdede, at der var lukket for adgang. Men hvis brugeren kunne lukke programmet ned, var der reelt ikke spærret for noget.

I 2015 var mere ransomware af typen, der krypterer data. Brugerens filer findes stadig på pc'en, men de er krypteret. Offeret må betale en løsesum for at få udleveret nøglen, der kan dekryptere filerne.

Som noget nyt dukkede der i 2015 for første gang ransomware op, der kørte på Linux-platformen. Programmet Linux.Encoder.1 viste sig dog at være programmeret på en måde, så det var muligt for et sikkerhedsfirma at dekryptere data uden at betale penge til bagmændene[4].

DKCERT mener:

Truslen fra ransomware understreger behovet for en effektiv backupstrategi. Hvis man har en offline kopi af data, kan man let få dem tilbage, efter at ransomware har krypteret dem. Derfor er det uheldigt, at 61 procent af de danske borgere ikke tager sikkerhedskopi af deres computer med jævne mellemrum.

4.2.2. > DDOS-AFPRESNING

Også i 2015 var der flere eksempler på angreb med trusler om at sætte et websted ud af drift, såkaldte DDoS-angreb (Distributed Denial of Service). Typisk foregår et angreb ved, at bagmændene først sender en stor mængde data mod webstedet i en kortere periode. Når de på den måde har bevist, at de kan få webstedet til at gå ned, sender de en mail til virksomheden. Her truer de med gentagne angreb, hvis man ikke betaler et beløb til en Bitcoin-tegnebog.

I nogle tilfælde har angrebene anvendt såkaldt UDP-forstærkning. Det vil sige, at de udnytter åbne netværkstjenester, der anvender UDP-protokoller (User Datagram Protocol). Det kan fx være DNS (Domain Name System), NTP (Network Time Protocol) eller SSDP (Simple Service Discovery Protocol). Tjenesterne kører hos organisationer, der uden at vide det bliver misbrugt til angreb: Bagmændene sender forespørgsler til de åbne tjenester. Afsenderadressen i forespørgslen er forfalsket, så den svarer til offerets IP-adresse. Tjenesten sender derfor svaret til den forfalskede adresse. I nogle tilfælde fylder svaret meget mere end forespørgslen – på den måde kan angriberen ved at afsende få bytes forårsage et angreb med store datamængder.

I årets løb så DKCERT flere eksempler på, at UDP-baserede tjenester på forskningsnettet blev misbrugt til den type angreb.

DKCERT mener:

Danske organisationer skal lukke for ekstern adgang til UDP-tjenester, så de ikke kan misbruges til DDoS-angreb.

4.2.3. > LÆKAGER AF FORTROLIGE DATA

Fortrolige data om personer kom også i 2015 i de forkerte hænder. Årets mest omtalte lækage var hackerangrebet på tjenesten Ashley Madison. Tjenesten er rettet mod personer i et fast forhold, der er interesseret i en affære. Derfor var det problematisk for mange af dens brugere, at deres navne og øvrige oplysninger blev offentliggjort. It-kriminelle forsøgte da også at udnytte dataene til afpresning mod de registrerede brugere, idet de truede med at kontakte deres ægtefæller og kolleger.

Andre store tilfælde af datalækage var Trump- og Hilton-hotelkæderne og den offentlige myndighed Office of Personnel Management.

Open source-databasen DataLossDB[5] registrerede i 2015 i alt 1.472 sager med tab af fortrolige data (se Figur 14). Det er en stigning på 15 procent i forhold til 2014.

USA's Identity Theft Resource Center[6] registrerede 781 sager, idet de opgør dem efter andre kriterier end DataLossDB. Centeret registrerede i alt 169 millioner dataposter, der kom i de forkerte hænder som følge af lækagerne. To ud af tre dataposter stammede fra systemer inden for sundhedssektoren.

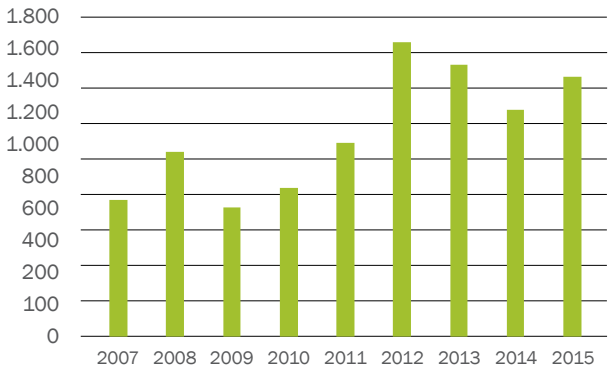
For it-sikkerhedsfolk var især én sag interessant: Angrebet på Hacking Team. Dette hackerangreb førte til offentliggørelse af fakta om firmaets kunder og produkter. Det var interessant, fordi firmaet fremstiller software til overvågning og spionage. Kunderne er offentlige myndigheder, politi og private virksomheder. Blandt de lækkede data var kildekode til et program, der udnyttede et hidtil ukendt sikkerhedshul i Adobe Flash Player[7].

DKCERT mener:

Stadig større dele af borgernes data ligger i databaser hos myndigheder og private virksomheder. Derfor er der brug for bedre beskyttelse af persondata. EU's persondataforordning kan blive et skridt mod en mere effektiv beskyttelse med bedre håndhævelse af reglerne.

FIGUR 14

Sager med tab af fortrolige data. Kilde: DataLossDB



4.2.4. > SIKKERHED PÅ MOBILE ENHEDER

Android var igen i år den foretrukne platform for udviklere af skadelige programmer til mobile enheder[8]. Brugere i Danmark bliver dog sjældent ramt, da Google formår at holde de fleste skadelige apps ude af Play Store. De spredes i højere grad gennem alternative app-butikker, der er populære i Asien, men ikke i Europa.

Undersøgelsen "Borgernes informationssikkerhed 2015"[2] viste da også, at kun fire procent af deltagerne havde downloadet en app til smartphone eller tablet, der viste sig at være skadelig.

Et usædvanligt angreb på Apples iOS-platform blev opdaget i september. En række apps fra Kina i den officielle App Store var inficeret med skadelig kode. Årsagen viste sig at være udviklingsværktøjet Xcode: Bagmænd havde inficeret værktøjet med koden og distribueret den inficerede version til udviklere af apps. På den måde blev en lang række apps inficeret. Truslen blev kendt under navnet XcodeGhost[9].

DKCERT mener:

Endnu er truslen fra skadelige apps på smartphones og tablets begrænset. Der findes masser af malware til især Android, men hovedparten når aldrig ud på danske brugeres enheder. Alligevel bør brugere og administratorer være opmærksomme på, at en smartphone er en computer og skal beskyttes lige som alle andre computere. Det gælder ikke kun beskyttelse mod malware, men også sikring af fortrolige data på enheden.

4.2.5. > TRUSLER MOD INTERNET OF THINGS

To sikkerhedsforskere demonstrerede i juli 2015 for første gang, at det var muligt at hacke sig ind på en kørende bil. De kunne både styre rattet, bremserne og underholdningssystemet. Det var en sårbarhed i netop underholdningssystemet, der gav dem mulighed for at fjernstyre den pågældende Jeep. Fiat Chrysler udsendte en sikkerhedsopdatering, der skulle lukke hullet[10].

Demonstrationen er et eksempel på sårbarheder i det, der kaldes for Internet of Things. Det er en samlebetegnelse for udstyr, der ikke er computere eller smartphones, men som alligevel indeholder software og kommunikerer over internettet. Foruden moderne biler kan det være termostatudstyr, webkameraer, smart-tv, babyalarmer, trådløse routere og meget andet udstyr. Det har fx været demonstreret, at en sårbar, internetopkoblet el-kedel kunne afsløre nøglen til husets trådløse netværk[11].

