DKCERT

DeiC DANISH e-INFRASTRUCTURE COOPERATION

TRENDRAPPORT

Status på informationssikkerheden i året der gik

15

DKCERT TRENDRAPPORT 2015

Redaktion: Shehzad Ahmad og Torben B. Sørensen

Tak til vore øvrige bidragydere: Tonny Bjørn, DKCERT, Niels Christian Ellegaard og Michael Hopp, Plesner, Anne Ermose og Ole Kjeldsen, Microsoft Danmark, Rasmus Theede, KMD, Martin Bech, DeIC, og Henrik Jensen, Roskilde Universitet

Design: Kiberg & Gormsen

Tryk: GSB Grafisk

DeIC-journalnummer: DeIC JS 2015-2

Om DKCERT

DKCERT bygger på en vision om at skabe værdi for uddannelsessektoren 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 uddannelsessektoren 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.

Denne viden benytter DKCERT til at udvikle services, der skaber merværdi for institutionerne på forskningsnettet og sætter dem i stand til bedre at sikre deres it-systemer.

DKCERT, et dansk Computer Security Incident Response Team, 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 Ministeriet for Forskning, Innovation og Videregående Uddannelser 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 Terena/Géant, samt akkrediteret TI-medlem af Trusted Introducer.

Indholdsfortegnelse

1. Velkomst

Velkommen til tal, grafer og tekster om informationssikkerhed – et område der år for år bliver mere vigtigt at tage alvorligt.

Velkommen til min sidste trendrapport som chef for DKCERT. Det har været spændende at følge udviklingen i informationssikkerheden i mine syv år på posten. Jeg har undervejs måttet erkende, at det ofte er svært at vinde gehør, når man taler for øget sikkerhed.

Årsagen er enkel: For langt de fleste mennesker er informationssikkerhed ikke noget, de bruger det meste af deres tid og opmærksomhed på. Medarbejderne i en virksomhed har travlt med at udføre deres job. De studerende på et universitet koncentrerer sig om studierne. Så er det vanskeligt at overbevise dem om, at de også skal tænke på informationssikkerheden.

Men mine år hos DKCERT har også vist mig, at det er nødvendigt at tage sikkerhedsopgaven alvorligt. For angrebene vokser både i antal og i styrke. Angriberne er blevet mere snedige og mere målrettede.

Ledelserne rundt om i Danmark må erkende, at informationssikkerhed i dag fylder mere, end den gjorde for fem år siden. Et brud på sikkerheden kan få alvorlige konsekvenser – i sidste ende kan det blive et spørgsmål om organisationens liv og død.

Derfor skal de afsætte de nødvendige ressourcer til at håndtere sikkerheden i dagligdagen: Tid, penge og personale.

Og så er det afgørende, at medarbejderne med sikkerhedsopgaver får den viden, de har brug for. Uden viden kommer vi aldrig over bjerget. Og vi sikkerhedsansvarlige må forstå, at sikkerhedsarbejdet er en proces, der aldrig slutter. Derfor skal vi også have den viden, der gør os i stand til at lede vores medarbejdere på vej mod en mere sikker hverdag.

Jeg vil gerne sige tak til de mange spændende mennesker, jeg har mødt i mine år hos DKCERT. Jeg ønsker min ledelse, min efterfølger og i særlig grad mine medarbejdere held og lykke – sikkerhedsområdet bliver kun vigtigere med tiden, så de får nok at se til.

God fornøjelse med læsningen!

Shehzad Ahmad
Chef, DKCERT

2. Resumé

I 2014 behandlede DKCERT over tre gange flere sikkerhedshændelser end året før. Året var præget af store hackersager i både Danmark og udlandet.

DKCERT håndterede i 2014 i alt 65.267 sikkerhedshændelser, hvoraf langt de fleste havde tilknytning til forskningsnettet. Det er en stigning på 250 procent. Væksten skyldes flere faktorer: Vi har modtaget flere henvendelser, flere af vores samarbejdspartnere indrapporterer nu hændelser automatisk, og vi har effektiviseret og automatiseret vores sagsbehandling yderligere.

Halvdelen af hændelserne var portscanninger, der som regel regnes for mindre alvorlige. 12 procent af sikkerhedshændelserne var brud på ophavsretten, primært piratkopiering af film. Andre 12 procent handlede om computere, der uden deres ejers vidende blev fjernstyret og misbrugt af it-kriminelle i såkaldte botnet.

På verdensplan voksede mængden af registrerede sikkerhedshuller i 2014 med 53 procent til 7.937 sårbarheder. Alvorlige sårbarheder udgjorde en fjerdedel. På grund af redesign og opgradering af DKCERTs scanningstjeneste har DKCERT ikke foretaget scanninger efter sårbare systemer i 2014.

2.1 > TENDENSER FRA ÅRET DER GIK

Filmselskabet Sony Pictures Entertainment blev hacket. Myndighederne i USA mente, at Nordkorea stod bag, fordi landets ledelse var utilfredse med filmen The Interview. Affæren demonstrerede, hvor vanskeligt det er at bevise, hvem der står bag angreb på internettet.

2014 var præget af to store sårbarheder: Heartbleed og Shellshock. Heartbleed gav angribere mulighed for at få fat i fortrolig information på sårbare computere. Shellshock var en sårbarhed i en kommandofortolker, som angribere kunne misbruge til at afvikle programmer.

I Danmark faldt der dom i CSC-hackersagen, hvor hackere havde fået adgang til cpr-numre og kørekortinformationer. Retten fandt svenske Gottfrid Svartholm Varg skyldig, selvom han forsvarede sig med, at hans computer var blevet fjernstyret under angrebet.

En gammelkendt type trussel dukkede op igen i 2014: Makrovirussen, der spredes med inficerede Office-dokumenter. Bagmændene havde fundet en metode til at narre ofrene til at slå den sikkerhedsfunktion fra, der skulle beskytte dem mod farlige makroer.

2.2 > TRUSLER OG TRENDS I 2015

Truslen fra efterretningstjenester og nationalstater var i fokus i 2014 og kommer det også i 2015. Det stiller nye krav til organisationers og virksomheders risikovurdering og analyse af, hvilke sikkerhedsværktøjer der er effektive.

Afpresning ved hjælp af software, der spærrer for brugerens adgang til data og programmer, bliver mere udbredt. Og det bliver sværere at gendanne data uden at betale løsesum.

I staten kommer den nationale strategi for cyber- og informationssikkerhed til at spille en stor rolle i 2015 i kraft af 27 konkrete initiativer. Samtidig bør organisationer og virksomheder begynde at forberede sig på EU's kommende persondataforordning – og at Windows 7 går på pension om fem år.

2.3 > GODE RÅD OM LEVERANDØRSIKKERHED

I kapitel 6: Det eksterne perspektiv giver eksperter uden for DKCERT råd om, hvordan man håndterer sikkerheden i forbindelse med underleverandører.

I juni kom en arbejdsgruppe under EU med et udspil til, hvordan man kan standardisere SLA'er (service level agreement) for cloud-tjenester. Det har gode takter og kan ende med at indgå i en egentlig international standard, skriver to advokater fra advokatfirmaet Plesner.

Microsoft kommer med forslag til de spørgsmål, kunder bør stille til sikkerheden, før de vælger cloud-leverandør.

Interne afdelinger kan også fungere som underleverandører. Her kan man fastlægge krav til sikkerheden med en såkaldt Operational Level Agreement (OLA). Det beskriver KMD's koncernsikkerhedschef.

Cloud gør brugerne kræsne: De er blevet vant til lækre brugergrænseflader og smarte funktioner. Hvis it-funktionen vil tilbyde dem mere sikre alternativer, skal de være konkurrencedygtige, skriver DeIC's divisionsdirektør.

Endelig gennemgår en sikkerhedskonsulent fra RUC, hvordan universitetet forbereder sig på den persondataforordning, som ventes endeligt vedtaget i slutningen af 2015.

3. Indledning

Enhver organisations informationssikkerhed afhænger af dens underleverandørers sikkerhedsniveau.

3.1 > INGEN COMPUTER ER EN Ø

"Intet menneske er en ø," skrev digteren John Donne i 1600-tallet. På samme måde er heller ingen it-organisation en ø. Alle vores systemer er forbundet med hinanden – og med systemer ude hos samarbejdspartnere.

Det giver store fordele, når det gælder kommunikation og fleksibilitet. Men det skaber også en sikkerhedsmæssig afhængighed: Organisationens egne it-systemer kan være sikret optimalt, men hvis underleverandørens system er hullet som en si, kan angribere udnytte det til at få adgang til organisationens data.

2014 bragte flere eksempler på, hvordan underleverandørers informationssikkerhed har indflydelse på et systems samlede sikkerhed. I den store sag om hackerangrebet på CSC fik hackerne adgang til fire millioner danskeres kørekortnumre. De lå i registre hos politiet, som leverandøren CSC stod for driften af. En uafhængig rapport viste siden, at CSC var nødt til at gennemføre otte forskellige tiltag for at rette op på "en meget betydelig svaghed" i virksomhedens systemer.[1]

I Se og Hør-sagen var det øjensynlig en ansat hos IBM, der misbrugte sin position til at få adgang til data om kendtes betalingskorttransaktioner. Som underleverandør til Nets stod IBM for driften af betalingskortsystemet.[2]

Også i udlandet var underleverandørers problemer med sikkerheden i fokus. Et hackerangreb på den amerikanske detailhandelskæde Target gav gerningsmændene adgang til kreditkortdata om over 110 millioner kunder.

Ifølge sikkerhedsreporter Brian Krebs kom hackerne ind i Targets it-systemer via en underleverandør, der leverede kølesystemer til butikkerne. Øjensynlig har en ansat hos underleverandøren klikket på et link i en mail, der førte til, at det skadelige program Citadel blev installeret på medarbejderens pc. Det gav bagmændene adgang til først kølesystemfirmaets egne it-systemer, siden til Target og måske også andre kunder.[3]

3.1.1 > BEGRÆNS ADGANGEN

Eksemplerne viser, at det kan få alvorlige konsekvenser, når sikkerheden halter hos en leverandør. Organisationer kan sætte ind på to områder for at mindske risikoen: Dels kan de stille skrappere krav til deres leverandører, dels kan de begrænse leverandørernes adgang.

Når en organisation indgår kontrakt med en leverandør, er fokus gerne på det, som leverandøren skal levere. Men man kan med fordel også skrive krav til it-sikkerhed ind i kontrakten – eventuelt i form af en tilhørende SLA (service level agreement).

Organisationen kan også selv gøre noget for at mindske risikoen: Den kan sørge for, at leverandører kun har adgang til de data og systemer, de har brug for. For eksempel er der næppe nogen forretningsmæssig grund til at give en leverandør af kølesystemer adgang til alle kunders betalingskortdata.

Forholdet til leverandører er direkte fremhævet i den nationale strategi for cyber- og informationssikkerhed som et af de seks indsatsområder. I strategien, der blev lanceret i december 2014, står der:

"En central del af arbejdet med cyber- og informationssikkerhed er derfor, at myndighederne stiller klare sikkerhedsmæssige krav til leverandørerne og løbende følger op på, at de overholdes. De statslige myndigheder skal arbejde mere systematisk med løbende at vurdere sikkerhedsniveauet i de løsninger, som drives af eksterne leverandører."

Læs mere om forholdet mellem kunde og leverandør, når det gælder it-sikkerhed, i kapitel 6: Det eksterne perspektiv.

[1] DR: PET-rapport afslører it-svagheder hos CSC, http://www.dr.dk/Nyheder/Indland/2014/10/17/1017124227.htm
[2] Wikipedia: Se og Hør-sagen, https://da.wikipedia.org/wiki/Se_og_H%C3%B8r-sagen
[3] Brian Krebs: Email Attack on Vendor Set Up Breach at Target, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

4. 2014 - året i tal

DKCERT behandlede mere end tre gange så mange sikkerhedshændelser i 2014 som året før. Portscanninger, piratkopiering og botnet var de hyppigste typer af hændelser.

4.1 > ÅRETS SIKKERHEDSHÆNDELSER

DKCERT håndterede i 2014 i alt 65.267 sikkerhedshændelser. Langt hovedparten af dem fandt sted på forskningsnettet (se Figur 1). Det er en konsekvens af, at DKCERT har skiftet fokus fra at behandle sikkerhedshændelser for alle, der henvendte sig, til kun at håndtere hændelser med relation til forskningsnettet.

Mængden af hændelser i 2014 udgør en stigning på 250 procent i forhold til året før. Det skyldes primært, at stadig flere hændelser indrapporteres automatisk fra it-systemer hos vores samarbejdspartnere. Det har medført en stigning i antallet af henvendelser. Da vi også har automatiseret en stor del af sagsbehandlingen, kan vi modtage og behandle langt flere hændelser end tidligere (se Figur 2).

4.2 > FORDELING PÅ TYPER AF HÆNDELSER

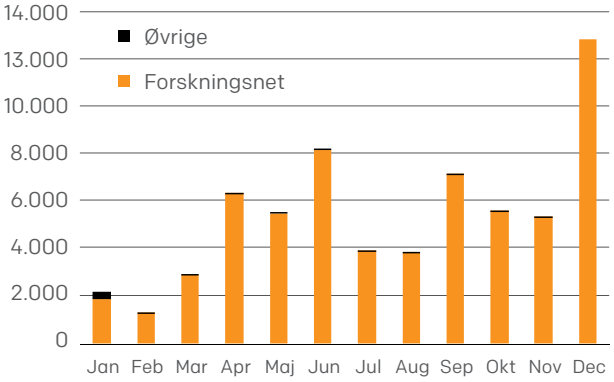
Godt halvdelen af sikkerhedshændelserne i 2014 var forskellige former for portscanninger. Det vil sige, at en hacker eller et program undersøger, om en computer svarer på henvendelser over nettet.

Brud på ophavsretten tegnede sig for 12 procent af hændelserne. En tilsvarende andel udgjorde tilfælde, hvor pc'er var involveret i botnet, så it-kriminelle kunne fjernstyre dem.

Fordelingen mellem de forskellige typer af hændelser fremgår af Figur 3 på side 10.

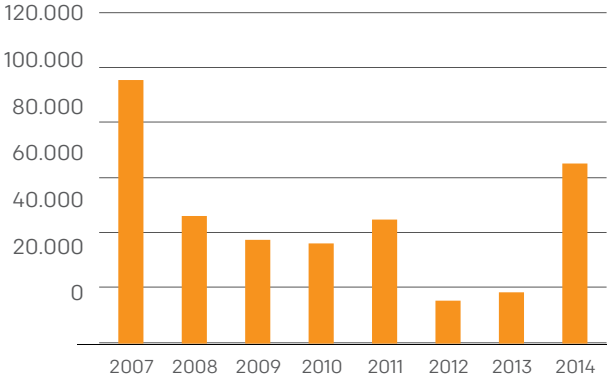
FIGUR 1

Sikkerhedshændelser håndteret af DKCERT i 2014



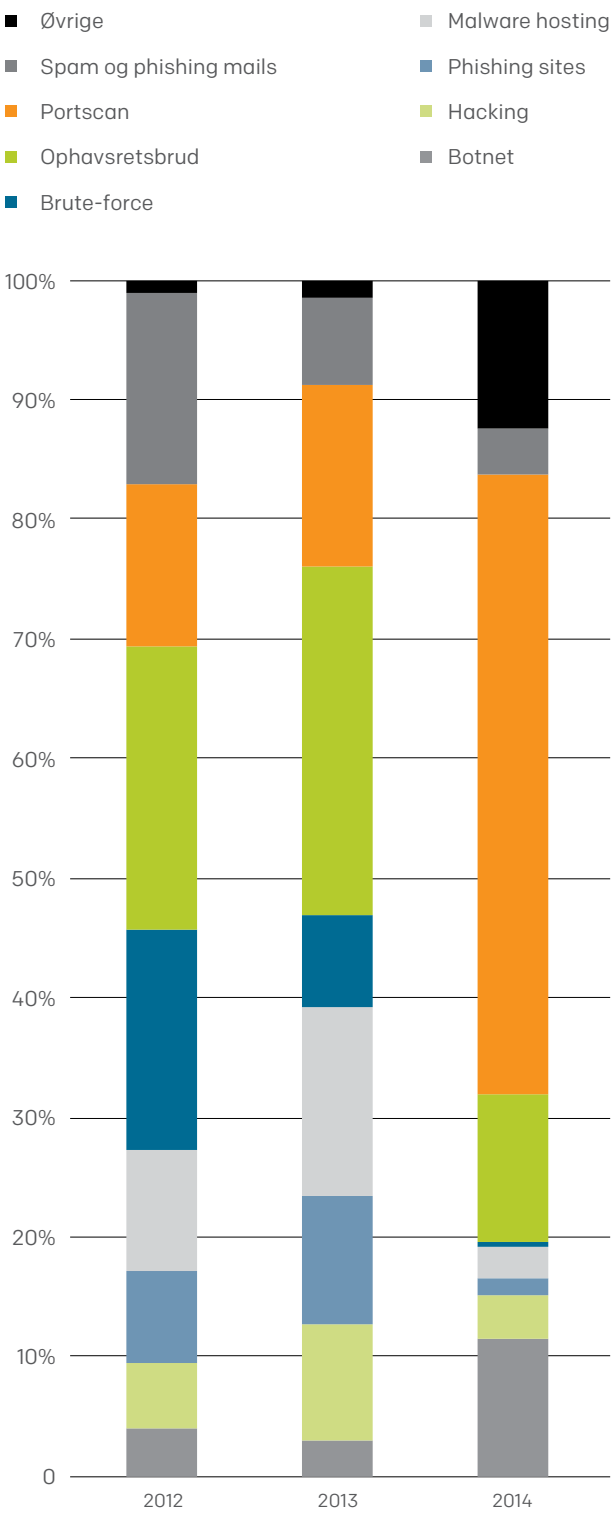
FIGUR 2

Sikkerhedshændelser håndteret af DKCERT 2007-2014



FIGUR 3

Fordeling mellem typer af sikkerhedshændelser 2012-2014



4.3 > PORTSCANNINGER

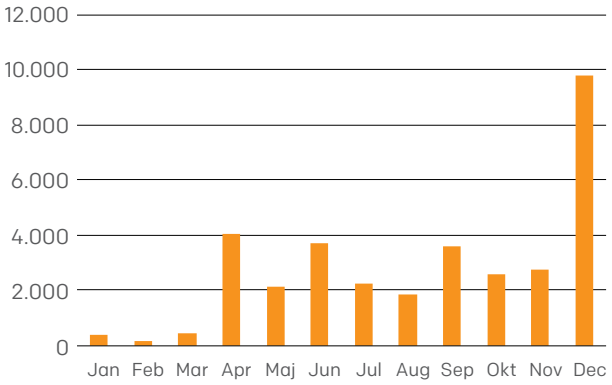
Mængden af portscanninger var jævnt fordelt over året, men steg voldsomt i december. Det skyldes, at en af vores eksterne kilder blev koblet direkte på vores sagssystem i den måned – der er altså ikke tale om en reel stigning i mængden af hændelser, men kun i vores registrering af dem.