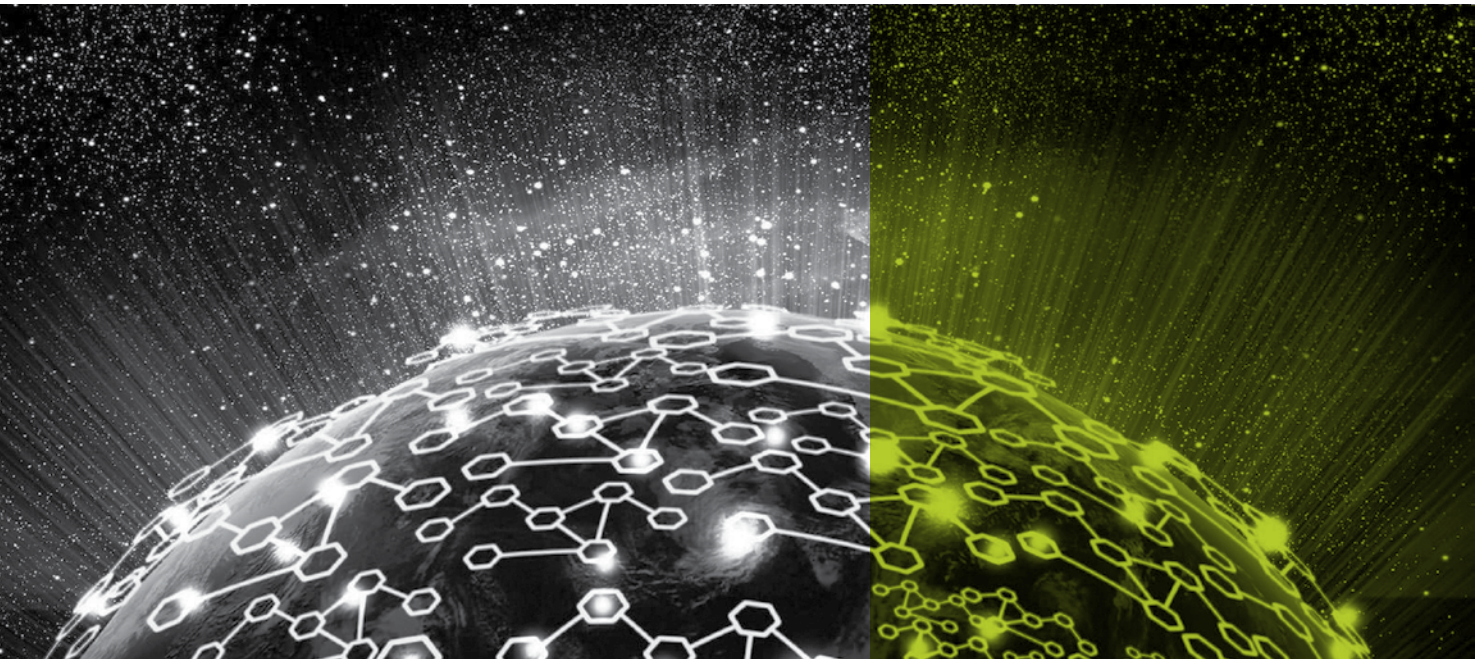
Mange sikkerhedsfolk ser Internet of Things som en forestående sikkerhedskatastrofe. Det skyldes flere ting: Udviklerne af apparaterne har sjældent tænkt sikkerheden ind i produktet under produktudviklingen. De er ikke gode til at udsende sikkerhedsopdateringer, der kan lukke sikkerhedshuller. Og bliver opdateringerne endelig udsendt, opdager brugerne det ikke – eller de er ikke klar over, hvordan de skal installere dem. Det er forholdsvis let at installere de månedlige opdateringer til Windows, men hvordan opdaterer man sin babyalarm?

DKCERT mener:

Demonstrationen af sårbarheden i Jeep-bilerne er et forvarsel om, hvad vi vil se i den kommende tid. Flere Internet of Things-apparater vil vise sig at være sårbare. I nogle tilfælde vil sikkerhedsforskere opdage det, i andre når de it-kriminelle at udnytte dem.

Producenterne skal være opmærksomme på, at når der indgår netværksopkoblede computere i deres apparater, skal de sikres på lige fod med "rigtige" computere. De skal tænke sikkerheden ind i produktudviklingsprocessen.

5. Det eksterne perspektiv



Fire bidragydere uden for DKCERT giver her deres syn på EU's persondataforordning.

De seneste 3-4 år har et stort samtaleemne blandt informationssikkerhedsfolk været den kommende EU-persondataforordning (General Data Protection Regulation, GDPR), der skal afløse Persondatadirektivet fra 1995. Efterhånden er snakken også nået ind på ledelsesgangene, hvor forordningen er blevet imødeset med blandede følelser.

Den danske persondatalov og tilhørende sikkerhedsbekendtgørelse er fra år 2000 og bygger på direktivet fra 1995. De trænger til en modernisering. Udviklingen - både hvad angår mængden og typen af personhenførbare data, der er blevet samlet op af offentlige myndigheder og private virksomheder, og hvad angår omfanget af både tilfældige læk og bevidste angreb – er gået stærkt i de forløbne år.

Debatten har krævet opstramning af sikkerheden og skærpet mulighed for at straffe de ansvarlige for datalæk.

Det har medført, at databeskyttelsesforordningen har været ventet med en blanding af forventning og frygt. Blandt sikkerhedsprofessionelle har det været set som en tiltrængt fornyelse af lovgivningen og som et instrument til få forretningen og ledelsen til at øge fokus på sikkerhed og til en nødvendig opstramning af processer og politikker. Andre har frygtet et øget bureaukrati og bøder, der kunne være livstruende for forretningen, for selv mindre, tilfældige og utilsigtede sikkerhedshændelser.

Nu er forordningens tekst kendt. Den ventes ganske vist først formelt vedtaget senere på foråret, men parterne har færdigforhandlet indholdet, så teksten er kendt – bortset fra en række bestemmelser, hvor der skal udfyldes med national lovgivning eller praksis. Forordningen vil træde i kraft to år fra den dato, hvor den er endeligt vedtaget. Det er ikke lang tid til at tilpasse processer og procedurer og få styr på institutionens behandling af persondata.

DKCERT har derfor bedt fire eksperter om at belyse indholdet og betydningen af de nye regler, som får afgørende betydning for arbejdet med databeskyttelse i de kommende år.

Nedenfor får vi således advokat Marie Albæk Jacobsens beskrivelse af de nye krav. Informationssikkerhedschef Henrik Rask beskriver, hvordan Aalborg Universitet planlægger at leve op til forordningen, og sikkerhedschef René Hedegaard Hansen, Terma, ser på de nye krav fra en privat virksomheds vinkel. Endelig beretter seniorjurist Anette Høyrup, Forbrugerrådet Tænk, om den betydning den nye forordning får for beskyttelsen af forbrugernes data.

Et gennemgående tema i bidragene er datastrømsanalyse. DKCERT anbefaler, at institutionerne hurtigst muligt igangsætter arbejdet med at kortlægge opsamling, behandling og lagring af personhenførbare data.

5.1. > PERSONDATAFORORDNING STILLER NYE KRAV

Af advokat Marie Albæk Jacobsen, Bech-Bruun

Den 15. december 2015 blev de tre EU-institutioner - Parlamentet, Kommissionen og Rådet - enige om den endelige tekst til den nye persondataforordning, der har været undervejs siden 2012.

Persondataforordningen blev fremsat med to primære formål: Harmonisering af reguleringen af behandlingen af personoplysninger inden for EU og sikring af en bedre retsstilling for datasubjektet (den registrerede).

Den gældende persondatalov hviler på et EU-direktiv, der er blevet implementeret forskelligt fra land til land. Persondataforordningen skal derfor sikre ensartet regulering på tværs af EU og dermed lette de administrative byrder for virksomheder og organisationer.

Ved en gennemgang af den endelige ordlyd af persondataforordningen kan man dog konstatere, at EU-institutionerne ikke helt er nået i mål. Der er således fortsat mulighed for national regulering inden for bestemte områder. Derimod er den registrerede borgers retsstilling blevet væsentligt forbedret. Det sker blandt andet gennem adgangen til dataportabilitet, retten til at blive glemt, samt strengere samtykkekrav.