Man kan diskutere, om en portscanning overhovedet udgør en sikkerhedshændelse. I mange tilfælde er der tale om helt legitim aktivitet. Det kan for eksempel være, hvis en bruger undersøger, om der ligger et websted på et bestemt domæne – så bliver der foretaget et opkald til TCP-port 80 på domænet. Kører der en webserver, svarer den, ellers fejler henvendelsen – og den registreres måske som en portscanning.

Når vi i DKCERT har valgt fortsat at registrere portscanninger som sikkerhedshændelser, skyldes det, at en portscanning kan være første skridt i et forsøg på at finde frem til sårbare computere, der kan angribes. Den indgår altså i rekognosceringsfasen af et angreb. Som hovedregel bør en portscanning ikke give grund til bekymring, medmindre den ser ud til at være del af et større mønster.

FIGUR 4

Sikkerhedshændelser med portscanninger



4.4 > BRUD PÅ OPHAVSRETTEN

12 procent af sikkerhedshændelserne handlede om brud på ophavsretten. Disse sager begynder som regel med en mail fra repræsentanten for et filmselskab. De har registreret, at en dansk IP-adresse har hentet eller distribueret piratkopier af selskabets film eller tv-serier. Det sker typisk ved hjælp af torrents (en metode til distribution af filer).

Anmeldelserne angiver ofte størrelsen på filen med piratkopien. Lægger man alle tallene sammen, blev der i 2014 klaget over filer på i alt 14,84 terabytes.

4.5 > BOTNET-INFEKTIONER

12 procent af hændelserne handlede om computere, der indgår i botnet (Figur 6). Et botnet består af computere, der er inficeret med skadelige programmer. De skadelige programmer kommunikerer med andre computere, der sender kommandoer til dem. På den måde kan botnet-bagmanden fjernstyre tusindvis af computere og sætte dem til at udføre et DDoS-angreb (Distributed Denial of Service), udsende spam eller lignende.

Mængden af botnet-hændelser er firedoblet i forhold til 2013.

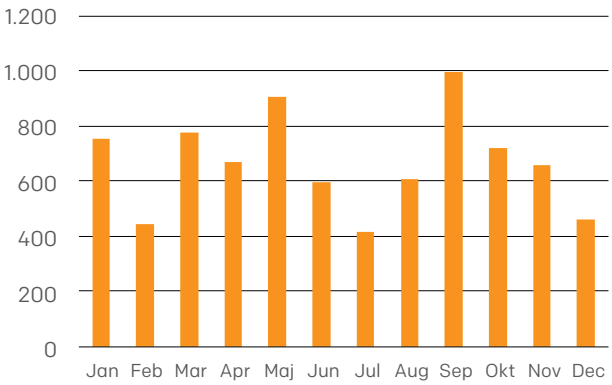
4.6 > PHISHING-MAILS OG SPAM

Hændelser med e-mails indeholdende spam eller forsøg på phishing udgjorde 3,7 procent af sikkerhedshændelserne. Spam er uønskede reklamer. Dem behandler DKCERT ikke klager over, men vi håndterer sager, hvor computere på forskningsnettet er involveret i at sende spam. Det skyldes som regel, at computeren er blevet indrulleret i et botnet.

Phishing er svindel, hvor afsenderen af mailen prøver at narre fortrolige oplysninger fra offeret. Som regel sker det ved at lokke offeret hen på en forfalsket webside, der giver sig ud for at tilhøre et websted, offeret har tillid til. Det kan for eksempel være med en mail, der oplyser, at brugeren skal bekræfte sine kontooplysninger ved at følge et link og udfylde en formular.

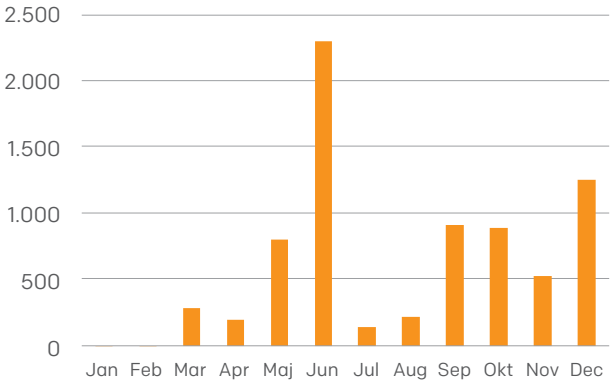
FIGUR 5

Hændelser om brud på ophavsretten (piratkopier)



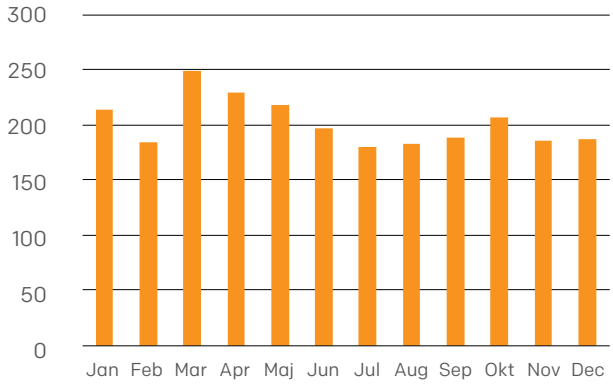
FIGUR 6

Botnet-inficerede danske computere



FIGUR 7

Hændelser med spam og phishing-mails



4.7 > SCANNINGER EFTER ANGREBSFORSTÆRKERE

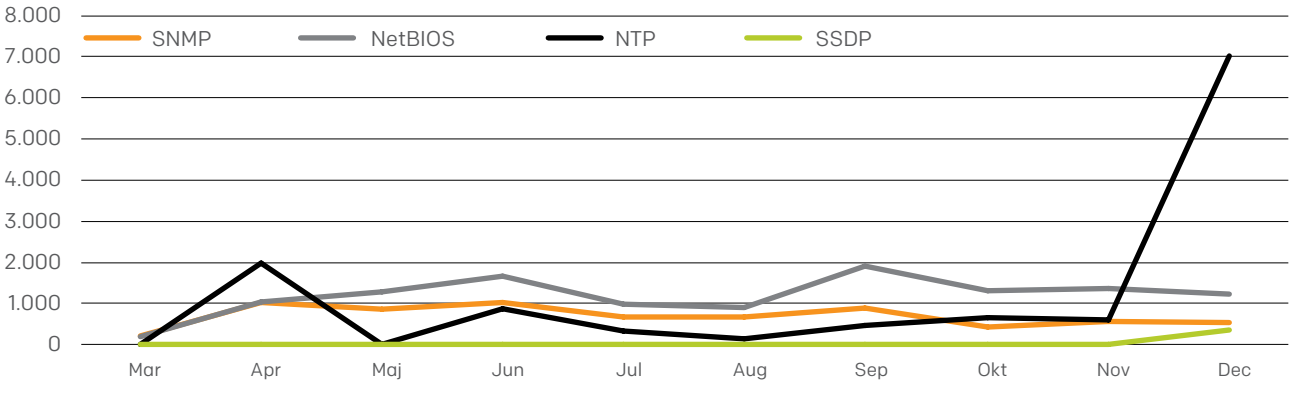
I år har vi set en del scanninger til brug i såkaldte reflection-angreb. De er også kendt som angreb med forstærkning. Det er DDoS-angreb (Distributed Denial of Service), hvor angriberen udnytter åbne tjenester på internettet som ufrivillige medhjælpere, der forstærker angrebet. Det sker ved, at angriberen forfalsker afsenderadressen i en pakke med en forespørgsel, der for eksempel bliver sendt til en tidsserver via protokollen NTP (Network Time Protocol).

Serveren svarer med en mængde data, der fylder mere end selve forespørgslen. Her ligger forstærkningsdelen af angrebet. Det omfattende svar fra serveren lander ikke hos angriberen, men hos offeret, hvis IP-adresse angriberen har angivet som afsender af forespørgslen. På den måde kan offerets computer blive overmandet af svar fra tusindvis af NTP-servere rundt om på nettet, som angriberen misbruger.

Tallene viser, at angriberne løbende leder efter servere, der er åbne for forespørgsler fra internettet på en række af disse tjenester. De anvender alle protokollen UDP (User Datagram Protocol), der i modsætning til TCP (Transmission Control Protocol) ikke giver sikkerhed for, at man kommunikerer med den afsender-adresse, der er angivet i pakken. Det gælder for eksempel SNMP (Simple Network Management Protocol), NetBIOS, NTP og SSDP (Simple Service Discovery Protocol). I december så vi en eksplosiv stigning i scanninger efter NTP-servere (se Figur 8).

FIGUR 8

Scanninger efter UDP-baserede tjenester, der kan misbruges til forstærkningsangreb



4.8 > MALWARE-UDVIKLINGEN

2,7 procent af sikkerhedshændelserne handlede om skadelig software, såkaldt malware. For at give et mere detaljeret billede af området har vi bedt sikkerhedsfirmaet F-Secure analysere deres data om infektioner i Danmark. Tallene dækker altså kun brugere af F-Secures produkter.

De viser, at otte ud af ti infektioner med malware i Danmark skyldes diverse varianter af trojanske heste (se Figur 9). Det kan være programmer, der angiver at være en videoafspiller, men som i virkeligheden er malware.

Exploits udgjorde 13 procent. Et exploit er et angrebsprogram, der udnytter en kendt sårbarhed i et program til at kompromittere sikkerheden.

Traditionelle virus udgjorde 3,7 procent. Ikke meget – men en tredobling i forhold til 2013. Så den velkendte virus, der spreder sig ved at inficere programfiler, eksisterer fortsat og er i fremgang. En overgang så det ud til, at den helt ville forsvinde til fordel for trojanske heste og orme.

Ser man på en topti over de mest udbredte familier af malware i Danmark, blev førstepladsen indtaget af et exploit: Majava, der udnytter kendte sårbarheder i ældre versioner af Java (se Figur 10). På andenpladsen var et såkaldt exploit kit ved navn Angler. Et exploit kit kører på en webserver, hvor det afprøver en stribe kendte sårbarheder på de pc'er, der besøger serveren. Har pc'en blot en af sårbarhederne, bliver den inficeret.

Fra 2013 til 2014 har de trojanske heste øget deres andel af infektionerne. Det er sket på bekostning af exploits, der udgjorde 32 procent i 2013, men kun 13,4 procent i 2014 (se Figur 11).

4.9 > FÆRRE DEFACEMENTS

I 2014 blev 3.345 websteder under dk-domænet overtaget af hackere, der udskiftede indholdet på dem med deres egne sider. Den type angreb kaldes web defacement. Ifølge statistikwebstedet Zone-H var angrebene jævnt fordelt over året, kun maj måned skilte sig ud med over 700 angreb (se Figur 12).

De fleste måneder var der næsten lige mange enkeltangreb og masseangreb. Ved et masseangreb overtager hackeren i ét hug alle de domæner, der ligger på en enkelt IP-adresse. Hvis der er tale om et webhotel, kan en stor mængde domæner på den måde blive ramt. I maj måned udgjorde masseangreb en stor andel af angrebene, der var ikke flere enkeltangreb end i årets øvrige måneder.

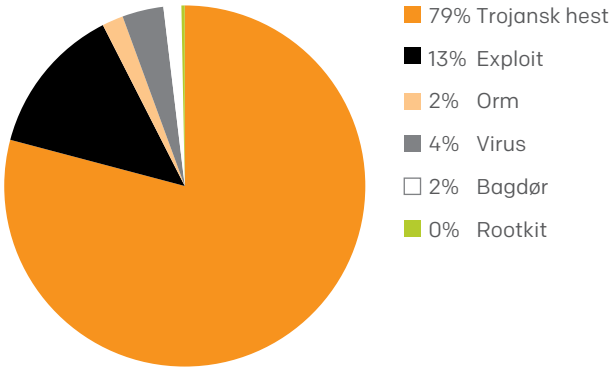
Med i alt 3.345 angreb i 2014 fortsætter de sidste tre års tendens med, at mængden af web defacements falder. Det mest aktive år var 2011, hvor 12.678 danske domæner blev hacket (Figur 13). Ellers skal vi tilbage til 2006 for at finde en voldsom stigning. Dengang skyldtes det Muhammedkrisen, hvor der på to måneder kom over 4.000 angreb.

4.10 > ÅRETS SÅRBARHEDER

I 2014 blev der registreret et rekordstort antal nye sårbarheder i it-systemer: National Vulnerability Database uddelte CVE-numre (Common Vulnerabilities and Expo-

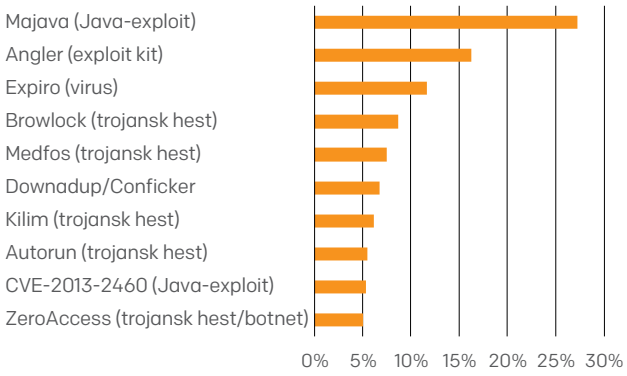
FIGUR 9 Kilde: F-Secure

Malware-infektioner i Danmark fordelt på typer



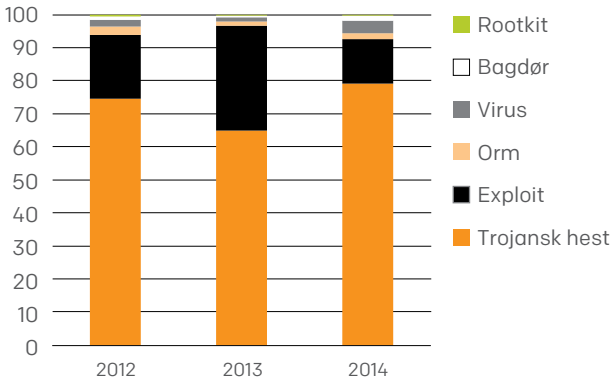
FIGUR 10 Kilde: F-Secure

Topti over malware i Danmark 2014



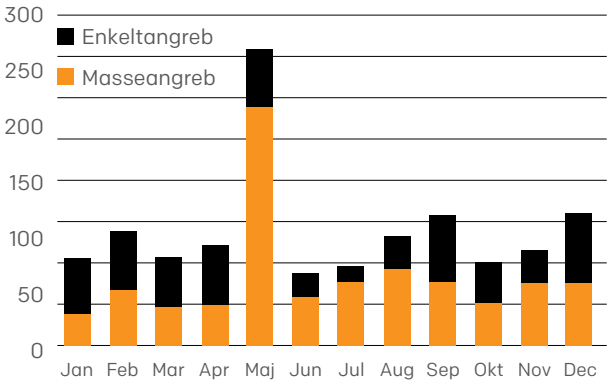
FIGUR 11 Kilde: F-Secure

Fordeling af malware-infektioner i Danmark 2012-2014



FIGUR 12 Kilde: Zone-H

Defacements på dk-domæner i 2014



sures) til i alt 7.937 nye sårbarheder. Det er en stigning på 53 procent i forhold til 2013.

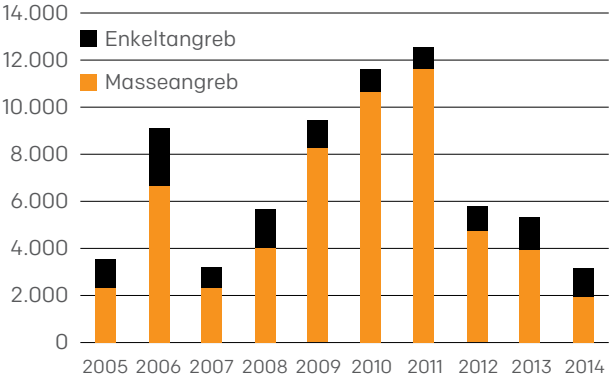
Selvom mængden af alvorlige sårbarheder steg en smule, udgjorde de en mindre andel af sårbarhederne end i 2013. De kritiske sårbarheder tegnede sig for 24 procent af alle sårbarheder mod 33 procent i 2013. Kritiske sårbarheder er defineret som sårbarheder med en CVSS-score (Common Vulnerability Scoring System) fra 7 til 10.

4.10.1 > SÅRBARHEDSSCANNINGER

I 2014 har DKCERT ikke udført sårbarhedsscanninger på systemerne på forskningsnettet. Det skyldes redesign og opgradering af scanningstjenesten. Scanningerne er genoptaget i januar 2015.

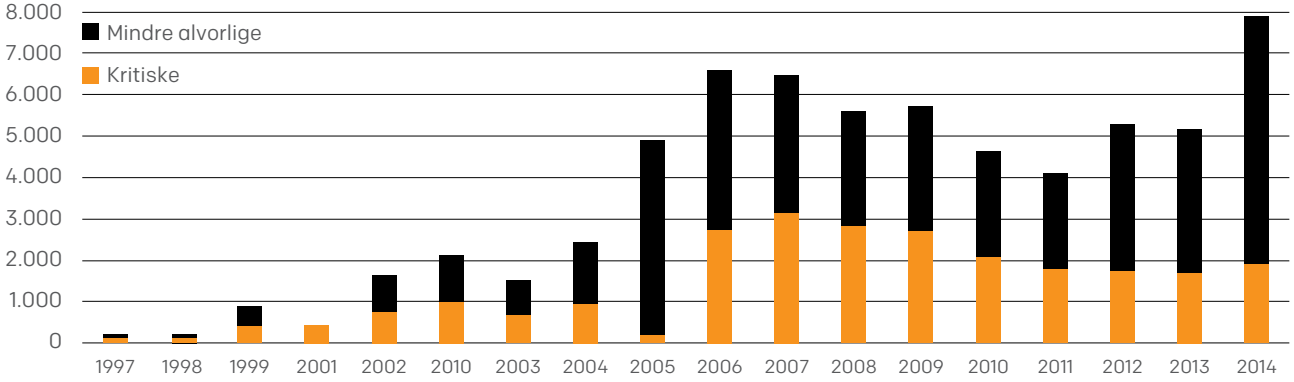
FIGUR 13 Kilde: Zone-H

Defacements på dk-domæner 2005-2014



FIGUR 14

Sårbarheder i IT-systemer ifølge National Vulnerability Database



5. 2014 - året i ord

Angreb kom fra traditionelle hackere, nationalstater og hacktivister i et år, hvor der faldt dom i Danmarks hidtil største hackersag.