Den store bevågenhed om persondataforordningen skyldes ikke mindst, at den indfører et hidtil uset bødeniveau på op mod 20 millioner euro eller fire procent af en virksomheds/koncerns globale omsætning ved overtrædelse af forordningen. For så vidt angår offentlige myndigheder og institutioner, er det overladt til de enkelte medlemsstater at træffe beslutning om, hvorvidt de skal underlægges samme bødeniveau som private virksomheder.

5.1.1. > SKÆRPEDE KRAV

Persondataforordningen skærper en del af de krav til behandlingen af personoplysninger, som allerede i dag gælder efter persondataloven. Det gælder kravene til indholdet af databehandleraftaler, oplysningsforpligtelsen over for datasubjektet, notifikationsforpligtelse i tilfælde af sikkerhedsbrud mv.

Herudover introducerer Persondataforordningen en række nyskabelser, hvoraf særligt tre er relevante i denne sammenhæng: Accountability, Data Protection by Design/by Default og Data Protection Officer (DPO).

5.1.2. > ACCOUNTABILITY

Den dataansvarlige skal kunne dokumentere, at behandlingen af personoplysninger opfylder de grundlæggende behandlingskrav. Heri ligger, at behandlingen alene sker til saglige formål, og at der ikke behandles flere personoplysninger end nødvendigt i forhold til formålet. Endvidere skal den dataansvarlige også være i stand til at redegøre for datastrømmene i virksomheden/organisationen og implementere passende persondatapolitikker.

5.1.3. > DATA PROTECTION BY DESIGN/DATA PROTECTION BY DEFAULT

Bestemmelserne vedrørende data protection by design/by default skal sikre, at virksomheder/organisationer indtænker persondatabeskyttelse som et fast element i udviklingen og/eller indkøb af eksempelvis nye it-systemer, nye produkter, apps, mv.. Det kan for eksempel ske gennem pseudonymisering af personoplysninger.

5.1.4. > DATA PROTECTION OFFICER (DPO)

Både dataansvarlige og databehandlere inden for det offentlige skal udpege en DPO (Data Protection Officer). Private virksomheder skal udpege en DPO, hvis virksomhedens kerneaktiviteter er systematisk og omfattende monitorering af datasubjekter eller omfattende behandling af følsomme oplysninger eller oplysninger om strafbare forhold. DPO'ens arbejdsområde bliver primært at sikre overholdelse af persondataforordningen og være kontaktperson i relation til Datatilsynet.

Særligt i relation til forskning er det endvidere værd at nævne, at persondataforordningen nu åbner op for, at datasubjektet kan give samtykke til forskning inden for bestemte områder, fordi det ikke, på det tidspunkt personoplysningerne indsamles, altid er muligt at fastlægge projektets specifikke omfang.

5.1.5. > IKRAFTTRÆDEN

Persondataforordningen forventes at blive endeligt vedtaget medio februar. Herefter begynder en toårig transaktionsperiode, så forordningen træder endeligt i kraft primo 2018.

Selvom persondataforordningen først træder i kraft om to år, bør virksomheder og organisationer allerede nu begynde at danne sig et overblik over behandlingen af personoplysninger, så udarbejdelse af relevante politikker og procedurer kan iværksættes og implementeres i god tid forinden.

5.2. > SÅDAN VIL AALBORG UNIVERSITET LEVE OP TIL PERSONDATAFORORDNINGENS KRAV

Af informationssikkerhedschef Henrik Rask, Aalborg Universitet

Aalborg Universitet (AAU) har gennem nogen tid interesseret sig for EU's persondataforordning. Det skyldes ikke mindst, at vi har erkendt, at det formodentlig bliver en stor opgave at indføre den i et universitetsmiljø som AAU's.

Kravene i den kommende forordning er for en stor dels vedkommende ikke nye krav – men "blot" flere krav om øget dokumentation, organisering, systematisering og processer.

Allerede i dag forventes det, at vi har eller kan skabe et overblik over, hvilke behandlinger vi foretager og hvilke typer af personoplysninger der behandles.

Forordningen opererer med, at vi skal have ét centralt sted, hvor der er overblik over alle de databehandlinger, vi foretager.

Der skal blandt andet derfor udpeges en Data Protection Officer (DPO). Det er en nyskabelse i forhold til den nuværende persondatalov. Der bliver stillet krav til faglige kvalifikationer og ekspertise for en DPO. Vedkommende skal også være uafhængig (organisatorisk placering). DPO'en får ansvaret for specifikke opgaver i forbindelse med databeskyttelse (se faktaboks om DPO).

Hvad skal der så til, for at AAU får styr på opgaven?

5.2.1. > OVERBLIK OVER DATASTRØMME

Først er vi nødt til at skabe fuldstændigt overblik over, hvordan datastrømme med persondata flyder.

Arbejdet bliver meget omfattende. Der findes uden tvivl mange tusinde datastrømme, der skal identificeres og dokumenteres. Den dokumentation har vi i dag kun i meget begrænset omfang.

I forbindelse med at vi afdækker datastrømme, skal vi klassificere data. Hvilke data er almindelige persondata og hvilke er særlige persondata? Klassifikation af data bliver et centralt og væsentligt element i kravene til fremtidig håndtering af data.

Det at klassificere data er nemt – i teorien. I praksis har det vist sig at være en rigtig svær øvelse. Jeg tror personligt, at dette bliver en af de helt store opgaver at implementere og forstå for alle interessenter på AAU.

Når der er styr på datastrømme og klassifikationer, skal vi udføre "Privacy Impact Assesments" (PIA's) for behandling af personoplysninger, som kan indebære specifikke risici for den registreredes rettigheder. Det er et af de krav, der ikke har været specifikt stillet i den nuværende persondatalov. En PIA udløser også krav til, at AAU's risikovurderinger skal inkludere persondata og risici forbundet med behandling af dem.

5.2.2. > KONSEKVENSER FOR EKSISTERENDE LØSNINGER

Indbygget databeskyttelse, privacy by design, er et krav, der kan betyde, at eksisterende tekniske løsninger skal ændres over tid. Vi er derfor nødt til allerede nu at have det i tankerne, så vi ikke kommer til at skulle lave for meget om af det, vi indfører i de kommende år.

Der tales også om "databeskyttelse via indstillinger" – privacy by default. Det medfører, at persondatabeskyttelse skal være standarden for AAU og de systemer, der anvendes til behandling af persondata. Også her er det min forventning, at der bliver en stor opgave i forhold til eksisterende systemer.

5.2.3. > STOR OPGAVE MED DOKUMENTATION

Hele området omkring dokumentation forventes at blive en betydelig opgave. Det har sådan set været et krav længe, men nu strammes der op med flere formelle og specifikke krav.

Vi skal fremover sikre, at vi centralt har fuldstændig dokumentation over alle vore behandlinger af persondata.

Dokumentationen skal være i en form, der er "egnet til Datatilsynet ved tryk på en knap".

Jeg har tidligere nævnt, at DPO'en får en række opgaver og ansvarsområder. Det er også klart, at han/hun ikke kan udføre dem alene. Det er min forventning, at en DPO får et projektlederansvar for opgaverne. Så må resten af AAU stille med projektdeltagere, for at vi kan komme i mål med projektet.

Det er endnu ikke besluttet, hvor en DPO skal placeres organisatorisk på AAU. Jeg forventer, at der meget snart bliver truffet en beslutning om det.

Der har været talt meget om bøder og bødestørrelser i forbindelse med EU's persondataforordning.

Noget tyder i skrivende stund på, at det offentlige ikke vil blive direkte omfattet (se faktaboks om bøder). Derfor er det ikke bøder, som en DPO kan benytte som "kølle", når han/hun skal sikre fremdrift i projektet. Personligt er min erfaring dog også, at køllemetoden virker rigtig dårlig på langt sigt, selvom det nogle gange kunne være rart med et trumfkort, der slår alle andre hensyn på et universitet.

Det bliver en rigtig spændende opgave at implementere EU's persondataforordning på et universitet – kedeligt bliver det bestemt ikke!