5.1 > HVEM STÅR BAG ANGREB?

Nordkorea stod bag et omfattende hackerangreb på Sony – eller gjorde landet nu også det? I 2014 kom det gammelkendte problem med at finde den skyldige bag hackerangreb igen i fokus.

Alle andre end de mindst sofistikerede angribere ved, hvordan de skal dirigere deres angreb gennem computere i andre lande, samt slette sporene efter sig, for at mindske risikoen for at blive opdaget. Hvis man modtager angrebspakker fra en dansk IP-adresse, er det således ikke bevis for, at der står en dansker bag angrebet. Der kan lige så godt være tale om en inficeret eller hacket computer, som bagmændene sender deres angreb igennem.

Den 24. november offentliggjorde ukendte gerningsmand de første af en række fortrolige dokumenter, som de havde fået fat i ved at hacke sig ind på filmselskabet Sony Pictures Entertainment. Senere satte malware på selskabets netværk flere af dets computere ud af drift.

Bagmændene, der kalder sig Guardians of Peace, var kritiske over for filmen The Interview, som stod for at få premiere. Filmen handler om et attentat på lederen af Nordkorea. USA's regering har ytret, at de mener, Nordkorea var centralt involveret i hackerangrebet. Det nægter Nordkorea.

Det amerikanske forbundspoliti, FBI, offentliggjorde flere detaljer, der peger på, at Nordkorea var involveret. Flere eksperter i it-sikkerhed tvivler derimod på, at det er tilfældet[4].

Offentligheden får næppe nogensinde sandheden at vide. Hverken i denne eller en lang række andre hackersager.

DKCERT mener:

Som sikkerhedsfolk må vi acceptere, at vi oftest ikke har en chance for at finde frem til bagmændene. Den viden bør vi naturligvis inddrage, når vi prioriterer vores indsats: Måske giver det mere sikkerhed at øge beskyttelsen af systemerne end at forsøge at finde bagmændene, når det er gået galt.

5.2 > HACKTIVISTER VIL TAGES ALVORLIGT

Hacktivisme – angreb på it-sikkerheden med politiske motiver – eksisterer fortsat. Således dukkede Anonymous-bevægelsen op igen ved flere lejligheder. Det skete for eksempel i november i forbindelse med urolighederne i den amerikanske by Ferguson, hvor politiet havde dræbt en sort, ubevæbnet teenager. Den racistiske organisation Ku Klux Klan uddelte brochurer og truede deltagerne i demonstrationerne.

Det fik Anonymous til at hacke sig ind på flere Twitterkonti, der tilhørte Ku Klux Klan. De demonstrerede, at de havde fået adgang, ved at tweete et billede af en enhjørning fra en Ku Klux Klan-konto[5].

Der har ellers været noget stille om Anonymous siden 2011-12, hvor en række prominente medlemmer blev arresteret. Aktionen mod Ku Klux Klan er da heller ikke startet i USA, men af en australsk gren af bevægelsen.

I begyndelsen af 2015 kom der yderligere livstegn fra Anonymous efter terrorangrebet på det franske magasin Charlie Hebdo. En belgisk gruppe, der brugte navnet Anonymous, iværksatte angreb på websteder, der tilhørte jihadister. Anonymous-folk fra Sverige tog dog afstand til aktionen. Det viser, at Anonymous fortsat er en løst forbundet bevægelse, ikke en stramt organiseret hackergruppe.

DKCERT mener:

Efter en periode med relativ stilhed er Anonymous-bevægelsen tilbage. Det viser, at hacktivisme som begreb ikke er dødt. Betragtet som trussel ser Anonymous mindre alvorlig ud nu, hvor de primært har angrebet svage mål såsom websteder og Twitter-konti med dårlig password-sikkerhed.

[4] Wikipedia: Sony Pictures Entertainment hack, https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

[5] The Independent: Ku Klux Klan Twitter accounts hacked by Anonymous over Ferguson threats, http://www.independent.co.uk/9864764.html

5.3 > INDGREB MOD PRIVATLIVSBESKYTTELSE

Efter terrorangrebet i januar 2015 mod det franske magasin Charlie Hebdo foreslog den britiske premierminister, David Cameron, at det skulle være forbudt at anvende kommunikationsteknologier, som myndighederne ikke kan læse. I praksis ville det betyde et forbud mod krypteret kommunikation, som en række tjenester på nettet benytter sig af[6].

Et tilsvarende forslag kom på banen i USA i oktober. Her slog FBI-direktør James Comey til lyd for, at myndighederne skulle have mulighed for at knække den kryptering, som Apple og Google giver mulighed for på smartphones. [7]

USA's præsident Obama ser ikke ud til at gå så vidt. Men han har foreslået at udvide de i forvejen meget høje straframmer i USA's hackerlovgivning, CFAA (Computer Fraud and Abuse Act)[8].

Disse tiltag er eksempler på, hvordan politikere kan ønske at ændre balancen mellem hensynet til den enkelte borgers privatlivsbeskyttelse og samfundets behov for at beskytte sig mod trusler. Formålet er at forhindre angreb, før de sker, eller opklare dem, efter de er sket.

DKCERT mener:

Tiltag der skal fremme sikkerheden, gør det ofte på bekostning af den enkelte borgers ret til privatliv. Nogle fortalere for overvågning mener, at hvis man ikke har noget at skjule, kan man ikke have noget imod overvågning. De overser, at selve retten til at have et privatliv er en fundamental menneskeret, der blandt andet fremgår af FN's menneskerettighedserklæring og Den Europæiske Menneskerettighedserklæring. Den ret har enhver borger, uanset om vedkommende har noget at skjule eller ej.

5.4 > TRUSLEN FRA USB-PORTEN

USB (Universal Serial Bus) er blevet, hvad navnet siger: Universel. Alle computere har en USB-port, og masser af elektronisk udstyr kan sluttes til den. Derfor er den også en oplagt vej ind i et system for en angriber. Det så vi for nogle år siden med Stuxnet, der var et skadeligt program, som spredte sig via USB-nøgler.

I august 2014 offentliggjorde sikkerhedsforskere sårbarheder i USB-nøgler fra flere leverandører. Sårbarhederne, som de kalder BadUSB, gør det muligt at installere ny firmware på enhederne[9]. Dermed kan USB-udstyr bruges til angreb. For eksempel kan et tastatur fungere som keylogger: Det kan opfange tastetryk og sende dem videre til uvedkommende. Eller USB-nøgler kan installere skadelig software.

Sikkerhedsmæssigt indebærer angrebet den udfordring, at det kan være vanskeligt at opdage. For eksempel kan antivirusprogrammer ikke scanne firmwaren i en USB-enhed.

Der cirkulerede i årets løb en god historie om en topleder, hvis pc blev inficeret via en USB-oplader til hans e-cigaret[10]. Den historie har ikke kunnet verificeres. Men det betyder ikke, at USB-truslen ikke er reel nok.

DKCERT mener:

BadUSB er et eksempel på den risiko, udstyr der ikke i sig selv er computere, kan udgøre for computersystemer. Der skal blot en enkelt inficeret USB-nøgle til at inficere et sårbart system – det har trusler som Stuxnet tidligere demonstreret. Med BadUSB kan en tilsyneladende uskadelig USB-oplader for eksempel agere key-logger.

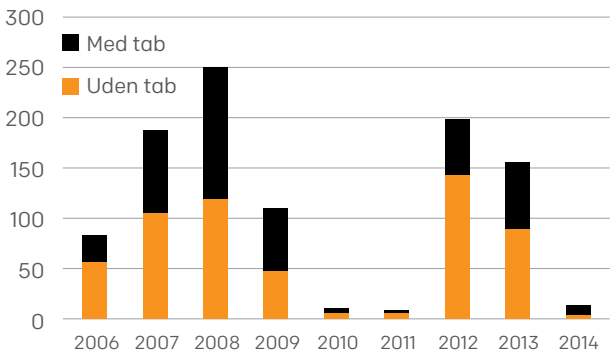
5.5 > BANKRØVERNE GÅR PÅ NETTET – ELLER GØR DE?

Fra 2010 til 2014 faldt mængden af bankrøverier i Danmark med 84 procent. Årsagen er sandsynligvis, at det er blevet sværere for røverne at få udbytte ved et røveri: Der er færre bankfilialer, og flere af dem ligger ikke inde med kontanter.

I stedet kunne man forvente, at mængden af netbankindbrud ville stige[11]. Det skete da også: I 2012 var

FIGUR 15 Kilde: Finansrådet

Netbankindbrud i Danmark med eller uden økonomisk tab. Søjlen for 2014 dækker kun 1.-3. kvartal



der 199 indbrud i netbanker mod 10 i 2011[12]. Men går man længere tilbage, var der 187 indbrud i 2007 og 251 i 2008 (se Figur 15). Det store fald i 2010 og 2011 skyldes sandsynligvis, at bankerne indførte NemID. Herefter gik der et par år, før de it-kriminelle fandt metoder til at omgå NemID-sikkerheden.

[6] The Independent: WhatsApp and iMessage could be banned under new surveil-lance plans, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html

[7] The Guardian: The government wants tech companies to give them a backdoor to your electronic life, http://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi

[8] Ars Technica: Obama wants Congress to increase prison sentences for hackers, http://arstechnica.com/tech-policy/2015/01/obama-wants-congress-to-increase-prison-sentences-for-hackers/?

[9] Security Research Labs: Turning USB peripherals into BadUSB, https://srlabs.de/badusb/

[10] Sophos: Should vapers fear malware-laced e-cigarettes? https://nakedsecurity.sophos.com/2014/11/28/should-vapers-fear-malware-laced-e-cigarettes/

[11] DR: Bankrøvere skifter branche, http://www.dr.dk/Nyheder/Indland/2015/01/06/155959.htm

[12] Finansrådet: Netbankindbrud – statistik, http://www.finansraadet.dk/Tal--Fakta/Pages/statistik-og-tal/netbankindbrud---statistik.aspx

Tallene for de første tre kvartaler af 2014 tyder på et kraftigt fald: I alt var der kun 15 indbrud i den periode. Det samlede tal for 2014 forelå ikke ved redaktionens slutning.

Det lykkes ikke altid for de it-kriminelle at få fat i penge, selvom de bryder ind i en netbank. I 2012 var det gennemsnitlige tab på godt 112.000 kroner. I 2014 var det foreløbig på 32.000 kroner (se Figur 16).

DKCERT mener:

Når en organisation øger den fysiske sikkerhed, gør den det mere tillokkende at angribe virtuelle aktiver. Derfor skal sikkerheden på for eksempel netbanker tilsvarende højnes, når det bliver sværere for røverne at få udbytte ved fysiske røverier.

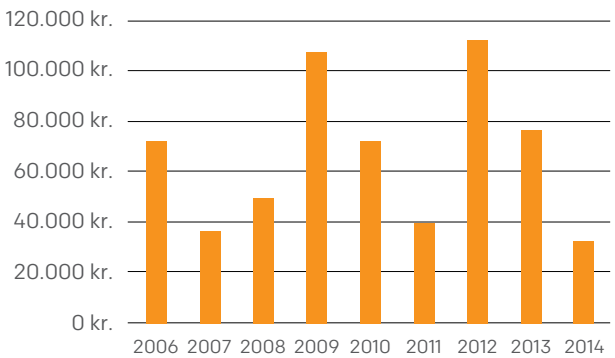
5.6 > CSC-HACKER BLEV DØMT

Den 30. oktober faldt der dom i en af Danmarkshistoriens mest omtalte hackersager: CSC-sagen [13]. En hacker havde brudt ind i en mainframe-computer hos CSC. Her fik vedkommende adgang til flere offentlige registre, heriblandt CPR-registret, politiets kriminalregister og Schengen-registret over internationalt efterlyste personer. Det skete fra den 7. april 2012 til den 27. august 2012.

[13] Version2: Tidslinje over CSC-hackersagen, http://www.version2.dk/interaktiv/csctidslinje

FIGUR 16 Kilde: Finansrådet

Det gennemsnitlige tab ved netbankindbrud i de sager, hvor der var økonomisk tab. Søjlen for 2014 dækker kun 1.-3. kvartal



Svensk politi advarede dansk politi om et muligt angreb i september 2012. Alligevel begyndte dansk politi først efterforskningen i begyndelsen af 2013[14].

Retten på Frederiksberg fandt svenske Gottfrid Svartholm Varg skyldig. En dansker blev fundet delvis medskyldig.

Svenskeren blev dømt, selvom han hævdede, at hans computer, der befandt sig i Cambodia under angrebet, havde været fjernstyret, da angrebet foregik.

DKCERT mener:

Det er positivt, at det lykkedes at få en hacker dømt, selvom der var tale om indicier snarere end beviser. Men sagen afslørede også store problemer med it-sikkerheden hos CSC og med politiets håndtering af sagen. Sagen er derfor en god anledning til at gennemgå it-sikkerheden hos leverandører af it-ydelser til det offentlige, der behandler fortrolige og personfølsomme oplysninger.

5.7 > CLOUD-TJENESTER LÆKKEDE BILLEDER

Knap 500 private billeder af berømtheder, primært kvinder, blev lækket i sensommeren. Flere af billederne viste nøgne personer. Billederne stammede fra Apples iCloud-tjeneste.

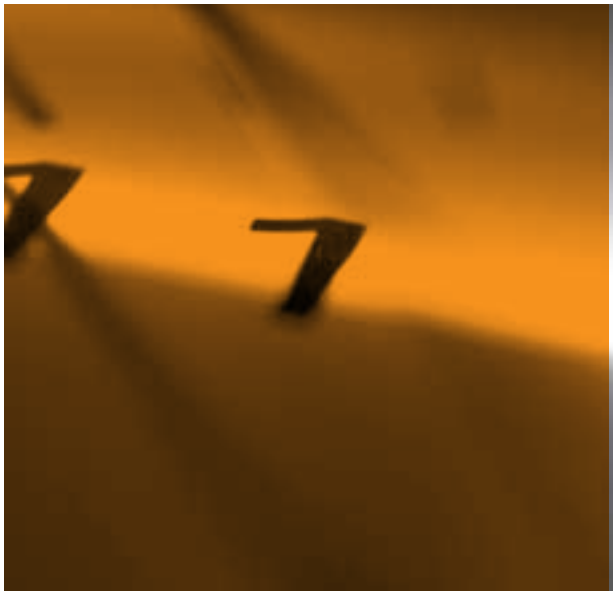
Apple oplyste senere, at hackerne havde udført et målrettet angreb, hvor de for eksempel havde afprøvet passwords eller udnyttet funktionen til at ændre password for en konto. Derimod mente Apple ikke, at angriberne havde udnyttet sikkerhedshuller i tjenesten.

Samtidig med offentliggørelsen af billederne kom der dog et værktøj, som angiveligt udnyttede et sikkerhedshul i tjenesten Find My iPhone til at afprøve passwords. Hullet fjernede den normale begrænsning for, hvor mange gange man må afprøve forskellige passwords[15].

[14] Politiken: Politiet indrømmer: Sov i timen i CSC-hackersag, http://politiken.dk/indland/ECE2468237/politiet-indroemmer-sov-i-timen-i-csc-hackersag/

[15] Jonathan Zdziarski: Hacked Celebrity iCloud Accounts, http://www.zdziarski.com/blog/?p=3783

[16] Engadget: Snapchat servers 'were never breached,' but your snaps may still be compromised, http://www.engadget.com/2014/10/10/snapchat-snapsave-alleged-breach/



I oktober gik det ud over brugerne af tjenesten Snapchat, der gør det muligt at sende billeder og beskeder, som slettes, efter brugeren har set dem. Nogle brugere havde anvendt et websted ved navn Snapsave til at gemme billeder. Det er i strid med Snapchats regler for brug af tjenesten. Snapsave blev øjensynlig hacket, hvorefter data herfra blev lækket[166]

DKCERT mener:

De lækkede private fotos fra iCloud og Snapchat demonstrerer behovet for beskyttelse af brugernes personlige data. Udbydere af den type tjenester bør derfor tilbyde to-faktor-autentifikation, hvor passwords suppleres med engangskoder fra en smartphone eller lignende.

5.8 > Heartbleed fik OpenSSL til at bløde

Den 7. april offentliggjorde udviklerne af krypteringssystemet OpenSSL et alvorligt sikkerhedshul i programmet. Sårbarheden, der blev kendt under navnet Heartbleed, gjorde det muligt at læse nogle data i en servers eller klients hukommelse [17]. Dermed kunne uvedkommende i nogle tilfælde få fat i fortrolige data. Det kunne være passwords eller private nøgler, der anvendes til krypteret kommunikation.

Sårbarheden blev rettet med OpenSSL version 1.0.1g. Ifølge webstatistikfirmaet Netcraft benyttedes omkring en halv million certifikater på potentielt sårbare websteder.

Flere tjenester advarede deres brugere om, at der var risiko for, at deres passwords var kompromitteret. De bad derfor brugerne skifte password.

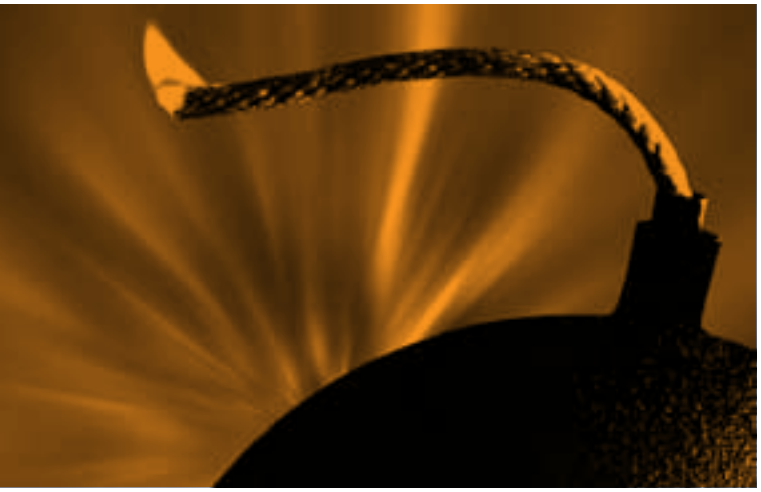
Sårbarheden satte fokus på problemer med sikkerheden og kodekvaliteten i OpenSSL-projektet. En direkte konsekvens blev oprettelsen af Core Infrastructure Initiative[18]. Det er en fond, der finansierer open source-projekter, der er af afgørende betydning for it-infrastruktur. Stifterne skyder hver mindst 100.000 dollars om året i fonden. Blandt de første modtagere af støtte fra fonden er OpenSSL, der får finansieret to fuldtidsudviklere.