BØDENIVEAU

Det er besluttet, at bødeniveauet hæves til 20 mio. euro. I Danmark kan myndighederne afgøre, hvilke regler og hvilket bødeniveau der skal gælde for offentlige virksomheder:

ARTIKEL 79:
3b. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 53(1b), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

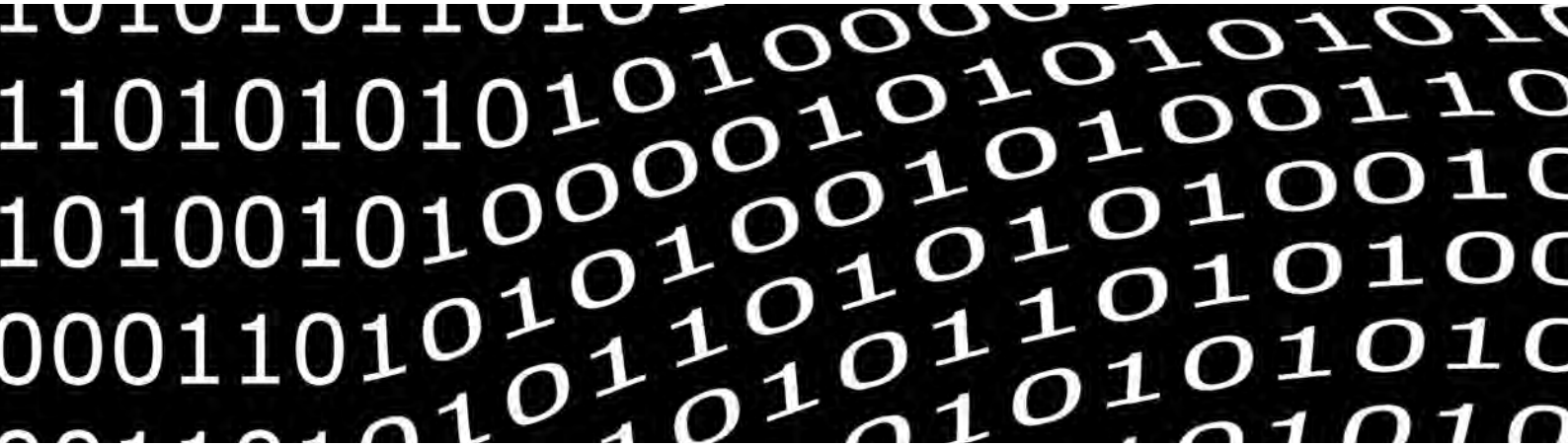
ARTIKEL 120A:
(120a) (new) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark, the fine is imposed by competent national courts as a criminal sanction and in Estonia, the fine is imposed by the supervisory authority in the framework of a misdemeanor procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine.

In any event, the fines imposed should be effective, proportionate and dissuasive.

DPO

Nedenstående er eksempler på opgaver, der formentlig lander på en DPO's opgaveliste:

- Sikre at der forefindes nødvendige databehandleraftaler.
- Sikre gennemførelse af awareness-træning.
- Udføre kontrol og audit af behandlinger.
- Sikre dokumentation for politikker, regler og procedurer.
- Sikre at der forefindes et årshjul for arbejdet.
- Ansvarlig for underretning (til Datatilsyn m.fl.) ved brud på reglerne.



5.3. > KONSEKVENSER FOR EN VIRKSOMHED: SÅDAN VIL TERMA LEVE OP TIL PERSONDATAFORORDNINGENS KRAV

Af sikkerhedschef René Hedegaard Hansen, Terma

Indledningsvis skal det understreges, at EU's persondataforordning i skrivende stund formelt set endnu ikke er endeligt vedtaget. Den foreløbige analyse, der ligger til grund for denne artikel, kan derfor nå at ændre sig, inden implementeringsfasen begynder.

Terma er en højteknologisk virksomhed med cirka 1.300 medarbejdere på globalt plan, hvoraf omkring 85 procent er ansat inden for EU. Terma arbejder med viden og produktion inden for forsvars- og rumfartsindustrien, hvor der stilles særdeles høje kvalitetskrav til produkter og håndtering af informationer. Vi kan derfor betegnes som en "compliance driven" organisation.

Det betyder, at langt størstedelen af vores arbejdsprocesser er understøttet af skriftlige politikker og procedurer. Det gælder også de processer, som i særlig grad involverer håndtering af persondata, hvilket primært vil sige vores personaleadministration. Her skal vi sørge for at håndtere de krav, som allerede i dag følger af persondataloven. Det overordnede ansvar for overholdelse af persondataloven er placeret i Termas juridiske afdeling. Det er også her, de forskellige politikker og procedurer beskrives og vedligeholdes.

Set fra sikkerhedschefens stol vil den nye persondataforordning ikke bringe revolutionerende ændringer med sig for Termas vedkommende. Helt grundlæggende skal vi stadig beskytte personoplysninger. Vi skal kun indsamle og behandle personoplysninger i det omfang, at der er en saglig, arbejdsrelateret begrundelse. Vi skal fortsat informere den registrerede om, hvilke informationer vi indsamler, hvad vi bruger dem til, og hvornår vi sletter dem.

De væsentligste ændringer, som Terma på nuværende tidspunkt har identificeret, er, at vi skal være endnu skarpere på at kunne dokumentere vores overholdelse af reglerne. Det omfatter dokumentation af, hvilke informationer vi indsamler, hvilke informationer vi behandler (og med hvilket formål), hvor informationerne eventuelt flyttes hen, og hvem der har adgang til dem m.v.

Det arbejde omfatter blandt andet, at vi gennemfører en datastrømsanalyse. Vi sikrer, at de medarbejdere, der behandler persondata, har modtaget den nødvendige træning. Endelig skal vi analysere, om vores procedurer og kontroller omkring elektroniske og fysiske behandlingssystemer, hvor persondata opbevares, er tilstrækkelige. Vi skal desuden være opmærksomme på at få implementeret de skærpede krav til dokumentation for samtykke fra den registrerede.

Terma er i skrivende stund ikke afklaret med hensyn til, om vi har brug for at implementere yderligere tekniske kontrolforanstaltninger til sikring af persondata. Det må afhænge af en nærmere risikoanalyse. Med bødestørrelser på op til fire procent af den globale omsætning eller 20 millioner euro er der fra lovgivers side lagt op til en skærpet kurs over for eventuelle overtrædelser. Det må naturligvis tages med i betragtning, når man laver sin risikoanalyse.

Uanset hvad, så er der ingen tvivl om, at implementeringsopgaven vil blive både ressource- og tidskrævende. Derfor kan jeg kun anbefale andre virksomheder at påbegynde arbejdet snarest muligt.

5.4. > DET BETYDER PERSONDATA-FORORDNINGEN FOR FORBRUGERNE

Af seniorjurist Anette Høyrup, Forbrugerrådet Tænk

Efter cirka fire år og 4.000 ændringsforslag er EU's persondataforordning endeligt vedtaget.

Det oprindelige udspil fra EU-Kommissionen fra 25. januar 2012 var fra et forbrugersynspunkt mere ambitiøst og lagde op til klare forbedringer, men det endelige resultat kan forbrugerne godt være tilfredse med. Samlet set sikrer EU's dataforordning en bedre beskyttelse af vores personlige oplysninger, end den nuværende persondatalov fra år 2000 gør.

5.4.1. > BEDRE KONTROL FOR FORBRUGERNE

Forbrugerne får bedre kontrol med egne oplysninger.

Princippet "right to be forgotten" indføres, så det fremover bliver nemmere for brugerne at få slettet deres oplysninger online. Med princippet pålægges virksomhederne at slette uønskede og ikke-relevante oplysninger hurtigt (udvidet sletteadgang - artikel 17).

Desuden får brugerne mulighed for at flytte deres oplysninger fra en tjenesteudbyder til en anden. Virksomhederne skal dels tilbyde brugerne et samlet overblik over, hvad de har indsamlet, og dels hjælpe med at få eventuelle data overflyttet (dataportabilitet – artikel 18).

Endelig sikres der mulighed for undgå automatisk profilering. Det dækker situationer, hvor ens adfærd på tværs af nettet indsamles, uden at man er klar over det, til brug for målrettet markedsføring (udtrykkeligt samtykke ved profilering - artikel 20).