DKCERT mener:

Heartbleed viste, hvor afhængig sikkerheden på internettet kan være af ganske få softwareudvikleres indsats. Den demonstrerede behovet for grundige test – og finansiering af dem. Sårbarheden viser også, at selv udviklere af sikkerhedssoftware ikke nødvendigvis har tænkt sikkerheden ind i projektet fra starten.

Vi tilslutter os holdningen hos Rådet for Digital Sikkerhed, der anbefaler, at brugere af OpenSSL fremover som standard anvender Perfect Forward Secrecy.

[17] The Heartbleed Bug, http://heartbleed.com/
[18] Core Infrastructure Initiative, http://www.linuxfoundation.org/programs/core-infrastructure-initiative



5.9 > SHELLSHOCK RAMTE SERVERE

I september blev flere sårbarheder i kommandofortolkeren Bash (Bourne-again shell) under Unix offentliggjort. De blev kendt under navnet Shellshock[19].

Sårbarheden lader en angriber afvikle kommandoer via Bash. Egentlig er der tale om en lokal sårbarhed, idet man skal være bruger på systemet for at udnytte den. Men da mange web-scripts og andre programmer kalder Bash, er det også muligt at udnytte den udefra ved angreb på servere.

Straks efter offentliggørelsen gik angribere i gang med at udnytte Shellshock til at opbygge botnet til DDoS-angreb (Distributed Denial of Service) og scanning efter flere sårbare computere.

Den første sårbarhed blev hurtigt rettet. Men senere fandt forskere flere sårbarheder. Det viste sig også, at de første rettelser ikke fjernede sårbarheden fuldt ud. Den 25. september kom der en rettelse, som øjensynlig beskytter mod alle de huller, der er opdaget.

DKCERT mener:

Sårbarheder som Shellshock og Heartbleed demonstrerer, at også meget udbredte systemer kan have sårbarheder, som oven i købet kan eksistere i mange år. Shellshock-sårbarhederne har været i Bash siden 1989. Derfor er det nødvendigt ikke kun at teste ny software, men også undersøge eksisterende løsninger for mulige sikkerhedshuller.

5.10 > PUDDEL ANGREB GAMMEL SSL-VERSION

POODLE (Padding Oracle On Downgraded Legacy Encryption) blev navnet på årets tredje store sårbarhed på internettet[20]. Den fik dog mindre praktisk betydning end Heartbleed og Shellshock, da den er mere krævende at udnytte til angreb.

Der er tale om en sårbarhed i den forældede version 3 af SSL (Secure Sockets Layer). Angrebet udnytter, at nogle browsere automatisk skifter over til den version, hvis en server ikke understøtter nyere versioner af krypteringsprotokollen. Det giver en angriber mulighed for at dekryptere data: Med 256 forespørgsler til serveren kan angriberen dekryptere en byte. Det gør det praktisk muligt at afkode de sessions-cookies, der styrer en brugers adgang til en server.

Men der er tale et man-in-the-middle-angreb. Derfor skal angriberen have mulighed for at placere sin computer mellem offerets browser og serveren. Endvidere skal browseren være indstillet til at acceptere SSL 3.

Disse hindringer er nok årsagen til, at vi ikke har hørt om større angreb, der udnyttede POODLE.

DKCERT mener:

POODLE-sårbarheden demonstrerer, at gamle sårbarheder kan dukke op på ny. Den understreger, hvor vigtigt det er at rydde op: Brugere og systemadministratorer bør fjerne programmer og protokoller, som de ikke længere har brug for.

[19] Wikipedia: Shellshock (software bug), https://en.wikipedia.org/wiki/Shellshock_%28software_bug%29

[20] Bodo Möller, Thai Duong og Krzysztof Kotowicz: This POODLE Bites: Exploiting The SSL3.0 Fallback, https://www.openssl.org/~bodo/ssl-poodle.pdf

5.11 > MAKROVIRUS GJORDE COMEBACK

De fleste havde regnet makrovirussen for død og borte. Men den gjorde comeback i 2014.

En makrovirus er skrevet i et scriptingsprog, typisk VBA (Visual Basic for Applications), og indlejret i et dokument. Den mest kendte og ødelæggende makrovirus var I Love You-virussen, der hærgede nettet i år 2000.

Siden ændrede Microsoft på opsætningen af Office-pakken, så brugeren aktivt skal tillade, at makroer afvikles. Det er sandsynligvis årsagen til, at denne type trussel stort set er forsvundet.

Indtil nu. I januar 2014 rapporterede det hollandske National Cyber Security Center, at makrovirus var blevet brugt i meget målrettede angreb i landet. Senere offentliggjorde sikkerhedsforsker Gabor Szappanos fra Sophos en analyse af et angreb med malwaren Napolar i slutningen af 2013[21] . Analysen viste, at Napolar brugte Word-makroer til at sprede sig.

Sidst på året kunne Microsoft Malware Protection Center fortælle om et stigende antal makrovirus. De havde især observeret to familier, Adnel og Tarbir[22].

Den nye generation af makrovirus har ikke fundet en teknisk metode til at omgå Office-pakkens beskyttelsesmekanismer. I stedet narrer de brugeren: I det inficerede dokument kan der være et område med en tekst, der er gjort så utydelig, at den ikke kan læses. Over teksten står der, at teksten er sløret af sikkerhedsmæssige hensyn. For at kunne læse den skal modtageren slå makroer til. Sker det, inficeres computeren.

DKCERT mener:

Makrovirussens genkomst viser, at tekniske hindringer sjældent er tilstrækkelige til at stoppe en trussel. Det er også nødvendigt at uddanne brugerne i at genkende og afværge trusler.

5.12 > VÆKST I DANSKE IT-SIKKERHEDSFIRMAER

Året igennem har vi set en vækst i mængden af danske firmaer, der beskæftiger sig med it-sikkerhed. Det bekræftede direktør Morten Bangsgaard fra brancheorganisationen IT-Branchen i april over for mediet Finans.dk[23].

"Vi kan se, at der er flere virksomheder, der kommer ind på det her marked, og vi kan se, at konkurrencen er blevet hårdere," sagde han.

I DKCERT mærker vi væksten ved, at de nye firmaer ofte henvender sig. Nogle vil blot drøfte aktuelle trends, andre spørger direkte til et samarbejde.

DKCERT mener:

Det er positivt, at flere virksomheder ser vækstpotentialet i it-sikkerhed. Det kan være med til at øge opmærksomheden om emnet – og i det lange løb forbedre it-sikkerhedsniveauet generelt i Danmark.

[21] Gabor Szappanos: VBA Is not dead, https://www.virusbtn.com/virusbulletin/archive/2014/07/vb201407-VBA

[22] Microsoft Malware Protection Center: Before you enable those macros... http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx

[23] Finans.dk: Frygt for hacking skaber nye it-virksomheder, http://finans.dk/artikel/ECE6636192/frygt_for_hacking_skaber_nye_it-virksomheder/

6. Det eksterne perspektiv

Fem personer uden for DKCERT giver her deres syn på emnet sikkerhed og leverandørrelationer.

Temaet for dette års trendrapport er, at en organisations it-sikkerhed er afhængig af sikkerheden hos underleverandører. Det gælder både traditionelle underleverandører som softwarehuse og outsourcingfirmaer og nye løsninger baseret på cloud.

I dette kapitel gennemgår Niels Christian Ellegaard og Michael Hopp fra advokatfirmaet Plesner indholdet af et bud på standardisering af SLA'er for cloud-løsninger. Anne Ermose og Ole Kjeldsen fra Microsoft Danmark giver råd til, hvordan en organisation kan vurdere it-sikkerheden hos sin cloud-leverandør.

Rasmus Theede fra KMD skriver om forholdet til den interne underleverandør og den rolle, OLA'er (Operational Level Agreement) spiller. Martin Bech fra DeIC (Danish e-Infrastructure Cooperation) beskriver, hvordan brugervenlighed har indflydelse på sikkerheden i cloud-systemer. Endelig gennemgår Henrik Jensen fra Roskilde Universitet EU's kommende persondataforordning og hvordan universitetet griber den an.

6.1 > FÅ STYR PÅ DIN CLOUD-SLA MED EU-VEJLEDNING

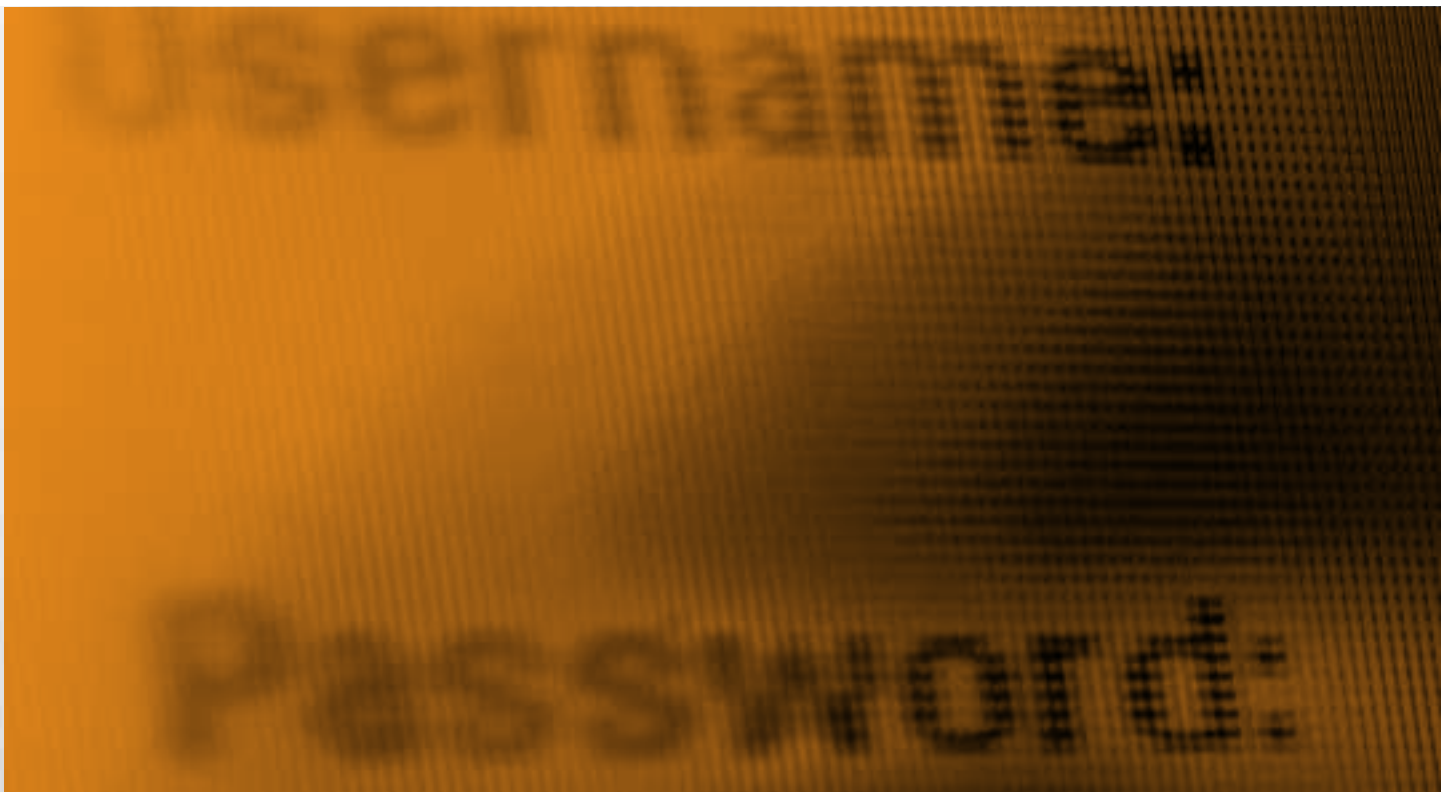
Af advokaterne Michael Hopp og Niels Chr. Ellegaard, Plesner

I juni 2014 fremsendte "The Cloud Industry Group" et forslag til en standardiseringsguideline for Service Level Agreements (SLA'er) for cloud services til EU-Kommissionen.

Målet er at skabe en ramme, som på den ene side giver en klar og fælles definition, og som på den anden side er neutral i forhold til teknologi og forretningsmodel. Rammen skal kunne anvendes globalt og uanset kundens størrelse og øvrige karakteristika for derved at skabe størst mulig sammenlignelighed.

For at opnå det opstiller SLA'en en række målsætninger (Service Level Objectives, SLO'er). Men da der netop er tale om målsætninger (hvad skal opnås), er det vigtigt, at cloud service-udbyderne er åbne om deres processer og metoder (hvordan de vil opnå de pågældende målsætninger).

Da der er tale om en standard, er de beskrevne Service Level Objectives ikke nødvendigvis udtømmende. De er



heller ikke nødvendigvis alle relevante for enhver aftale om cloud services. Det vil altså stadig være op til aftaleparterne – med udgangspunkt i standarden – at definere netop de krav og mål, som er relevante i det konkrete tilfælde.

I praksis stiller det særlig krav til, at køberen forholder sig til de forretningsprocesser og data, som en eventuel cloud-løsning skal understøtte eller behandle. Køberen må også tage stilling til, hvilke drifts- og sikkerhedsmæssige aspekter det er særligt vigtigt at sikre bliver tilgodeset.

Aftaleparterne skal stadig definere og specificere de krav og mål, der er vigtige for aftalen. Som det er nævnt i standarden, bør arbejdet med den konkrete aftale overlades til kompetente og erfarne advokater.

6.1.1 > TONEANGIVENDE HOLD BAG VEJLEDNINGEN

Standarden er udarbejdet af arbejdsgruppen Cloud Select Industry Group (C-SIG SLA Subgroup) nedsat af EU-Kommissionen. Arbejdsgruppens medlemmer kommer fra blandt andet Cloud Security Alliance, Microsoft, Amazon, Google, IBM, Salesforce og Oracle.

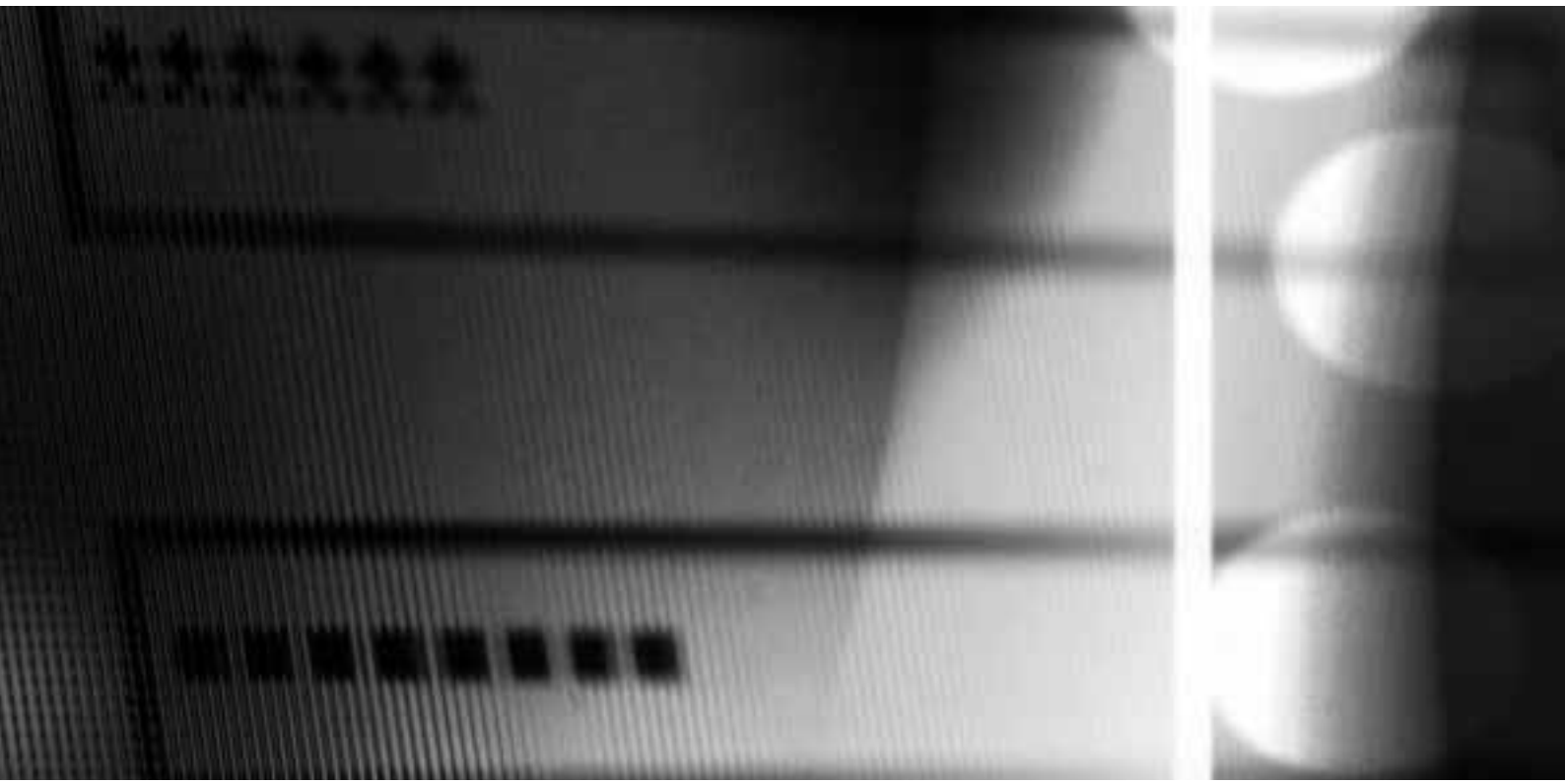
Standarden fastsætter ikke pligtmæssige krav, der skal overholdes i en cloud-SLA. Men den giver nyttige oplysninger til lovgivere, cloud-kunder og cloud-udbydere, når de skal fastsætte de konkrete cloud-SLA'er i kontrakten. Der findes nemlig i dag ikke standarder for cloud-SLA. Mange tager derfor udgangspunkt i standarder for hostingløsninger, der kun er direkte anvendelige for visse cloud-tjenester.