5.4.2. > SIKKERHEDSBRUD SKAL ANMELDES

Gennemsigtigheden omkring dataindsamling øges gennem en ny anmeldelsespligt for virksomheder. Senest 72 timer efter en virksomhed har opdaget et risikofyldt sikkerhedsbrud, skal den anmelde det til Datatilsynet. De forbrugere, som kan være berørt af databruddet, skal også underrettes. Denne nye forpligtelse bør kunne skabe mere synlighed omkring sikkerhedsniveauet i Danmark (underretningspligt – artikel 31 og 32).

Kravene til virksomheders it-sikkerhed strammes, da der indføres et princip om, at databeskyttelse skal bygges ind i it-løsningernes design. Der er en række forudsætninger, der skal være opfyldt, for at det kræves, så det er endnu uklart, hvor omfattende kravet bliver for virksomhederne (by design and by default – artikel 23 og 30). En anden nyhed, som kan forbedre sikkerheden, er kravet om, at virksomheder i visse situationer er forpligtet til at udarbejde en privatlivskonsekvensanalyse, inden de lancerer en ny tjeneste.

5.4.3. > HÅNDHÆVELSE MED BØDER OG DPO

Mulighederne for håndhævelse forbedres også. Offentlige myndigheder forpligtes til at ansætte en "databeskyttelsesansvarlig", som skal sikre, at alle forhold vedrørende databehandling er i orden. Det samme gælder private virksomheder, idet det dog gøres afhængigt af indhold og omfang af de typer oplysninger, de behandler (Data Protection Officer – artikel 35).

Der indføres højere bøder for overtrædelse af persondataloven og en adgang til at udstede administrative bøder. For private virksomheders vedkommende bliver bødeniveauet på et helt andet niveau, end hvad især danske virksomheder har været vant til. Det vil formentlig få en præventiv effekt til gavn for forbru-

gerne. I modsætning hertil står den offentlige sektor, som formentlig slipper for bødepålæg, da det bliver op til medlemsstaterne at lovgive herom (administrative bøder – artikel 79).

5.4.4. > KRÆVER VELVILJE HOS VIRKSOMHEDERNE

En ting er, hvad der står på papiret, noget andet er, hvordan forbrugerne vil komme til at mærke ændringerne i deres hverdag. De nye stramninger i loven kan ikke stå alene, hvis man vil gøre alvor af forordningens nye rettigheder, sikre privatlivet og dæmme op for hacking.

For at forbedringerne skal få en reel effekt, kræver det velvilje hos virksomhederne - både de offentlige og private. De skal implementere databeskyttelsen i tjenesterne som standard. Sikres rettighederne ikke teknisk, så de faktisk kan håndteres, ændrer reglerne ingenting. Myndighederne skal også have et bredere fokus. De skal være med til at understøtte en digital udvikling, hvor sikkerhed ikke kun handler om at overholde reglerne, men også ligger i selve valget af teknologisk løsning.

Og endelig er der behov for, at forbrugerne rustes til at kunne gennemskue digitale tjenester, håndtere deres oplysninger og forebygge egen sikkerhed. Det bør ske gennem øget forbrugerinformation, så den enkeltes viden og kompetencer styrkes.

FEM FORBEDRINGER FOR FORBRUGERNE

1. Ret til at få slettet oplysninger.
2. Mulighed for at skifte udbyder og få data med.
3. Mulighed for at undgå profilering.
4. Krav om anmeldelse af sikkerhedsbrud.
5. Privatlivsbeskyttelse skal tænkes ind fra begyndelsen.

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. > SVINDLERE AUTOMATISERER MÅLRETTET PHISHING

”Kære <navngiven forsker>. Jeg har for nylig læst din artikel <navn på artikel>. Den er meget nyttig for mit forskningsområde. Jeg vil høre, om du måske kan sende mig følgende artikler til hjælp i mit aktuelle forskningsprojekt?”

Sådan en mail modtog en række danske forskere i januar. Mailen var på engelsk og angav at komme fra en forsker ved et tysk universitet.

Hver mail var stilet til den enkelte forsker personligt. Navn og e-mailadresse var korrekt, og der blev henvist til flere artikler, som modtageren havde publiceret.

Afsenderadressen så umiddelbart rigtig ud: ”<navn>@uni-muenchin.de”. Skulle den have været rigtig, skulle domænet dog have været ”uni-muenchen.de”.

Så der er altså tale om mail-svindel. Oven i købet et særdeles overbevisende svindelnummer: Mailen er målrettet den enkelte forsker og roser vedkommende for en god artikel. Hvem ville ikke reagere positivt på den slags?

6.1.1. > HER KOMMER SVINDLEN IND I BILLEDET

Afsenderen beder forskeren sende et par artikler. I mailen er der link til dem. Og det er her, svindlen kommer ind i billedet.

Det ene link fører til omtalen af en af modtagerens artikler på forskerportalen ScienceDirect. Det andet fører til en forfalsket login-side, der efterligner portalen ved forskerens universitet.

Formålet med hele øvelsen er altså at lokke brugernavn og adgangskode ud af forskeren.

6.1.2. > AUTOMATISERET PROCES

Universitetet modtog et halvt hundrede mails. Alle rettet mod forskellige forskere, og alle med konkrete henvisninger til artikler modtageren havde skrevet.

Jeg antager, at svindlerne har automatiseret processen. De har sikkert taget udgangspunkt i ScienceDirect eller en lignende portal, hvor man kan finde forskeres navne, mailadresser og publikationer.

Så skal der ikke de store evner til at skrive et script, der henter data ud og udformer målrettede mails rettet mod forskerne.

Svindlerne kan oven i købet udvælge bestemte forskningsområder, som de især er interesserede i at spionere mod.

Automatiseringen fremgår af, at mailene var fuldstændig enslydende. Eneste forskel var navne og titler på artiklerne.

Den forfalskede afsender var i øvrigt også forskellig fra mail til mail. Der var angivet fuldt navn, universitet og institut på afsenderen – sikkert fundet på en forskerportal eller det tyske universitets websted.

Det danske universitet opdagede hurtigt problemet og fik ændret passwords for de forskere, der havde klikket på linket.

6.1.3. > HVEM TJEKKER LINKS?

Jeg finder affæren interessant, fordi den er et tegn på, hvordan phishing-svindel udvikler sig. Jeg frygter, at vi kommer til at se flere lignende svindelforsøg i fremtiden.

De fleste forsøg på phishing er meget primitive. En mail fra banken om, at din konto er spærret. Men da du ikke er kunde i den pågældende bank, bliver den hurtigt slettet.

Hvordan ville du reagere, hvis du modtog en lige så målrettet mail som den, der blev sendt til de danske forskere?

Som Computerworld-læser er du nok årvågen nok til at tjekke, hvor et link fører hen, før du klikker på det.

Men hvor mange af dine kolleger ville gøre det?

6.1.4. > INFORMATION KAN SKRÆLLES

Stadig mere information om os ligger frit tilgængeligt ude på nettet. Det gør det lettere at udføre den form for automatiseret phishing.

Forestil dig for eksempel et script, der skræller data fra LinkedIn- eller Facebook-profiler. Det sender målrettede mails til alle, der har meldt sig til en gruppe med et bestemt emne.

Hvordan vil medlemmerne af en gruppe om Porscher for eksempel reagere på en mail med link til billige reservedele målrettet til lige præcis deres model?

Eller hvad med en mail til medlemmerne af et politisk diskussionsforum med link til et lækket udkast? De skal bare lige logge ind først.

6.1.5. > VI MÅ UNDERVISE

Vi kan ikke undgå den type angreb. Men vi kan forberede vores brugere på dem, så de bliver bedre til at gennemskue dem.

Her er der brug for awareness-kampagner og undervisning. Det er et område, som jeg gjorde en indsats for i min tid som informationssikkerhedschef på Københavns Universitet. Og det vil jeg også slå et slag for i min nye rolle som chef for DKCERT.