6.1.2 > VÆR KLAR TIL NY INTERNATIONAL STANDARD

Standarden er ikke kun brugbar her og nu til udformning af cloud-SLA. Der arbejdes også på, at standarden skal indgå i ISO/IEC 19806-projektet.

Idet gruppen består af flere sværvægtere inden for cloud, er det ikke utænkeligt, at standarden vil indgå i en kommende formel standard.

Der er gode erfaringer og billige point at hente ved at lade sig inspirere af standarden, og det kan give tryghed for de involverede parter, at der tages afsæt inden for en dedikeret cloud-ramme.



6.1.3 > DE VÆSENTLIGSTE PUNKTER

Standardens væsentligste afsnit vedrører først og fremmest en definition af cloud-begreber og spørgsmål om, hvilke overvejelser man bør inddrage i relevante SLO'er i forhold til en række elementer:

- Ydelse (tilgængelighed, svartider, kapacitet, funktionalitetsindikatorer, support, reversibilitet og ophør).
- Sikkerhed (driftssikkerhed, autentificering og autorisation, kryptografi, håndtering af sikkerhedshændelser, logging og monitorering, auditering og sikkerhedsverificering, sårbarhedsstyring og governance).
- Datahåndtering (dataklassificering, spejling, backup og genskabelse, data life cycle og dataportabilitet).
- Databeskyttelse (code of conduct, standarder og certificeringer, formålsafgrænsning, dataminimering, begrænsninger på brug, opbevaring og videregivelse, gennemsigtighed og underretning, accountability, angivelse af fysisk behandlingssted og intervenability).

> ***SLA'er har kun værdi i det omfang, de kan måles.***

Navnlig databeskyttelse er et emne, der optager mange europæiske brugere af cloud-tjenester og myndigheder - fx Datatilsynet i Danmark i de to sager om henholdsvis Google Docs og Microsoft Office 365.

Afsnittet om databeskyttelse afspejler de forhold, som de europæiske databeskyttelsesmyndigheder har tillagt stor betydning ved vurderingen af tjenesterne. Man er derfor godt hjulpet i forhold til myndighedskravene ved at skæve til dette afsnit.

6.1.4 > VÆR OPMÆRKSOM PÅ FORHANDLING AF SLA'EN

En særlig problemstilling virksomheder og organisationer skal være opmærksomme på, er muligheden for at forhandle en allerede udarbejdet cloud-SLA. Cloud-tjenester er typisk en standardtjeneste, og det betyder ofte, at udbyderen vil være utilbøjelig til at ændre i SLA. Det giver meget ofte problemer, ikke mindst ved forholdsvis nye udbydere på markedet, hvor SLA'en måske ikke er tilstrækkelig gennemarbejdet og tilpasset den konkrete tjeneste.

Her er det vigtigt at være opmærksom på, at mange cloud-SLA'er vil være undergivet udenlandsk ret. Kunden er nødt til at vurdere, om tjenesten både lever op til de tekniske krav og til de krav, kunden stiller i forhold til risici og det retsmæssige. Lever udbyderen ikke op til de krav, og kan SLA'en ikke forhandles, kan det føre til, at kunden må afstå fra at indgå aftale med udbyderen.

SLA'er har kun værdi i det omfang, de kan måles. Målemetoden er derfor afgørende for værdien af SLA'erne. Parterne bør derfor også sikre sig, at der er en fælles forståelse af målemetoden for de vedtagne SLA'er – og at ændring heri sker under aftalte former.

Med dette opmærksomhedspunkt in mente giver standarden samlet set et godt udgangspunkt for, at de relevante områder berøres i en cloud-SLA. Husk dog, at djævlen ligger i detaljen, og at den konkrete kontrakt altid bør overlades til en kvalificeret advokat.

> ***Standarden giver samlet set et godt udgangspunkt for, at de relevante områder berøres i en cloud-SLA.***

6.2 > HVORDAN VURDERER JEG IT-SIKKERHEDEN HOS MIN CLOUD-LEVERANDØR?

Af advokat Anne Ermose og teknologidirektør Ole Kjeldsen, Microsoft Danmark

I 2014 blev cloud computing for alvor mainstream hos såvel borgere som virksomheder og offentlige organisationer. Når der samtidig er fokus på it-sikkerheden, er evidensbaseret tillid til de platforme og leverandører, man som organisation vælger at benytte, helt afgørende.

Den tillid kan kun etableres gennem kritisk vurdering af leverandørens håndtering af både sikkerhedslag, privatlivsbeskyttelse, gennemsigtighed og ikke mindst overholdelse af internationale standarder og certificeringer.

Men hvordan skal man som kunde vurdere sin leverandør, så man sikrer sig, at man ud over strategiske, økonomiske og konkurrencemæssige fordele også får en sikker løsning – endda en sikrere løsning end mange har i dag?

6.2.1 > KRAV TIL LEVERANDØRER

Skåret ind til benet er cloud computing drevet af stordriftsfordele, som kommer alle parter til gode. Teknologien tillader leverandøren at drifte identiske services til tusindvis af forskelligartede kunder. Men det indebærer samtidig, at kunder ikke individuelt kan justere eller ændre f.eks. driftskontrakter for at tilgodese enkeltbehov.

Derfor er det helt centralt for potentielle cloud-kunder at investere tid og ressourcer i at forstå leveringsaftalen, servicemål og overordnede kendetegn ved den vurderede platform. Kunden bør overordnet stille krav til leverandøren om, at dokumentationsmateriale er let tilgængeligt, og at der tilbydes klare leveringsaftaler.

Nedenfor er fremhævet en række fundamentale forhold, man som kunde minimum bør få svar på:

6.2.2 > HVORDAN UDØVER JEG KONTROL MED DATABEHANDLING OG IT-SIKKERHED?

Individuelle fysiske inspektioner af cloud-datacentre er oftest praktisk umulige, da de udgør en ikke ubetydelig sikkerhedsrisiko for leverandøren. Udfordringen er her, at for personhenførbare informationer kræver persondataloven, at den dataansvarlige udøver kontrol med databehandlingen hos databehandleren. Det er dog almindeligt anerkendt, at for cloud kan kontrol udøves ved hjælp af uafhængige tredjepartsinspektioner, f.eks. på grundlag af en international standard som ISO 27001.

6.2.3 > HVEM EJER MINE DATA, OG HVORDAN KAN DE BRUGES?

For de fleste vil det være selvfølgeligt, at de bevarer ejendomsretten til egne data, og at kundedata kun kan bruges af leverandøren til at levere servicen. Den selvfølgelighed kan man blot ikke altid forvente i forbindelse med cloud-leverancer, hvor datadrevne forretningsmodeller kan ændre ejerforholdet. Sådan en afledt kommerciel brug af kundedata kan rejse persondataretlige spørgsmål og skal også af den grund overvejes nøje.

6.2.4 > HVEM HAR ADGANG TIL KUNDEDATA OG PÅ HVILKE VILKÅR?

Som kunde har man en klar, berettiget forventning om, at adgang til kundedata for tredjeparter er stærkt begrænset. En leverandør skal klart kunne beskrive, hvilke tredjeparter (f.eks. underleverandører) der får adgang til data og under hvilke omstændigheder.

Leveringsaftalen bør også fastlægge, at leverandøren er ansvarlig for underleverandører. Behov for fleksibilitet i forhold til udskiftning af underleverandører bør reguleres ved f.eks. at pålægge leverandøren ansvar for notifikation ved udskiftning af underleverandører.

En særlig problemstilling relaterer sig til adgangen for myndigheder til at tilgå kundedata. Leverandører er forpligtet til at følge lovgivningen i de lande, de opererer i, men myndighedsadgang bør være begrænset til tilfælde, hvor der eksisterer en juridisk forpligtelse til at give adgang. Kunden bør som minimum modtage forudgående information om myndighedsadgang, medmindre sådan information er forbudt.

6.2.5 > ER DER GENNEMSIGTIGHED I FORHOLD TIL GEOGRAFISKE OVERFØRSLER AF DATA?

Persondataretten beskriver, at overførsel af personhenførbare data frit kan ske inden for EU. Overførsel ud af EU bør kun ske, hvis databehandlingen i det modtagende land anses for at være tilstrækkelig sikker. Efter dansk ret anses behandlingen af data for at være tilstrækkelig sikker, uanset hvor i verden behandlingen sker, såfremt der mellem kunde og leverandør er aftalt EU-kommissionens Standard Modelkontrakt. Aftalen om EU-USA Safe Harbor kan som alternativ dække overførslen til Safe Harbor-certificerede leverandører i USA.

6.2.6 > ER DER KLARHED OVER SUSPENSION OG EXIT- BETINGELSER?

Cloud-leverandøren kan have legitime interesser i at suspendere eller undtagelsesvist helt opsige en leverance, f.eks. hvis en kunde bruger en service på ulovlig vis eller udgør en sikkerhedsrisiko for andre kunder. Sådanne betingelser skal naturligvis være klare, præcise og rimelige.

Tilsvarende gælder for bestemmelser om kundens beslutning om opsigelse af leveringsaftalen. Her er det navnlig vigtigt at have præcise aftalebestemmelser om, hvordan man kan flytte sine data og inden for hvilke tidsfrister. En leverandør bør også kunne forpligte sig til uigenkaldeligt at slette alle kundedata efter et vist antal dage.

6.2.7 > ER DER FLEKSIBILITET I ARKITEKTUR OG ØKOSYSTEM?

Brug af cloud indledes ofte med enten specifikke løsninger, som kræver minimal integration med eksisterende infrastruktur (f.eks. disaster recovery), flytning af hele isolerede workloads eller opbygning af en ny løsning helt fra bunden i cloud, fordi det er nemmest. Hurtigt derefter søges så endnu større gevinster ved enten at flytte hele eller dele af eksisterende løsninger til en cloud-platform i såkaldte hybrid cloud-scenarier. Således ender man med at have behov for både IaaS-, SaaS- og PaaS-løsninger.

Det er derfor afgørende for valg af cloud-platform, at den er fuldt fleksibel i understøttelse af disse forskellige løsningsarkitekturer og ikke kun tilbyder et rent cloud-scenarie, hvor alt i en løsning skal flyttes eller bygges til afvikling i skyen. Vurdér også bredden og kvaliteten af platformens økosystem af partnere. Kan man få den nødvendige tekniske assistance og rådgivning?

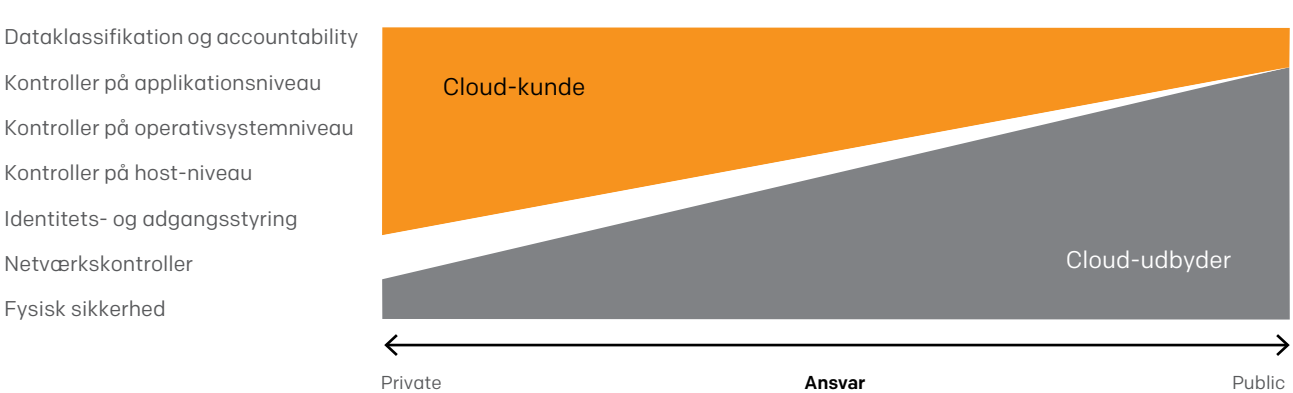
> ***En leverandør skal klart kunne beskrive, hvilke tredjeparter der får adgang til data og under hvilke omstændigheder.***

6.2.8 > HVORDAN ER DEN SIKKERHEDSMÆSSIGE ROLLEFORDELING?

Det er vigtigt at gøre sig klart, at efter persondataloven kan en dataansvarlig ikke fraskrive sig ansvaret for behandling af personoplysninger, heller ikke selvom databehandlingen finder sted hos en ekstern databehandler. Stil derfor krav om gennemsigtighed i drift og f.eks. revisionsrapporter og ikke mindst overholdelse af valgte standarder og certificeringer. Kun sådan er der mulighed for objektivt at vurdere risici i forhold til dette ansvar. Figur 17 illustrerer forholdet og angiver, hvilke sikkerhedslag leverandøren bør have ansvaret for.

FIGUR 17

Fordelingen af ansvaret for sikkerheden mellem kunde og udbyder afhænger af, om man anvender privat eller public cloud



6.2.9 > UDNYT POTENTIALET I CLOUD

Ovenstående tjekliste er en god, men ikke udtømmende start, når man skal vurdere sin cloud-leverandør. På trods af udfordringerne viste 2014, hvor stort potentiale der er i cloud for brugere, organisationer og samfundet som hele. Det tjener os til gavn som samfund, at danske virksomheder og den offentlige sektor ikke er i tvivl, om de skal udnytte nye muligheder, men alene vurderer hvornår, hvad og hvor meget.

Endnu udestår, at vi som samfund tager hånd om alle de politiske og juridiske elementer, som ofte kan hæmme udnyttelsen af det fulde potentiale – men det er en helt anden og længere historie!

> ***Efter persondataloven kan en dataansvarlig ikke fraskrive sig ansvaret for behandling af personoplysninger, heller ikke selvom databehandlingen finder sted hos en ekstern databehandler.***

6.3 > INTERNE AFDELINGER ER OGSÅ LEVERANDØRER

Af koncernchef for kvalitet & sikkerhed
Rasmus Kærsgaard Theede, KMD

En Operational Level Agreement (OLA) er en kontrakt, der definerer, hvordan forskellige it-afdelinger inden for en virksomhed planlægger at levere en specifik service eller tjeneste.

OLA'en bliver ofte glemt, når SLA'en (Service Level Agreement) er på plads. Det er en skam. OLA'en er nemlig designet til at løse problemet med it-siloer og tendensen til at "pege fingre". Det gør den ved klart at definere et sæt leverancekriterier, som hver it-afdeling er ansvarlig for.

I modsætning til Service Level Agreements (SLA), som dokumenterer de specifikke mål, oplyser OLA'en præcist, hvordan de involverede parter i en leverance vil interagere med hinanden for at nå disse mål. OLA'ens formål er derfor at sikre samarbejde, og dermed sammenhæng, i leverancen.

Hvis OLA'en ikke er på plads især ved mere komplekse it-leverancer, der spænder over flere afdelinger, er det ofte svært for organisationer at definere, hvordan de vil overholde servicemål. Det gør det også svært at afgøre, hvor der skal ske forbedringer, hvis målene ikke stemmer overens med forventningerne. OLA'en er derfor en vigtig del af såvel ITIL (Information Technology Infrastructure Library) som kvalitetsprocessen.

> ***Hold OLA'en så simpel, men specifik som muligt.***

> ***OLA'ens formål er at sikre samarbejde og sammenhæng i leverancen.***

6.3.1 > KAN GÅ UD OVER SIKKERHEDEN

Forhåbentlig er sikkerheden en integreret del af enhver it-leverance. Sikkerheden vil komme til at lide, hvis det ikke er klart defineret, hvem der gør hvad. Hvem har for eksempel ansvaret for at udbedre sårbarheder i en nyudviklet applikation? Hvem sørger for daglig backup? Hvem sikrer dokumentation m.m.?

Er der ikke en klar OLA, er svaret meget ofte: ingen. Og når det så går galt, ender man ofte med at skændes om, hvem der burde have haft ansvaret. Med OLA'en undgås det. Ansvaret er klart defineret, og man ved præcis, hvor kæden hoppede af, så man kan implementere de nødvendige forbedringer.

Der findes en mængde frit tilgængelige templates, metoder og teknikker til at udforme OLA'er. Mit bedste råd er at holde OLA'en så simpel, men specifik som muligt for at undgå misforståelser. Derudover:

1. Start med at definere præcist, hvad vi gerne vil opnå. Det står ofte i SLA'en.
2. Definer de centrale aktører (udviklingsgruppen, netværksafdelingen, serveransvarlige med flere). Hvem har ansvaret for hvad?
3. Forstå og beskriv præcist, hvad de enkelte aktørers rolle er i leverancen. Og vær enige.
4. Planlæg, hvem der håndterer de uforudsete begivenheder, der vil opstå, så intet falder mellem stolene.
5. Test og test igen. Foretag ændringer, når der er nødvendigt. En OLA er sjældent statisk.

En OLA har kun værdi, hvis den bliver overholdt af alle parter, og der er enighed om den. Den skal derfor ikke kun være kendt af ledelsen, eller af dem der har udformet den, men af hele leveranceapparatet fra A til Z.

6.3.2 > KONSEKVENSER ER NØDVENDIGE

Bliver den alligevel ikke overholdt, er det vigtigt, at det får konsekvenser. Der skal udformes en skriftlig beskrivelse af afvigelsen, så man kan finde ud af, hvorfor OLA'en ikke blev overholdt, og hvordan man forhindrer, at det sker igen.

Her er ledelsens opbakning som altid helt nødvendig.

GOD ARBEJDSLYST!

6.4 > SIKKER ANVENDELSE AF CLOUD KRÆVER BRUGERVENLIGHED

Af divisionsdirektør Martin Bech, DeIC

Forskere og undervisere har brug for at dele dokumenter og data med hinanden og med kontakter uden for deres eget universitet eller institut. I dag er den oplagte løsning til den opgave en cloud-tjeneste. Systemer som Dropbox og Facebook gør det let at oprette grupper, der deles om data.

Den type systemer løser et konkret problem. For eksempel er det ikke let at give en medarbejder i en virksomhed adgang til data i it-systemerne på et universitet, selvom vedkommende deltager i et forskningsprojekt. Hvis data fra projektet udgøres af filer, er det til gengæld let at dele dem med en cloud-løsning.

Men det udgør en udfordring for informationssikkerheden. For de populære cloud-systemer er ikke bygget med henblik på de sikkerhedskrav, et universitet stiller. For eksempel garanterer udbyderne ikke, at person-følsomme data behandles efter persondatalovens krav.

Derfor er vi, der beskæftiger os med it i den akademiske verden, på udkig efter sikre alternativer til de populære cloud-løsninger.

Vi gør os umage for at sikre, at alternativerne leverer den sikkerhed, som de udbredte systemer ikke kan garantere. I kravspecifikationerne stiller vi krav om, at der indgås databehandleraftaler, at personfølsomme data ikke udleveres til tredjeland og lignende. Så vi har styr på den formelle sikkerhed.

6.4.1 > BRUGERNE VÆLGER FRIT

Erfaringerne viser imidlertid, at det er svært at få brugerne til at flytte over til vores alternative løsninger.

I universitetsverdenen har vi en god tradition for frit valg af metoder og værktøjer. Derfor kan og vil vi ikke gennemtvinge, at de ansatte og studerende bruger de alternativer, vi stiller til rådighed. Men når det ikke er muligt, må vi i stedet sikre, at vores alternative løsninger er konkurrencedygtige.

> ***Vi skal vænne os til at se sikkerhed for institutionen som meget mere end sikkerheden på de it-systemer, vi har kontrol over.***

De skal simpelthen være lige så brugervenlige, enkle at bruge og lækre at se på som de udbredte cloud-løsninger, de konkurrerer med.

Det har vi nok overset i den akademiske it-verden. Vi har fokuseret på de formelle sikkerhedskrav. Men vi har glemt, at vores alternativer skal konkurrere med de løsninger, vores brugere selv har valgt – eller i hvert fald fungere som supplement til dem.

Derfor mener jeg, at universiteter og andre i den akademiske it-verden skal tænke på sikkerhedskrav på en ny måde: I dag er det en sikkerhedsmæssig ulempe, hvis et system er vanskeligere at bruge end en gratis og udbredt konkurrent.

6.4.2 > STIL HØJE KRAV TIL BRUGERVENLIGHED

Så vi skal skrive krav om brugervenlighed ind i kravspecifikationerne. Det gælder både, når vi indkøber cloud-services, og når vi selv udvikler alternative løsninger.

Hvis vores alternativer ikke er brugervenlige, er det ligegyldigt, om de er sikre – for brugerne anvender dem ikke.

Brugervenlighed skal her forstås i den mest udvidede forstand. Det handler også om, hvorvidt tjenesten er tiltalende ud fra en følelse af "trendyness," "lækkerhed" og andre bløde aspekter, som vi som sikkerhedsfolk er noget uvante med at forholde os til.

6.4.3 > INTERN IT KONKURRERER MED CLOUD

For tiden står slaget især om tjenester af Dropbox-typen. Men en tilsvarende tendens er på vej inden for masser af områder, som ellers tidligere har været bestemt af arbejdsgiveren. Det gælder mail, kalender, telefonsamtaler, videokald, computing og adgang til speciel software. Kort sagt er it-afdelingerne nu i en konkurrencesituation med tjenester, som findes ude på nettet.

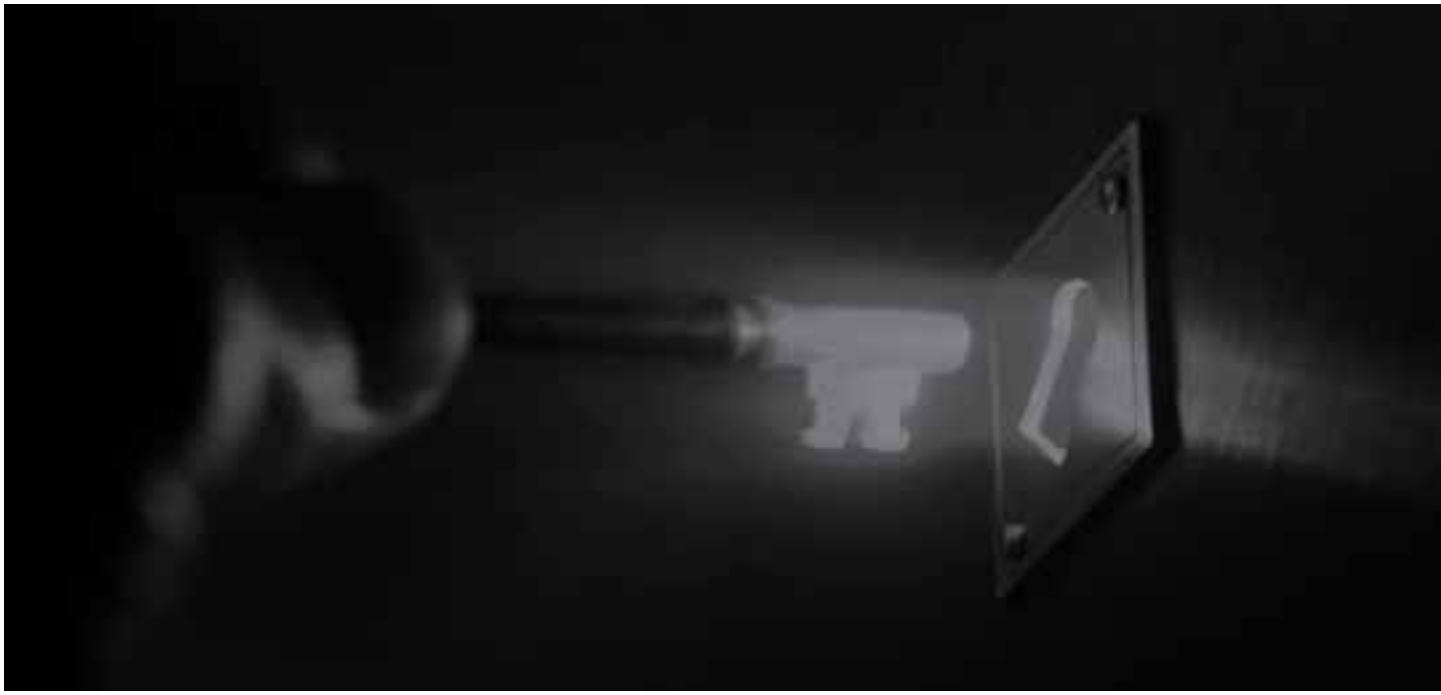
Vi skal altså vænne os til at se sikkerhed for institutionen som meget mere end sikkerheden på de it-systemer, vi har kontrol over. Vi skal tage brugernes adfærd med vores data i betragtning. Vi må erkende, at hvis vores systemer ikke er brugervenlige og relevante, så anvender brugerne bare noget andet.

Man kan selvfølgelig tage en dialog med sine ansatte om, hvilke tjenester de bruger. Men på et universitet vil den dialog have svære vilkår, hvis de alternativer vi anviser, er for lukkede, for gammeldags eller måske har for lidt kapacitet.

Det er på tide at vurdere vores tjenesteudbud ud fra nye kriterier – af hensyn til sikkerheden!

> ***Hvis vores alternativer ikke er brugervenlige, er det ligegyldigt, om de er sikre – for brugerne anvender dem ikke.***

> ***Vores systemer skal simpelthen være lige så brugervenlige, enkle at bruge og lækre at se på som de udbredte cloud-løsninger, de konkurrerer med.***



6.5 > EU'S DATABESKYTTELSESFORORDNING SKÆRPER KRAV TIL PERSONDATAHÅNDTERING

Af it-sikkerhedskonsulent Henrik Jensen, Roskilde Universitet

Er din organisation klar til at håndtere EU's kommende persondataforordning? Da forordningen ventes vedtaget inden for de næste halvandet år, er vi på Roskilde Universitet allerede begyndt at kigge på kravene i forordningen. Med udgangspunkt i de hovedlinjer der allerede kendes, har vi valgt at fokusere på de krav, der kendes fra det nuværende udspil.

Den teknologiske udvikling og særlig den stigende udveksling af personoplysninger via elektroniske tjenester i forbindelse med e-handel og brug af sociale medier nødvendiggør en opdatering af reglerne for beskyttelse af personoplysninger, som anvendes i it-mæssig sammenhæng.

EU-kommissionen har taget initiativ til en opdatering. Den får form af en forordning, der modsat et direktiv ikke skal implementeres i medlemslandenes nationale lovgivning, men har direkte virkning. Forordningen skal afløse det nuværende direktiv om databeskyttelse. Med valget af en forordning lægges der op til, at den danske persondatalov ophæves.

6.5.1 > ØGET FOKUS PÅ PRIVACY

Den ny forordning vil, ud over at have fokus på de allerede eksisterende myndighedskrav i den nuværende persondatalovgivning, have et skærpet fokus på privacy. Det er en væsentlig opstramning i forhold til den eksisterende danske persondatalov.

Forordningen betyder, at virksomheder og organisationer får større krav om at tage ansvar for databeskyttelse. Der strammes op med nye forpligtelser for at øge fokus på databeskyttelse. Samtidig sker der en smidiggørelse og harmonisering af reglerne for hele EU.

Med forordningen falder den danske persondatalov helt bort. Samtidig giver forslaget mere magt til EU-kommissionen og til et "overdatatilsyn" på EU-niveau via det såkaldte one-stop-shop-forslag. Den ny forordning indeholder skrappere sanktionsmuligheder end dem, vi kender i dag. Der er blandt andet mulighed for økonomiske sanktioner. De muligheder findes ikke i den nuværende persondatalovgivning.

6.5.2 > PROJEKT I TO FASER

Set i lyset af de øgede krav til beskyttelse af persondata har RUC allerede nu forbedret processer og forretningsgange med henblik på den nye forordning. Vi har nedsat en tværorganisatorisk arbejdsgruppe på universitetet.

Den har som formål at udarbejde et projektinitieringsdokument (PID) om implementeringen af forordningen.

Arbejdet er delt i to faser. I første fase nedsætter vi en projektgruppe, der består af repræsentanter fra institutterne, informationssikkerhedskonsulenten og en juridisk kompetence, som tilknyttes ad hoc. Projektgruppen har til opgave at analysere, hvordan vi er dækket ind i dag i forhold til overholdelse af den nuværende persondatalov. Desuden skal den identificere, hvilke nye tiltag der bliver introduceret i forbindelse med forordningen.

Anden fase i projektet bliver at videreføre arbejdet fra analysefasen, så vi sikrer, at implementeringen af handlingsplanen, der er et resultat af fase et, foretages i relevante funktioner på RUC.

6.5.3 > VÆSENTLIGE ELEMENTER I FORORDNINGEN

Arbejdsgruppen har til hovedformål at sikre sammenhæng mellem den eksisterende persondatalov, EU-forordningen og universitetets forpligtelser. Den skal altså sikre transformationen fra "as is"-situationen til en kommende "to be"-situation gennem udarbejdelsen af en GAP-analyse.

Arbejdsgruppen har især fokus på følgende elementer fra forordningen:

1. Krav til procedurer ved sletning af registreringer inklusive hos tredjepart (fysisk og i databaser).
2. Krav om udtrykkeligt samtykke ved databehandling (f.eks. studieadministration, ESDH og det digitale eksamenssystem).
3. Som offentlig institution skal vi have en Databeskyttelsesansvarlig (DPO), en ny stillingsbetegnelse hos os og sikkert også hos andre.
4. Krav om dokumentation for enhver behandling af persondata.
5. Krav om kontrol af beskyttelsesmekanismer (hvordan kontrollerer vi i dag?).
6. Dokumentationskrav i relation til offentlige myndigheder (skal kunne tåle "revision" fra Datatilsynet).
7. Krav om risikovurderinger i forhold til databehandling af persondata.
8. Krav om underretning til de involverede, hvis persondata kompromitteres (kendes fra USA).

I første omgang har arbejdsgruppen til opgave at skabe fælles forståelse for de begreber, der er knyttet til arbejdet med og brugen af persondata på tværs af organisationen. Desuden skal den sikre, at der udarbejdes et klassifikationssystem. Det definerer referencer, der entydigt, sikkert og effektivt forbinder informationer om personer, både ansatte og studerende, tillige med forskerdata og i forholdet til universitetets forretningsgange.

6.5.4 > TVÆRORGANISATORISK PROJEKT

Arbejdet med forordningen oprettes som et tværorganisatorisk projekt. I første omgang nedsætter vi en arbejdsgruppe, der udelukkende analyserer nødvendige forudsætninger og identificere organisatoriske krav og behov. Den danner rammerne for det videre arbejde med implementeringen af forordningen på RUC.

En fælles forankring på tværs af organisatoriske enheder medfører en fælles koordinering i arbejdet på tværs af institutter og administrationen. Og den smidiggør processen med den endelige implementering af forordningen på universitetet.

På Roskilde Universitet har informationssikkerhedsfunktionen påtaget sig rollen som ansvarlig for implementeringen af forordningen. Informationssikkerhedsfunktionen etablerer og driver også det nødvendige klassifikationssystem i samarbejde med øvrige interessenter.

I forbindelse med konkrete implementeringsopgaver eller ved bedømmelse af forslag til klassifikationssystemet vil vi nedsætte projektgrupper og eventuelle underudvalg med fagspecifik viden. De operative opgaver varetager institutterne og fællesadministrationen gennem arbejdsgrupper og/eller eksisterende udvalg.

> ***Med forordningen falder den danske persondatalov helt bort.***

6.5.5 > DET BETYDER FORORDNINGEN FOR RUC

Arbejdet med implementering af forordningen kommer til at betyde muligheder i to retninger:

1. Vi får mulighed for at implementere grundlaget for et solidt fundament til beskyttelse af persondata.

2. Vi får internt drøftet og italesat arbejdet med personhenførbare data i en kontekst, som afspejler vores organisation og virke.

Ud over mulighederne findes der også konsekvenser for universitetet, både i form af lovformelighed (compliance) og økonomiske og tekniske krav, som vi selvfølgelig ikke kan negligere. De compliancemæssige konsekvenser indebærer både økonomiske udfordringer og udfordrer vores daglige processer, eksempelvis med kravet om det udtrykkelige samtykke.

> ***Ud over de negative konsekvenser ser vi lige så meget frem til de positive, hvor incitamentet til sikker håndtering af persondata bliver skærpet.***

På den økonomiske side forventer vi øgede omkostninger til ansættelsen af en Data Protection Officer (DPO) samt kravet om information til de involverede, hvis data kompromitteres. På den tekniske side forventer vi, at sletninger og registreringer kommer til at blive en udfordring. Ikke så meget i databaser, men mere i forhold til de sikkerhedskopier som løbende er foretaget.

Et andet interessant område, der kommer yderligere fokus på med den kommende forordning, er Privacy Impact Assessment (PIA). En PIA vurderer risikoen for de studerende, ansatte og forskningsobjekters rettigheder, hvis deres persondata bliver kompromitteret. På universitetet anvender vi eksempelvis en skabelon til vores vurderinger, som Dansk Industri (DI) har udarbejdet[24].

Der er ingen tvivl om, at forordningen kommer til at betyde, at der skal anvendes flere administrative ressourcer. Det gælder i forhold til kontroller, men så sandelig også i forhold til de administrative processer omkring sikring af compliance.

Ud over de negative konsekvenser ser vi lige så meget frem til de positive, hvor incitamentet til sikker håndtering af persondata bliver skærpet. Det gælder forholdet til konkrete og tidssvarende krav til de tekniske og administrative processer, men ikke mindst i forhold de sanktionsmuligheder som findes i form af anselige bødestraffe for ikke at overholde forordningen.

[24] DI's skabelon for Privacy Impact Assessment, http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Trusler%20og%20loesninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

7. Klummer af Shehzad Ahmad

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

7.1 > DEN VÆSENTLIGSTE HINDRING FOR IT-SIKKERHED: HVERDAGENS TRAVLHED

Har du kigget logfilerne fra firewallen igennem? Næppe. Men du gør det, så snart du lige har fået printeren på første sal til at fungere igen og oprettet den nye bruger i ERP-systemet. Ikke?

Hverdagen for mange it-folk består af en nærmest ubrudt række af afbrydelser i det, de egentlig skulle beskæftige sig med. Jeg tænker på brandslukning af typen "Min mail virker ikke" eller "Vi skal bruge en projektor i det nye mødelokale." Den slags opgaver tager tid fra dem, vi burde fokusere på.

7.1.1 > DET ENKLE DIAGRAM

Jeg har berørt emnet kort i tidligere klummer. Men for nylig faldt jeg over et dia-gram, der illustrerer problemet meget enkelt og sigende. Diagrammet er udarbejdet af en amerikansk analytiker, Wendy Nather fra 451 Research[25]. Hun har taget ud-gangspunkt i den gode, gamle Maslows behovspyramide.

Titlen er ganske rammende: "The hierarchy of IT needs. Or, why you can't get your management team to take security seriously." Ligesom Maslow begynder pyramiden nedefra med de mest basale behov. Hos Maslow er det menneskets behov for mad, varme og et sted at sove.

Wendy Nathers pyramide handler om kravene til it-funktionen. Pyramiden er opbygget ud fra, hvilke trusler it-folk tager mest alvorligt.

Derfor lyder det nederste krav ganske enkelt: "Få det til at køre." Den største trussel for en it-ansat er, at systemet ikke virker. Sikkerheden kan vi altid kigge på senere – den er alligevel irrelevant, hvis systemet ikke er i luften.

7.1.2 > HOLD DET KØRENDE

Næste trin på pyramiden går ud på at sikre, at systemet bliver ved med at køre. Det må ikke løbe tør for diskplads. En ændring må ikke sætte det ud af drift. Strømmen må ikke blive afbrudt. Den kender enhver, der har installeret de seneste rettelser fra Microsoft for derefter at se blue screen of death på brugernes skærme.

På pyramidens tredje trin skal vi undgå, at den nye it-løsning smadrer noget i resten af vores it-system.

Det fjerde trin handler om at ændre på vores nye løsning uden at ødelægge den.

Og sådan fortsætter det op ad pyramiden: Trin efter trin med de trusler som vi it-folk prioriterer i hverdagen. Går det galt på et af trinene, rutsjer vi hele vejen ned til bunden og må begynde forfra med at få det til virke.