Jeg glæder mig til at dele flere holdninger og informationer om informationssikkerhed med læserne via mine klummer her i Computerworld.

6.2. > DETTE ENKLE TRICK FJERNER NI UD AF TI SÅRBARHEDER

Med en enkel ændring kan du forhindre angribere i at udnytte ni ud af ti sårbarheder.

Du skal blot fjerne administratorprivilegierne fra dine Windows-brugeres konti. Teknisk set er det ikke kompliceret. Det er heller ikke nyt.

Sikkerhedseksperter har i mange år argumenteret for, at almindelige brugere bør være logget ind på en konto uden administratorprivilegier.

Når man er administrator, må man alt på computeren: Installere programmer, installere drivere, ændre firewall-opsætning, og hvad man ellers har lyst til.

Nogle sårbarheder giver angribere mulighed for at køre programmer med samme privilegier som den bruger, der er logget ind, når sårbarheden aktiveres.

Dermed kan angriberen fuldstændig det samme som brugeren: Installere programmer og ændre på væsentlige indstillinger.

Hvis man fjerner administratorprivilegierne, fjerner man ikke sårbarhederne. Men man begrænser den skade, de kan medføre.

6.2.1. > VIRKER PÅ 97 PROCENT

En analyse fra firmaet Avecto viste for nylig, hvor effektiv metoden er. Firmaet har analyseret de 240 sårbarheder, som Microsoft rettede i 2014.

Analysen viser, at 97 procent af de kritiske sårbarheder får mindsket deres skadevirkning, hvis man fjerner administratorprivilegierne.

For Internet Explorer var andelen helt oppe på 99,5 procent.

Tilsvarende analyser har tidligere peget i samme retning. I 2009 viste en analyse fra BeyondTrust, at ni ud af ti kritiske sårbarheder i Windows 7 blev uskadeliggjort med metoden.

Begrænser man mængden af administratorkonti, mindsker man også risikoen ved såkaldte pass-the-hash-angreb.

Det er angreb, hvor angriberen opsnapper den hashværdi, der autentificerer en bruger på et system.

Hvis brugeren har begrænsede privilegier, mindsker det risikoen. Angriberen kan måske overtage brugerens session, men han eller hun kan ikke volde alvorlig skade.

6.2.2. > EN KLAR ANBEFALING

Center for Cybersikkerhed udsendte for halvandet år siden anbefalingen "Cyberforsvar der virker".

Den anbefaler, at man begynder med at implementere fire sikringstiltag - og et af dem er netop at begrænse antallet af konti med domæne- eller lokaladministratorprivilegier.

Det skulle altså være ganske enkelt: Fjern administratorprivilegierne og slip for en masse sikkerhedsrisici.

Alligevel er jeg overbevist om, at rigtig mange danske pc-brugere i både den offentlige og den private sektor har fuld kontorl over deres computere - de er det, der i Windows-sammenhæng kaldes lokal administrator.

Det skulle ikke undre mig, om det er flertallet.

6.2.3. > KULTUREL BARRIERE

Hvorfor undlader vi at bruge et oplagt middel til at øge sikkerheden?

Jeg tror, en del af forklaringen er historisk og kulturel.

Da pc'erne kom frem, udgjorde de et brud med den centrale kontrol, edb-afdelingen havde udøvet.

Før pc'en måtte enhver bruger rette sig efter de regler, edb-folkene udstak.

Med pc'en fik brugeren kontrol over sin computer.

Han eller hun kunne installere et regnearksprogram og selv udføre de beregninger, som edb-afdelingen ellers brugte måneder på at tilrette de centrale systemer til.

Jeg kommer fra universitetsverdenen.

Der hersker en stolt tradition for, at hver forsker og underviser selv vælger sine værktøjer - og naturligvis har hånd- og halsret over dem.

Noget lignende findes utvivlsomt i mange professioner. Hvem tør fortælle en ingeniør, at han ikke må installere programmer på sin pc?

6.2.4. > TEKNOLOGI LETTER OPGAVEN

Heldigvis er teknologien på vores side.

Stadig flere programmer kan i dag installeres uden administratorprivilegier.

Og Microsoft har gjort det enklere at være standardbruger: Man slipper for de bunker af advarsler, som UAC (User Account Control) kom med, da det blev indført i Windows Vista.

Alligevel er det ikke alle organisationer, der kan løse problemet blot ved at flytte fluebenet fra administrator til standardbruger, når de opretter brugere.

Er der brug for mere avanceret styring af privilegierne, findes der en række værktøjer, man kan investere i.

De giver for eksempel mulighed for at indføre undtagelser, hvor teknologien kræver det - så en medarbejder kan køre et enkelt program med administratorprivilegier uden at være administrator.

6.2.5. > VI SAVNER EN KULTURÆNDRING

Men teknologiske løsninger er ikke nok.

De sikkerhedsansvarlige må lære deres brugere, hvorfor det giver bedre sikkerhed at fjerne administratorprivilegierne. Og de skal lytte til brugerne og afgøre, om der er legitime begrundelser for at indføre undtagelser.

Der er brug for en kulturændring.

Kan vi gennemføre den, kan vi højne informationssikkerheden væsentligt.

6.3. > SÅDAN UDVÆLGER DU DE DATA DER ER VÆRD AT BESKYTTE

Nogle af dine data er mere værd end andre.

Det ved du selvfølgelig godt. Men har du tænkt over, hvad det betyder for din investering i it-sikkerhed?

Mængden af data i verden vokser eksponentielt. Samtidig stiger antallet af angreb og forsøg på angreb også voldsomt.

Konsekvensen er, at vi sikkerhedsfolk simpelthen ikke har ressourcer til at beskytte alt.

Vi må erkende, at vi har data, som vi kan miste, uden at det får fatale konsekvenser.

Men det stiller krav til os: Vi er nødt til at afgøre, hvilke data der er livsvigtige for os - og hvilke der ikke er det.

6.3.1. > VI MÅ KLASSIFICERE

Jeg taler her om klassificering af data. Klassificering foregår ved, at man opdeler data i klasser ud fra deres forretningsmæssige værdi.

For eksempel kan man inddele data i klasserne fortroligt, internt og offentligt.

Dataklassificering indgår som en af de aktiviteter, en organisation skal gennemføre, for at den kan blive certificeret ud fra kravene i ISO 27001. Dermed er det en øvelse, som mange vil komme ud for, efterhånden som standarden bliver mere udbredt.

6.3.2. > KRAV SKAL AFVEJES

Under klassificeringen skal man både overveje konsekvenserne for tilgængelighed, integritet og fortrolighed.

For eksempel kan der være data, hvor fortrolighed ikke er afgørende. Det er data, som udenforstående ikke kan bruge til noget.

Men de samme data kan indgå i driften på en måde, så de absolut ikke kan undværes. Her vejer tilgængelighed altså tungere end fortrolighed.

Så klassificeringen hænger sammen med en risikovurdering.

Man må overveje, hvilke konsekvenser det får, hvis dataene kommer i de forkerte hænder. Eller hvis systemet bringes ud af drift.

6.3.3. > EN STOR OPGAVE

Udfordringen ved arbejdet er ikke så meget at tænke i klasser. Det har andre gjort før jer, og der er gode kilder at trække på.

Nogle kan bruge de fortrolighedsklasser, Forsvaret anvender, og som kendes fra statsministeriets sikkerhedscirkulære. For andre passer en simplere model, som den jeg nævnte tidligere, bedre.

Nej, den store udfordring ligger i udførelsen: I skal vurdere hver eneste stump data i jeres virksomhed eller organisation.

Både data og de systemer, der behandler data, skal beskyttes i henhold til klassifikationen.

Nogle data klassificeres ud fra den værdi, de har for jeres egen organisation.

Andre skal klassificeres som følsomme, fordi lovgivningen stiller krav til, hvordan I beskytter dem. Det er for eksempel data om kunder eller medarbejdere, der falder ind under persondataloven.

Næste udfordring kommer, når arbejdet er gjort. Så skal klassifikationerne holdes ved lige.

I skal løbende tjekke, at data stadig er klassificeret korrekt - og nye datatyper skal ind i systemet.