7.1.3 > TRUSLEN FRA REVISOREN

Jeg er særlig glad for Wendy Nathers næstøverste trin: Beskyt mod auditører og sikkerhedsrevisorer. Det lyder måske kættersk, men i mange organisationer vejer hensynet til at bestå en auditering tungere end ønsket om at beskytte mod rigtige angreb.

At beskytte mod angribere er placeret allerøverst på Wendy Nathers pyramide. En ganske lille trekant afslutter hendes pyramide, hvor alle de øvrige hensyn fylder langt mere. Trist, men sandt.

I dagligdagen har de færreste it-organisationer ressourcer til at arbejde aktivt med informationssikkerheden.

7.1.4 > NEDSKRIV PROCEDURER

Som jeg før har skrevet, mangler sikkerhedsarbejdet i de fleste organisationer tre ting: Tid, penge og ressourcer i form af arbejdskraft. Det får vi kun, hvis ledelsen erkender behovet for informationssikkerhed.

Medarbejdere prioriterer de opgaver, deres ledelse giver dem besked på at prioritere – eller de opgaver, de selv finder mest presserende. Hvis medarbejderen sidder med næsen nede i logfilerne, og en frustreret bruger kommer ind på kontoret og beder om hjælp til sin pc, er det meget forståeligt, at medarbejderen vælger at hjælpe sin kollega først.

Derfor skal der være styr på forretningsgangene. Aftalte og nedskrevne processer sikrer, at sikkerhedsmedarbejderen ikke bliver afbrudt med brandslukningsopgaver.

[25] Wendy Nather: The hierarchy of IT needs, http://informationsecurity.451research.com/?p=5679

En central servicedesk er første skridt på vejen. Her indsamler it-afdelingen fejlmeldinger og ønsker fra brugerne, så de kan prioriteres og fordeles til medarbejderne. Ønsker du flere råd om effektivisering af it-arbejdet, kan jeg varmt anbefale ITIL (Information Technology Infrastructure Library).

Hvis it-afdelingerne får bedre styr på dagligdagen, bliver det muligt at rykke sikkerheden længere ned i it-behovspyramiden – og det vil være til gavn for os alle.

7.2 > HELT AFGØRENDE: SÅDAN FÅR DU SIKKERHEDEN SKREVET IND I KONTRAKTEN

For nylig havde jeg den fornøjelse at holde indlæg på den årlige DeiC-konference. DeIC (Danish e-Infrastructure Cooperation) er en virtuel organisation, der blandt an-det omfatter forskningsnettet og DKCERT.

Mit indlæg handlede om aktuelle trends inden for sikkerhed. Der var især ét emne, som vakte interesse: Sikkerhed og SLA'er (service level agreement). Jeg tror, aktuel-le sager som Se og Hør-skandalen har øget opmærksomheden om outsourcing som en sikkerhedsudfordring – det skrev jeg også om i en tidligere klumme.

Nets havde outsourcet driften af dankortsystemet til IBM. En ansat hos IBM mis-brugte øjensynlig sin adgang til systemet. Hvem har nu ansvaret? Er det Nets, der står for dankortsystemet, eller IBM, som driften er outsourcet til? Det spørgsmål kan vi kun besvare, hvis vi kender kontrakten mellem parterne.

7.2.1 > LEVERANDØRENS SIKKERHED ER DIN SIKKERHED

Spørgsmålet om ansvaret for informationssikkerheden er vigtigt at overveje for alle, der lægger dele af deres it ud til eksterne leverandører. Hvordan er din virksomhed stillet, hvis din leverandør ikke har styr på sikkerheden?

Mange virksomheder placerer deres websted på et webhotel. Hvad betyder det for jer, hvis webhotellet bliver hacket eller sat ud af drift? Hvis I tager imod ordrer via jeres webshop, kan det hurtigt blive dyrt at stå uden websted. Hvad siger kontrakten med webhotellet om den situation?

Hvis den er som de fleste, fraskriver udbyderen sig ethvert ansvar for skader, der skyldes hackerangreb og lignende. Jeg vil råde dig til at kigge dine kontrakter efter i sømmene med fokus på sikkerheden.

Som regel vil spørgsmål om sikkerhed blive placeret i en SLA. SLA'en er det dokument, der definerer kontraktens indhold i praksis.

SLA'en konkretiserer jeres aftale: Hvad du som kunde forventer at modtage. Hvad leverandøren lover at levere. Hvordan I måler det, der leveres. Hvad leverandøren skal betale i bod for overskridelser.

7.2.2 > TJEK SIKKERHEDSPOLITIK

Helt overordnet skal I se på leverandørens sikkerhedspolitik og tjekke, at den stemmer overens med jeres ønsker. Derudover skal en SLA med fokus på sikkerhed for eksempel give svar på disse spørgsmål:

1. Hvordan beskytter leverandøren de systemer, kunden bruger, mod virusangreb?
2. Hvordan sikrer leverandøren data mod at komme i de forkerte hænder?
3. Hvilke garantier for oppetid giver leverandøren?
4. Hvordan beskytter leverandøren mod ansatte, der misbruger adgangen til jeres data?
5. Hvor hurtigt informerer leverandøren kunden om brud på sikkerheden?

Med cloud-tjenester, der leveres som SaaS (Software as a Service), placerer du dine data i leverandørens system.

Vigtige data om din virksomheds kunder, deres kontaktinformationer og indkøbshistorik ligger i den slags systemer.

Her skal kontrakten tage højde for, hvordan du som kunde kan få fat i de data. Hvordan tager I sikkerhedskopi? Kan I få dataene udleveret? Og i hvilket format?

Når jeres virksomhed behandler persondata, skal den overholde lovgivningens krav. For eksempel må personfølsomme data som regel kun opbevares inden for EU's grænser.

7.2.3 > VÆR FORSIGTIG

Her skal I være forsigtige: Jeg har været ude for, at en cloud-udbyder havde sine servere i Europa. Men det viste sig, at sikkerhedskopien lå i USA.

Mange it-firmaer har lagt deres support ud i lande med billig arbejdskraft. Hvis supporteren i Manila kan slå op i data om dine kunder, er det også et tegn på, at kravene ikke bliver overholdt.

7.2.4 > STØT JER TIL STANDARDER

Det kan være en god ide at koble sig på eksisterende standarder. For eksempel kan kunden i kontrakten kræve dokumentation for, at leverandøren overholder kravene i ISO 27001. Det garanterer, at leverandøren har etableret et system til at holde styr på sikkerheden.

Men det er ikke nok, at jeres leverandør kan vise et ISO 27001-stempel. I skal gennemgå det såkaldte SoA-dokument (Statement of Applicability). Det fortæller, hvordan certificeringen er afgrænset.

Det kan være, at de dele af leverandørens system, der er certificeret, er nogle helt andre end dem, I skal bruge. Spørg også ind til, hvordan leverandøren konkret sikrer jeres data:

Hvordan er deres firewall-setup? Bruger de et IPS (Intrusion Prevention System)? Hvordan overvåger de løbende systemet? Hvilke procedurer har de for logfiler, og hvor tit gennemgår de dem?

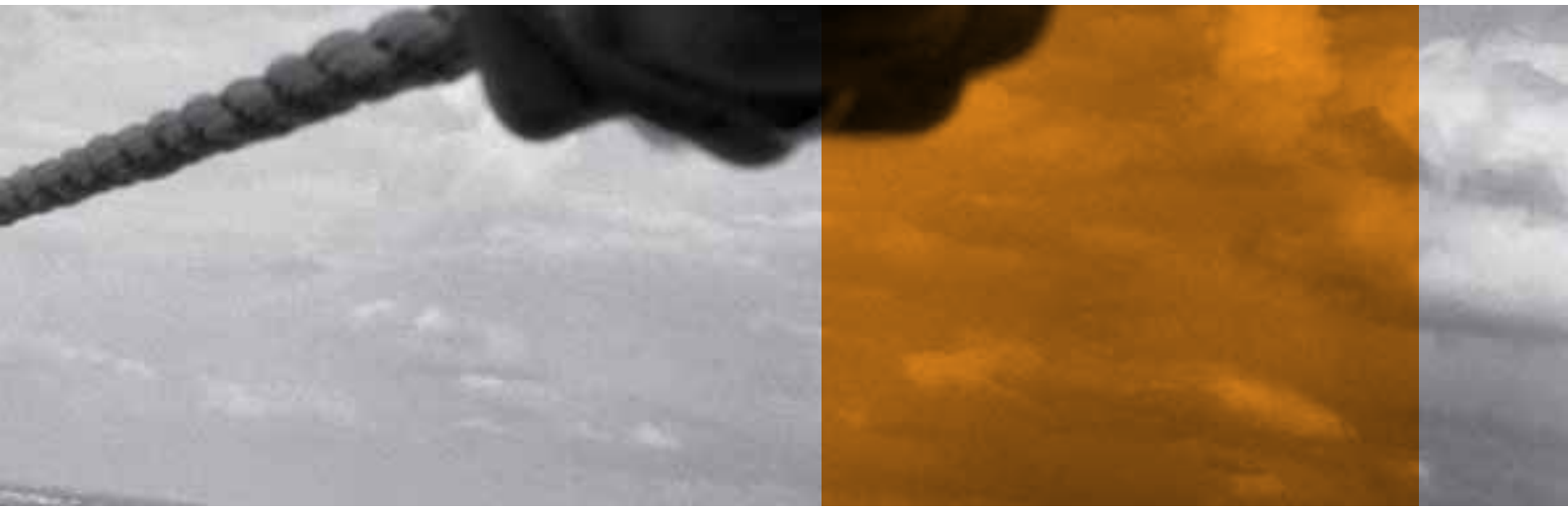
Sårbarheder i it-systemer er stadig et ømt punkt i mange organisationer. Når et system ikke er opdateret, er det et oplagt mål for hackerangreb.

Så I skal vide, hvordan leverandøren holder styr på softwareopdateringer. Hvor tit installerer de sikkerhedsopdateringer? Hvor tit scanner de deres systemer for at finde dem, der mangler en opdatering?

7.2.5 > FØLG OP LØBENDE

Endelig vil jeg understrege, at SLA'en i sig selv ikke udgør nogen garanti for sikkerheden. Sikkerhed er en løbende proces. Derfor skal I jævnligt følge op på, at målene i SLA'en bliver overholdt.

I skal også vedligeholde og opdatere SLA'en løbende. Men pas på, at den ikke ender som et hoveddokument med en masse bilag, så den bliver helt uoverskuelig.



Så er det bedre med nogle års mellemrum at overveje, om hele SLA'en skal opdateres, så indholdet fra bilagene skrives ind i den.

En ekstern sikkerhedsrevision er også en god ide. I kan fx skrive ind i kontrakten, at en uafhængig enhed auditerer sikkerheden med faste intervaller.

7.3 > PAS PÅ MEDARBEJDERNE: DERFOR ER VIRKSOMHEDSKULTUREN AFGØRENDE FOR SIKKERHEDEN

En medarbejder er på vej ud fra virksomheden, da han kommer i tanke om, at han har glemt at udskrive dagsordenen til mødet i morgen tidlig. Og nu er computeren lukket ned.

Heldigvis har kollegaen i nabokontoret for vane aldrig at slukke sin pc. Så medarbejderen låner pc'en, udskriver dagsordenen og tager hjem med ro i sindet.

Virksomhedens sikkerhedsansvarlige kan derimod ikke have ro i sindet. Medarbejderens handling udgør ingen direkte sikkerhedsrisiko. Men den påpeger to alvorlige problemer ved kulturen i virksomheden.

For det første ser medarbejderen ingen problemer ved lige at låne sin kollegas pc.

7.3.1 > GLEMMER AT LÅSE PC

Han tænker ikke over, at virksomheden muligvis logger brugen af netværket – og at loggen nu vil vise, at en ansat har udskrevet en dagsorden til et møde, han ikke er indkaldt til.

For det andet glemmer kollegaen i nabokontoret at låse sin pc. Han bør logge ud eller som minimum slå pauseskærmen til, så uvedkommende ikke kan bruge pc'en, når han er væk fra den.

Foruden glemsomme kolleger kan også rengøringspersonale eller nattevagter udnytte den slags pc'er med fri adgang.

7.3.2 > TEKNOLOGI LØSER IKKE ALT

Kulturen i en virksomhed er efter min mening et afgørende element i dens informationssikkerhed. I nogle tilfælde kan den vise sig at være altafgørende. Årsagen er, at teknologi ikke løser alt.

Vi kan købe nok så mange firewalls, antimalwareløsninger og SIEM-systemer. Men hvis medarbejderne ikke har sikkerhedskulturen inde under huden, kan investeringerne være forgæves.

Derfor skal du som leder være opmærksom på, hvilken sikkerhedskultur din organisation har[26].

7.3.3 > ANSÆT UD FRA SIKKERHED

Ledelsen kan sætte ind to steder, når det handler om at opbygge og vedligeholde en sikkerhedskultur: Ansættelser og i hverdagen.

Ansættelsen er den vigtigste. Hvis du ansætter folk med den rette indstilling til informationssikkerhed, kan du undgå alvorlige problemer senere.

Sørg for at få en straffeattest fra ansøgeren. Hvis medarbejderen skal arbejde med særligt følsomme data, skal vedkommende også sikkerhedsgodkendes. Hverken en ren straffeattest eller en sikkerhedsgodkendelse er imidlertid garanti for, at du har fundet den rette medarbejder.

Spørg ind til, hvordan vedkommende vil håndtere konkrete opgaver. Bemærk, om ansøgeren naturligt tager sikkerhed med i sine svar.

Du skal også informere om jeres sikkerhedspolitik og personalepolitik, og hvad de konkret betyder for, hvordan medarbejderen skal opføre sig på arbejdspladsen.

7.3.4 > LØBENDE KONTROL

Efter ansættelsen skal den viden suppleres. Jeg anbefaler et tæt samarbejde med jeres HR-afdeling. Tag en snak med dem om, hvordan I tænker sikkerheden ind i den samlede introduktion af nye medarbejdere.

Foruden HR bør I også inddrage kommunikationsafdelingen. De kan sikre, at informationerne bliver givet i et sprog, medarbejderne kan forstå.

Sikkerhed er en løbende proces. Jeg kender et firma, der en gang om året kræver at se alle medarbejderes straffeattest. Det kan være en metode til at opdage, om nogen er på vej ud i noget snavs.

[26] Glenda Rotvold: How to Create a Security Culture in Your Organization, http://content.arma.org/IMM/Nov-Dec2008/How_to_Create_a_Security_Culture.aspx

Virksomhedskulturen begynder hos ledelsen. Hvis ledelsen giver udtryk for, at det der med sikkerhed mere er en irritation i hverdagen end noget, der er nødvendigt, så forplanter den holdning sig hurtigt ned i organisationen.

Det gælder ikke kun topledelsen, men også mellemlederne. Hvis mellemlederne ikke respekterer sikkerheden, bør virksomheden ikke have plads til dem.

Så læg mærke til, hvordan du selv og dine kolleger i ledelsen taler om sikkerhed – og hvordan I agerer i praksis. Skriv også kulturen ind i jeres sikkerhedspolitik. Det kan for eksempel se sådan ud:

"Alle medarbejdere har ansvar for at bidrage til at beskytte virksomhedens informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. De skal derfor løbende informeres og undervises i informationssikkerhed."

Kravet om undervisning skal også gælde for mellemledere og den øvrige ledelse.

7.3.5 > FARVEL TIL DEN PRIVATE ENHED

Vores arbejds- og privatliv smelter mere og mere sammen. Det skyldes ikke mindst teknologien: Med smartphones er vi også på arbejds-mailen kl. 22. Og telefonen fra jobbet indeholder billeder af vores børn.

Den sammenblanding af private data og arbejdsdata udgør en sikkerhedsrisiko. For eksempel kan en medarbejder bruge Dropbox til at få adgang til dokumenter fra sin tablet. Men når tablet-computeren bliver stjålet, har tyven fri adgang til virksomhedens data.

De unge er digitale indfødte. De er vokset op med internet, smartphones og cloud som en naturlig del af deres digitale liv. De forventer, at data er tilgængelige, uanset hvor og hvornår de har brug for dem.

Digitale indfødtes engagement og viden er en stor gave til virksomheden. Men de udgør en alvorlig udfordring for sikkerhedskulturen. Hvordan vil du håndtere den?

8. Fremtidens trusler og trends

8.1 > TRUSLER MOD INFORMATIONSSIKKERHEDEN I 2015

8.1.1. ANGREB FRA STATER OG EFTERRETNINGSTJENESTER

Risikoen for angreb fra nationalstater og deres efterretningstjenester har fået langt mere opmærksomhed i offentligheden efter Edward Snowdens afsløringer. Den tidligere medarbejder i NSA (National Security Agency) har løbende lækket materiale fra tjenesten, der afdækker en omfattende aktivitet med aflytning og tapning af dataforbindelser.

For eksempel kom det frem i 2014, at NSA og Storbritanniens GCHQ (Government Communications Headquarters) tilsyneladende stod bag et hackerangreb på det delvist statsejede belgiske teleselskab Belgacom i 2013. Til angrebet blev benyttet et avanceret værktøj ved navn Regin. Samme program blev brugt i et angreb mod EU-kommissionen i foråret 2011[27].

DKCERT mener:

Danske organisationer skal i deres risikovurdering medtage muligheden for angreb fra nationalstater og spionageorganisationer på lige fod med traditionel it-kriminalitet.

8.1.2 > AFPRESNING OG RANSOMWARE

Ransomware er en trussel i vækst. Det handler om software, der spærrer for brugerens adgang til programmer og data. Bagmændene kræver løsepenge for at give brugeren adgang igen.

En undersøgelse som Danmarks Statistik foretog for DKCERT og Digitaliseringsstyrelsen i efteråret, viste, at otte procent af deltagerne havde været ramt af ransomware [28].

[27] Wired: Researchers Uncover Government Spy Tool Used to Hack Telecoms and Belgian Cryptographer, http://www.wired.com/2014/11/mysteries-of-the-malware-regin/

[28] Digitaliseringsstyrelsen/DKCERT: Borgernes informationssikkerhed 2014, https://www.cert.dk/borgersikkerhed2014/Borgernes_informationssikkerhed_2014.pdf

Kun to procent af de ramte endte med at betale løsesummen. Det skyldes blandt andet, at mange formåede at få data tilbage uden hjælp fra bagmændene.

Sikkerhedsfirmaerne beretter imidlertid, at der er vækst i ransomware baseret på kryptering. Disse trusler krypterer offerets data. Så kan man kun få data tilbage, hvis man får den nøgle, som data er krypteret med.