6.3.4. > VI ER BAGUD I VÅBENKAPLØBET

Det lyder måske mærkeligt, at vi som sikkerhedsfolk skal acceptere, at nogle data kan gå tabt. Men det er en nødvendig konsekvens af det våbenkapløb, vi deltager i.

Vi dataejere er konstant bagud i forhold til dem, der har ondt i sinde. Vi har ikke råd til at beskytte alt.

Derfor er det nødvendigt at prioritere.

Vi må afgøre, hvor guldet i vores virksomhed befinder sig. Og når vi har fundet det, skal vi beskytte det.

Klassificering af data er et af de første skridt på vejen mod en styret sikkerhedsindsats.

For at det kan virke, er det afgørende, at medarbejderne kender og forstår systemet. De skal vide, hvilke data I regner for særligt følsomme, så de kan behandle dem korrekt.

Det kan indførelsen af dataklassifikation i sig selv hjælpe med til: Når data ikke er klassificeret, regnes alle data for lige vigtige - eller uvigtige.

Men når I har sat en værdi på data, bliver det klart for medarbejderne, hvad der er værd at beskytte.

6.4. > SÅDAN VURDERER DU RISIKOEN FOR BRUD PÅ SIKKERHEDEN

Rigsrevisionen har undersøgt informationssikkerheden i it-systemer, der understøtter samfundsvigtige opgaver i seks institutioner.

Undersøgelsen fokuserer på, hvordan institutionerne styrer udvidede administratorrettigheder. Det kan være de rettigheder, en systemadministrator udstyres med, eller rettigheder for en systemkonto.

Konklusionen lyder, at institutionerne ikke har efterlevet en række anerkendte anbefalinger om god it-sikkerhedspraksis.

Endvidere skriver Rigsrevisionen: "Der er behov for ledelsesmæssig fokus og prioritering for at rette op på de konstaterede forhold."

Jeg kunne ikke være mere enig.

Effektiv informationssikkerhed kræver, at ledelsen går aktivt ind i arbejdet.

Det vigtigste redskab i den forbindelse er risikovurderingen.

Der findes ingen it-risici. Der findes kun forretningsrisici.

Enhver risiko tilknyttet et it-system har i sidste ende en forretningsmæssig konsekvens.

Derfor skal ledelsen på banen.

6.4.1. > KONSEKVENS GANGE SANDSYNLIGHED

Jeg definerer en risiko som konsekvensen af et sikkerhedsbrud set i forhold til sandsynligheden for, at det sker.

Et sikkerhedsbrud opstår på grund af en kombination af en sårbarhed og en trussel.

En sårbarhed kan for eksempel være mangelfuld kontrol med administratorrettigheder.

Truslen består i, at uvedkommende kan udnytte sårbarheden og få adgang med administratorprivilegier.

Konsekvensen af dette sikkerhedsbrud kan være, at hackere får fat i fortrolige data. En anden konsekvens kan være, at systemet bliver inficeret med skadelig software.

For at kunne risikovurdere sikkerhedsbruddet skal vi have et bud på sandsynligheden: Hvor sandsynligt er det, at truslen vil blive udmøntet i praksis?

Hvis konsekvensen er meget alvorlig, men sandsynligheden er forsvindende lille, bliver den samlede risikovurdering lav.

Sat på formel er risiko altså lig med konsekvens gange sandsynlighed.

6.4.2. > DIREKTØRENS VÆRKTØJ

Risikovurdering er det praktiske værktøj, ledelsen kan bruge i sikkerhedsarbejdet.

Direktøren kan ikke vurdere, om en sikkerhedsrettelse til virksomhedens CMS er vigtig.

Men hvis it-organisationen kan levere data om sårbarhed, trussel, konsekvens og sandsynlighed, kan ledelsen træffe en informeret beslutning om, hvad den skal gøre ved risikoen.

I teorien lyder det måske enkelt. Men mange års erfaring med risikovurdering har lært mig, at udfordringerne dukker op, så snart man skal gøre det i praksis.

For eksempel kan det være vanskeligt at sætte tal på sandsynlighed.

Jeg anbefaler, at man opdeler sandsynlighed og konsekvens i fire niveauer.

6.4.3. > DE FIRE T'ER

Når en risiko er vurderet, er der fire ting, vi kan vælge at gøre ved den. På engelsk taler man om de fire T'er: Treat, transfer, tolerate og terminate.

- Treat: Vi behandler et eller flere af elementerne i risikoen. Vi kan fx fjerne sårbarheden ved at opdatere software.
- Transfer: Vi overfører risikoen til en anden. Det gør vi, når vi tegner en forsikring: Går noget galt, betaler forsikringsselskabet.
- Tolerate: Vi beslutter at leve med risikoen. Det vil typisk være, hvis risikoen er lille, eller hvis det er meget dyrt at gøre noget ved den.
- Terminate: Vi holder op med at bruge de systemer, som risikoen er forbundet med, så den forsvinder.

Som det fremgår, er der meget at holde styr på. Mit råd er derfor, at man anvender et rammeværk til opgaven.

Der findes flere rammeværk til risikovurdering. Går man ISO-vejen, kan man vælge ISO 27005.

Et godt alternativ er Octave Allegro fra CERT ved Carnegie Mellon University.

Octave Allegro er overskueligt og nemt at komme i gang med.

Vælg et rammeværktøj, der passer til jeres opgave, og som I føler jer fortrolige med.

6.4.4. > ET UDBREDT PROBLEM

Rigsrevisionen skriver i rapporten, at resultaterne kan være gældende for en større kreds af statslige institutioner end de seks, der er blevet undersøgt.

Jeg kunne tilføje: Og for mange andre offentlige institutioner og private virksomheder.

Problemet med at holde styr på privilegerede brugerkonti er velkendt.

Og jeg er sikker på, at det samme gælder problemet med at få ledelsens bevågenhed, når det gælder informationssikkerhed.

Her kan risikovurderingen blive en løftestang: Den lader dig som it-ansvarlig vise den øvrige ledelse, at det her handler om at håndtere forretningsmæssige risici for tab af penge, anseelse, kunder eller andet.

7. Fremtidens trusler og trends

Industrispionage, afpresning og salg af stjålne data vil fortsætte. Ledelserne bliver i højere grad nødt til at tage ansvaret for informationssikkerheden.

7.1. > TRUSLER MOD INFORMATIONSSIKKERHEDEN I 2016

To teknologier er med til at gøre livet lettere for it-kriminelle. Begge handler om anonymisering. Tor-netværket gør det muligt at skjule, hvor man bevæger sig rundt på nettet. Det har ført til etableringen af det såkaldte dark web: En underverden af websteder, hvor it-kriminelle kan udveksle stjålne data, købe angrebsprogrammer eller leje angrebskapacitet. Alt foregår i fuld anonymitet.

Den anden teknologi er den virtuelle valuta Bitcoin. Den gør det muligt at overføre penge til andre, uden at udenforstående kan se, hvem der betaler hvem. Teknisk set er Bitcoin ikke fuldstændig anonym: Tjenesten anvender pseudonymer. Men i praksis bruger it-kriminelle den på grund af den høje grad af beskyttelse af navnene på de implicerede. Således afkræver bagmændene bag ransomware i dag typisk betaling i Bitcoin.

7.1.1. > AFPRESNING FORTSÆTTER

Gennem de sidste 20 år har it-kriminaliteten bevæget sig fra angreb, der skulle teste tekniske barrierer, til angreb med det formål at tjene penge. Den tendens vil fortsætte. Derfor vil vi også i 2016 se mange forsøg på afpresning, både med ransomware og med trusler om DDoS-angreb.

7.1.2. > INDUSTRISPIONAGE

Den seneste trusselsvurdering fra Center for Cybersikkerhed vurderer risikoen for spionage mod myndigheder og virksomheder til at være høj. Det er også DKCERTs opfattelse. Danske forskningsinstitutioner skal være forberedt på angreb, der går efter deres seneste forskningsresultater og planer.

Et af midlerne vil fortsat være målrettede e-mails, såkaldt spear phishing. Det er angreb, hvor angriberen skaffer sig information om offerets organisation. På den måde kan mailen se ud til at komme fra en kollega, som modtageren kender og har tillid til.

Vi venter også flere spear phishing-angreb, hvor målet direkte er penge. Det kan være faktureringssvindel, hvor de kriminelle sender faktura på opgaver, der aldrig er udført. Eller de kan narre bogholderiet til at ændre den konto, som en underleverandør modtager betaling på.

7.1.3. > HACKTIVISME

Vi vurderer truslen fra hacktivisme (cyber-aktivisme) til at være begrænset. Det fremgår også af, at antallet af defacements de senere år har været langt lavere, end da Muhammedkrisen rasede i begyndelsen af 2006. Dengang blev antallet af defacements firedoblet på en måned.

Truslen afhænger dog af, hvor stor opmærksomhed Danmark pådrager sig. I 2015 var der flere tilfælde af DDoS-angreb mod Island som protest mod landets hvalfangst. Noget tilsvarende kunne ske, hvis en aktivistgruppe kastede sig over Færøernes hvalfangst.

Også den negative internationale opmærksomhed om Danmarks flygtningepolitik kunne føre til hacktivist-angreb. Foreløbig har der dog ikke været tegn på det.

7.2. > SIKKERHEDSTRENDS I 2016

DKCERT venter, at informationssikkerheden bevæger sig endnu længere ind på direktionsgangene og i rektoraterne. Sikkerhed er et ledelsesansvar, men det er et ansvar, mange ledere forsøger at slippe for. Det bliver sværere nu.

Staten har allerede indført et krav om, at statslige organisationer skal efterleve kravene i den internationale standard for sikkerhedsstyringssystemer, ISO 27001. Og i 2016 vedtager EU persondataforordningen, der giver fælles regler for beskyttelsen af persondata på tværs af EU-landene.

7.2.1. > BESKYTTELSE MOD AFPRESNING

De seneste udgaver af ransomware udnytter stærk kryptering. Det gør det praktisk umuligt at bryde krypteringen og få data tilbage. Det bedste forsvar er derfor en solid strategi for sikkerhedskopiering.

Beskyttelse mod DDoS sker mest effektivt på netværksniveau. Når angrebet først når frem til ens server, kan det være for sent at gøre noget. Derfor er det en god ide at høre, hvad netværksudbyderen kan tilbyde. Måske kan udbyderen filtrere angrebstrafik fra eller få den stoppet hos det netværk, den stammer fra.

DKCERT mener:

Som konsekvens af kravet om ISO 27001 i staten og EU's persondataforordning venter vi, at informationssikkerhed for alvor bliver et ledelsesspørgsmål. Det stiller nye krav til it-folkene: De skal blive endnu bedre til at tale forretningens sprog, når de kommunikerer med ledelsen.

Her bliver risikovurdering et nyttigt redskab. Den typiske topleder kan ikke forholde sig til, at en web-applikation har en SQL-indsætningssårbarhed. Men lederen kan godt forstå, hvis der er en kvantificerbar risiko for, at uvedkommende får adgang til kundedatabasen.

En stor del af reglerne i persondataforordningen findes allerede i den eksisterende persondatalovgivning. Men nu får myndighederne for første gang mulighed for at straffe overtrædelser, så det kan mærkes. Derfor kan persondataforordningen betyde, at persondatalovgivningen for første gang rent faktisk bliver overholdt.

8. Anbefalinger

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

Som i de tidligere trendrapporter giver vi her vores bud på anbefalinger og gode råd om informationssikkerhed. Da DKCERT nu fokuserer på rollen som CERT for DeIC og forskningsnettet, har vi i år valgt ikke at komme med anbefalinger til borgere og virksomheder. I stedet er vores anbefalinger målrettet vores primære målgrupper: It-ansvarlige og ledelse på uddannelses- og forskningsinstitutioner.

Mange af vores anbefalinger tager udgangspunkt i den internationale standard for styring af informationssikkerhed, ISO 27001. Helt overordnet anbefaler vi alle, der er involveret i informationssikkerhed, at sætte sig ind i den standard. Den giver en metodisk, struktureret og afprøvet tilgang til opgaven.

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 27001.

1. Forlang ledelsens aktive involvering i informationssikkerhedsarbejdet.
2. Ajourfør og vedligehold informationssikkerhedspolitikken.
3. Hold brugernes enheder opdateret. Det gælder også, når de anvender deres egne enheder til arbejds- eller studieformål (BYOD, Bring Your Own Device).
4. Effektiviser patch management – gerne ud fra principperne i ITIL.
5. Hav øget fokus på sikkerheden i institutionens webapplikationer og backend-systemer.
6. Begræns brugernes privilegier, bl.a. ved at fjerne lokal administrator-rettigheden i Windows.
7. Indfør whitelisting af de applikationer, brugerne må køre.
8. Klassificer data for at identificere kritiske data.
9. Begræns adgangen til kritiske data og beskyt dem eventuelt med kryptering.
10. Indfør tiltag mod misbrug via gæstenetværk gennem logning og overvågning.
11. Hav fokus på sikkerheden ved udvikling af applikationer og tjenester samt tilretninger af eksisterende systemer.
12. Anvend single sign-on suppleret med to-faktor-autentifikation.
13. Tænk sikkerhed ind i relationen til leverandører og samarbejdspartnere.

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 persondataloven, 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. Hold de ansatte, studerende og gæster informeret om informationssikkerhedspolitikken og aktuelle problemer.
5. Etabler et beredskab og udarbejd en beredskabsplan for kritiske hændelser.
6. Prioriter og synliggør risikostyring.
7. Foretag løbende risikovurderinger af forretningskritiske systemer.
8. Afsæt ressourcer til uddannelse og kompetenceudvikling i informationssikkerhed.
9. Arbejd sammen med andre institutioner om informationssikkerhed.
10. Afsæt tid, penge og personale til håndtering af informationssikkerhed.
11. Kortlæg flowet af persondata i organisationen med henblik på at leve op til EU's persondataforordning.

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 Innovation. DKCERT er en tjeneste fra DeIC. Se også www.deic.dk

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

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 e-Science.

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 hacker 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.

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.

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 login-løsning 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.

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.

Stuxnet
Stuxnet er en orm, der spreder sig via USB-nøgler ved at udnytte en sårbarhed i Windows' behandling af genveje. Herefter angriber den industrielle Siemens WinCC SCADA-systemer. Den menes at være udviklet til at sabotere Irans atomprogram.

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

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

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

Trojansk hest
Et program der har andre funktioner 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 > **Zone-H:** Archive, http://zone-h.org/archive

2 > **DKCERT/Digitaliseringsstyrelsen:** Borgernes informationssikkerhed 2015, https://www.cert.dk/borgersikkerhed2015/Borgernes_informationssikkerhed_2015.pdf

3 > **National Vulnerability Database:** Statistics, https://web.nvd.nist.gov/view/vuln/statistics

4 > **DKCERT:** Kode til Linux-ransomware kan knækkes, https://www.cert.dk/nyheder/nyheder.shtml?15-11-11-10-07-14

5 > **DataLossDB:** Statistics, http://datalossdb.org/statistics

6 > **Identity Theft Resource Center:** Data Breach Reports 2015, http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

7 > **Wikipedia:** Hacking Team, https://en.wikipedia.org/wiki/Hacking_Team#2015_data_breach

8 > **Kaspersky:** Mobile malware evolution 2015, https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/

9 > **DKCERT:** Massevis af iOS-apps inficeret via bagdør i udviklingsværktøj: Dette bør Apple gøre nu, https://www.cert.dk/artikler/artikler/CW20151002.shtml

10 > **DKCERT:** Chrysler lukker sikkerhedshul i biler, https://www.cert.dk/nyheder/nyheder.shtml?15-07-22-09-34-09

11 > **The Register:** Connected kettles boil over, spill Wi-Fi passwords over London, http://www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots/, https://www.pentestpartners.com/blog/finding-wireless-kettles-with-social-networks/

T R E N D R A P P O R T

16

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DeiC DANISH e-INFRASTRUCTURE COOPERATION