DKCERT mener:

Væksten i ransomware med kryptering betyder, at ofrene får langt dårligere chancer for at gendanne data uden at have kontakt med bagmændene. Derfor er det endnu vigtigere, at organisationer lægger en backupstrategi og løbende tester, at den fungerer.

8.1.3 > TRUSLEN INDEFRA

2014 gjorde en velkendt trussel aktuel på ny: Den betroede medarbejder, der misbruger arbejdspladsens tillid til at få fat i fortrolig information. Det ser ud til at være sket i Se og Hør-skandalen, hvor ugebladet brugte oplysninger om kendte personers korttransaktioner til at opspore dem på rejser i udlandet. Oplysningerne kom øjensynlig fra en medarbejder i den virksomhed, der behandlede betalingskorttransaktionerne.

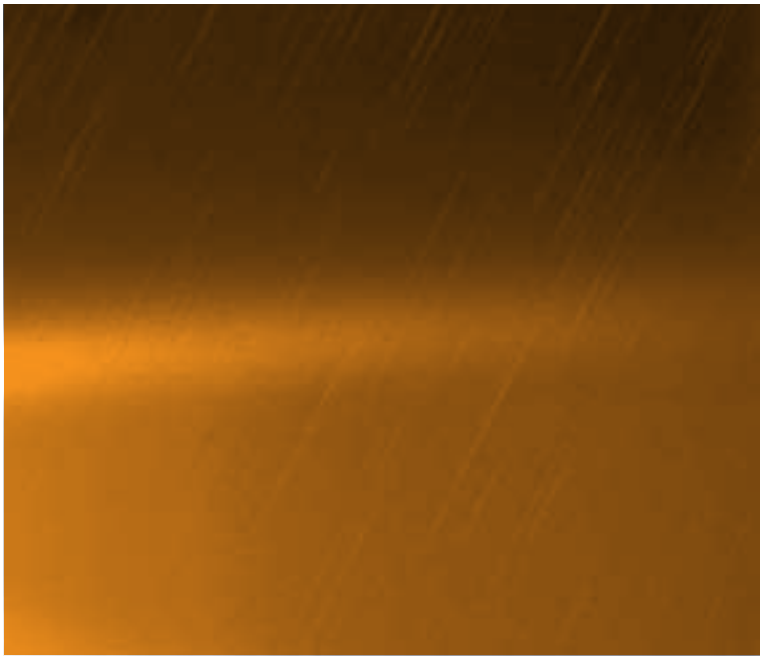
Organisationer kan sætte ind på tre områder for at mindske risikoen fra betroede medarbejdere: Information, uddannelse og awareness-kampagner. Endvidere kan de gøre noget for at sikre, at dem de ansætter, udgør en minimal risiko. Organisationen bør også foretage en vis kontrol og overvågning for at fange eventuelt misbrug hurtigt.

DKCERT mener:

Stadig flere værdifulde oplysninger findes i digital form. Det gør det lettere at stjæle dem end i gamle dage, hvor man skulle håndtere fysiske dokumenter. Derfor er der brug for beskyttelse mod internt misbrug. Et vigtigt middel er rollebaseret adgangskontrol, der begrænser, hvilke data forskellige typer medarbejdere har adgang til.

8.1.4 > KULTURSAMMENSTØD

Edward Snowdens afsløringer har øget opmærksomheden på truslen mod vores digitale privatliv. De har været med til at skabe en bevægelse, der arbejder for øget sikkerhed via kryptering og anonymisering. Den bevægelse



er både i opposition til de officielle sikkerhedstjenester og til den digitale underverden: De vil hverken aflyttes af efterretningstjenesten eller af den russiske mafia.

Derved opstår der en kulturkløft, hvor bevægelsen ikke opfatter autoriteterne inden for it-sikkerhed som garanter for fortroligheden og beskyttelsen af persondata. For eksempel kan de være modstandere af NemID, fordi krypteringsnøglerne opbevares centralt. I stedet foretrækker de krypteringsløsninger, hvor de selv kontrollerer nøglerne.

DKCERT mener:

Kulturkløften mellem de traditionelle, etablerede sikkerheds-organisationer og de nye bevægelser kan føre til dårligere sikkerhed, fordi vi ikke udnytter hinandens ressourcer. Det er nødvendigt, at grupperne mødes og finder frem til de områder, hvor de har fælles interesser.

For eksempel kan udbydere af webtjenester udlove dusører til dem, der opdager sikkerhedshuller i deres tjenester, i stedet for at true dem med sagsanlæg for brud på tjenestens regler for brug.

Politiet kan også overveje at ansætte folk med "hackerbaggrund" – både på grund af deres tekniske viden og fordi de kender selve hackerkulturen.

8.1.5 > INTERNET OF THINGS UDFORDRER SIKKERHEDEN

Igen i år venter vi problemer med sikkerheden på alt det udstyr på internettet, der ikke er traditionelle computere – det såkaldte Internet of Things.

Vi har hidtil især set udfordringer, når det gælder routere i private hjem. De er ofte udstyret med gammel firmware med kendte sårbarheder. De færreste private brugere er opmærksomme på, at deres trådløse router kan have brug for ny software. Og skulle de vide det, er de ikke altid i stand til at gennemføre opdateringen.

I takt med at stadig mere udstyr kommer på nettet, vokser den sikkerhedsmæssige udfordring. Det gælder for eksempel såkaldte wearables – tøj og smykker med indbygget internetadgang. I 2014 var det især motionsarmbånd og armbåndsure, ikke mindst drevet af den megen omtale af Apple Watch. Den sikkerhedsmæssige udfordring gælder også biler, der udstyres med flere avancerede funktioner, som ligeledes kommunikerer over internettet.

DKCERT mener:

Da de første computere kom på world wide web, var sikkerheden ikke i fokus. I stedet koncentrerede udviklerne sig om at udnytte alle de nye muligheder. Hvis det samme sker for internet of things, venter der store sikkerhedsproblemer forude.

8.2 > SIKKERHEDSTRENDS I 2015

8.2.1 > NATIONAL STRATEGI FOR CYBER- OG INFORMATIONSSIKKERHED

I slutningen af 2014 offentliggjorde regeringen en samlet strategi for cyber- og informationssikkerhed[29]. Den skal professionalisere statens arbejde med sikkerhed og øge samfundets robusthed over for angreb.

Strategien indeholder 27 initiativer fordelt på seks indsatsområder:

1. Professionalisering og styrket it-tilsyn.
2. Klare krav til leverandører.
3. Styrket cybersikkerhed og mere viden på området.
4. Robust infrastruktur i energisektoren og telesektoren.
5. Danmark som stærk international medspiller.
6. Stærk efterforskning og klar information til borgere, virksomheder og myndigheder.

Strategien skal revideres allerede i 2016. Her vil der komme nye tiltag.

[29] Digitaliseringsstyrelsen: Strategi for cyber- og informationssikkerhed, http://www.digst.dk/Arkitektur-og-standarder/Cyber-og-informationssikkerhed

8.2.2 > EU STILLER KRAV TIL DATABESKYTTELSEN

EU's forhandlinger om den kommende persondataforordning ventes afsluttet sidst i 2015[30]. Forordningen kommer til at afløse den nuværende persondatalov.

Forordningen medfører, at nogle virksomheder skal udpege en såkaldt "data protection officer." De skal også indføre retningslinjer og foranstaltninger, der sikrer forsvarlig behandling af personoplysninger.

Skulle det gå galt, så data kommer i de forkerte hænder, kan konsekvensen blive en bøde på op til 100 millioner euro eller fem procent af virksomhedens omsætning.

DKCERT mener:

Det er på tide for danske virksomheder, myndigheder og organisationer at forberede sig på at leve op til kravene i den kommende databeskyttelsesforordning. Her kan det være en god ide at starte med at indføre ISO 27001, den internationale standard for håndtering af informationssikkerhed.

8.2.3 > WINDOWS 7 – NEDTÆLLINGEN ER BEGYNDT

Den 13. januar 2015 standsede Microsoft mainstream-support til styresystemet Windows 7. Det betyder, at der ikke kommer nye funktioner til systemet. Derimod vil Microsoft fortsat levere sikkerhedsopdateringer frem til den 14. januar 2020. Samme dato gælder for Windows Server 2008[31].

Danske virksomheder og organisationer har dermed knap fem år til at planlægge, hvordan de vil skifte over til en afløser for Windows 7 og Windows Server 2008.

DKCERT mener:

Der er stadig virksomheder, der bruger Windows XP, som der ikke er kommet sikkerhedsopdateringer til siden maj 2014. Det udgør en sikkerhedsrisiko. For at undgå en gentagelse, når Windows 7 mister support, bør virksomheder og organisationer allerede nu begynde at forberede sig på overgangen til deres næste styresystem.

[30] Lett: Opdatering – EU's persondataforordning, http://www.lett.dk/viden/faglige-nyheder/nyt-fra-persondataret-oktober-2014/opdatering-%E2%80%93-eu%E2%80%99s-persondataforordning

[31] Microsoft: Windows lifecycle fact sheet, http://windows.microsoft.com/en-us/windows/lifecycle

9. 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 universiteter og andre højere læreanstalter.

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.

9.1 > ANBEFALINGER TIL IT-ANSVARLIGE PÅ UNIVERSITETER

DKCERT anbefaler, at universitetets it-ansvarlige udarbejder en risikovurdering som grundlag for alle it-sikkerhedstiltag. En risikovurdering kan med fordel udarbejdes ud fra anbefalingerne i ISO 27001.

1 Hold brugernes enheder opdateret. Det gælder også, når de anvender deres egne enheder til arbejds- eller studieformål (BYOD, Bring Your Own Device).

2 Forlang ledelsens aktive involvering i informationssikkerhedsarbejdet.

3 Ajourfør og vedligehold informationssikkerhedspolitikken.

4 Begrænsadgangen til kritiske data og beskyt dem eventuelt med kryptering.

5 Indfør tiltag mod misbrug via gæstenetværk.

6 Hav øget fokus på universitetets webapplikationer.

7 Anvend single sign-on suppleret med to-faktor-autentifikation.

8 Tænk sikkerhed ind i relationen til leverandører og samarbejdspartnere.

9 Effektiviser patch management – eventuelt ud fra principperne i ITIL.

10 Optimer generelt processer og procedurer.

9.2 > ANBEFALINGER TIL LEDELSEN PÅ UNIVERSITETER

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 universitetets ledelse afsætter de fornødne ressourcer til at løfte opgaven.

1 Inkluder informationssikkerhed i den langsigtede strategiske planlægning.

2 Tænk 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 informationssikkerheds-politikken og aktuelle problemer.

5 Etabler et beredskab og udarbejd en beredskabsplan for sikkerhedshændelser.

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 universiteter om informationssikkerhed.

10 Sørg for, at en beredskabsplan for kritiske hændelser bliver udviklet og løbende vedligeholdt.

11 Afsæt tid, penge og personale til håndtering af informationssikkerhed.

10. Ordliste

Anonymous-bevægelsen
En løst defineret internetbaseret gruppe, som i 2003 opstod via hjemmesiden 4chan.org. Gruppen benytter sig blandt andet af DDoS-angreb i deres kamp for ytringsfrihed og mod, hvad de anser som censur og misbrug af nettet. Er særlig kendt for sin modstand mod Scientology Kirken og for sin støtte til Wikileaks og The Pirate Bay.

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

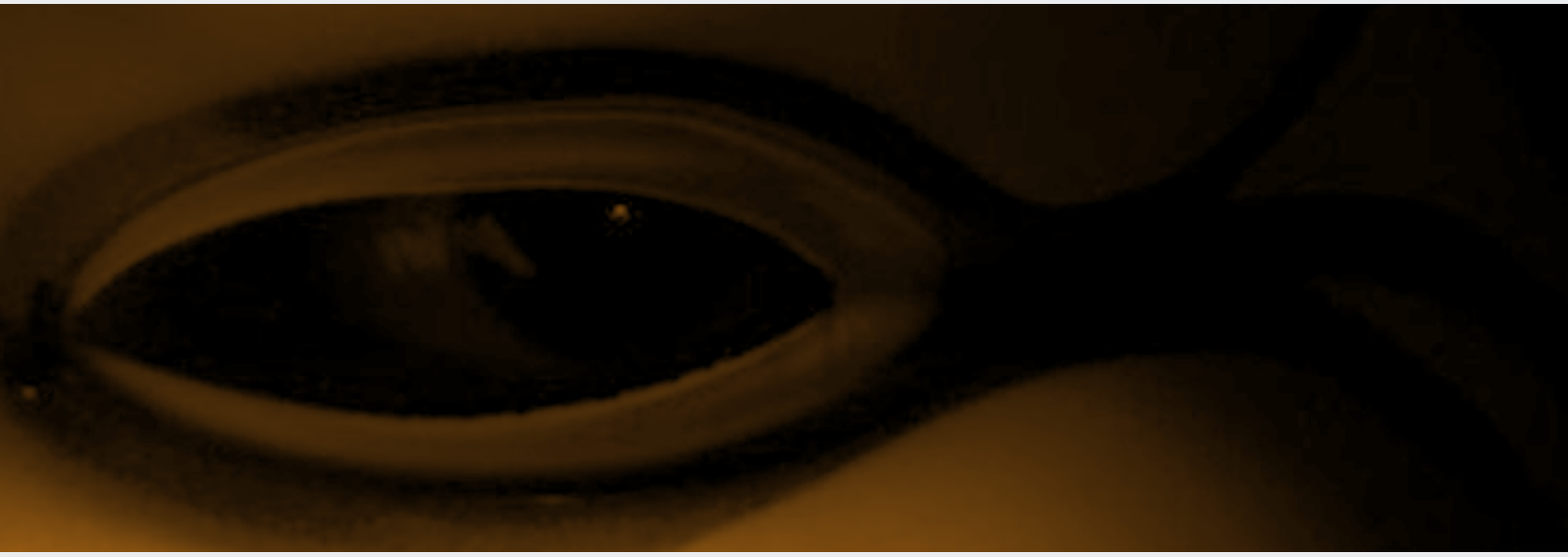
BYOD
Bring Your Own Device. Et koncept hvor organisationer lader de ansatte selv stå for indkøb og drift af deres eget udstyr. For eksempel kan de bruge deres egen smartphone til job-relaterede formål.

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.

Compliance
Overensstemmelse eller efterlevelse af gældende regler. I it-sikkerhedssammenhæng beskriver compliance organisationernes evne til at efterleve krav til informationssikkerhed efter gældende lovkrav eller godkendte standarder som for eksempel ISO 27001 eller lignende.

Data Leak Prevention, DLP
System, der på grundlag af centralt definerede politikker identificerer, overvåger og beskytter data, der er lagret, i bevægelse eller i brug, mod uautoriseret brug og tab. Beskyttelsen sker ved dybdegående analyse af data og et centralt styret management framework. DLP beskytter også organisationer mod social engineering og intern misbrug af data.

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 ved en sammenlægning af Forskningsnettet og Dansk Center for Scientific Computing (DCSC). DeIC er etableret som et resultat af Infrastruktur Roadmapprocessen i regi af Styrelsen for Forskning og Innovation, og gennem en national samarbejdsaftale om koordinering og etablering af fælles e-Infrastruktur til e-Science for alle forskningsområder. Aftalen blev indgået mellem Styrelsen for Forskning og Innovation og alle universiteterne i efteråret 2011. DeIC skal sikre den bedst mulige nationale ressourceudnyttelse på e-Infrastrukturområdet.

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 Forsvarsministeriet.

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 27001/27002
En normativ standard for it-sikkerhed. I familien indgår ud over de to normative standarder ISO 27001/2 og ISO 27006 en række standarder med retningslinjer for, hvordan en organisation kan implementere og overholde de normative standarder.

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 mobil-telefon som sms, et fingeraftryk, der angives via en fingeraftrykslæser, en kode fra et papirkort eller lignende.

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

Virus
Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres virussen, og den inficerer andre programfiler. Oprindelig kunne kun egentlige programmer indeholde virus, men dokumenter med makroer kan også gøre det.

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

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

11. Figurliste

12. Kilder og referencer

Tallene henviser til kildernes fodnotenumre.

1 **DR:** PET-rapport afslører it-svagheder hos CSC, http://www.dr.dk/Nyheder/Indland/2014/10/17/1017124227.htm

2 **Wikipedia:** Se og Hør-sagen, https://da.wikipedia.org/wiki/Se_og_H%C3%B8r-sagen

3 **Brian Krebs:** Email Attack on Vendor Set Up Breach at Target, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

4 **Wikipedia:** Sony Pictures Entertainment hack, https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

5 **The Independent:** Ku Klux Klan Twitter accounts hacked by Anonymous over Ferguson threats, http://www.independent.co.uk/9864764.html

6 **The Independent:** WhatsApp and iMessage could be banned under new surveillance plans, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html

7 **The Guardian:** The government wants tech companies to give them a backdoor to your electronic life, http://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi

8 **Ars Technica:** Obama wants Congress to increase prison sentences for hackers, http://arstechnica.com/tech-policy/2015/01/obama-wants-congress-to-increase-prison-sentences-for-hackers/?

9 **Security Research Labs:** Turning USB peripherals into BadUSB, https://srlabs.de/badusb/

10 **Sophos:** Should vapers fear malware-laced e-cigarettes? https://nakedsecurity.sophos.com/2014/11/28/should-vapers-fear-malware-laced-e-cigarettes/

11 **DR:** Bankrøvere skifter branche, http://www.dr.dk/Nyheder/Indland/2015/01/06/155959.htm

12 **Finansrådet:** Netbankindbrud – statistik, http://www.finansraadet.dk/Tal--Fakta/Pages/statistik-og-tal/netbankindbrud---statistik.aspx

13 **Version2:** Tidslinje over CSC-hackersagen, http://www.version2.dk/interaktiv/csctidslinje

14 **Politiken:** Politiet indrømmer: Sov i timen i CSC-hackersag, http://politiken.dk/indland/ECE2468237/politiet-indroemmer-sov-i-timen-i-csc-hackersag/

15 **Jonathan Zdziarski:** Hacked Celebrity iCloud Accounts, http://www.zdziarski.com/blog/?p=3783

16 **Engadget:** Snapchat servers 'were never breached,' but your snaps may still be compromised, http://www.engadget.com/2014/10/10/snapchat-snapsave-alleged-breach/

17 **The Heartbleed Bug:** http://heartbleed.com/

18 **Core Infrastructure Initiative:** http://www.linuxfoundation.org/programs/core-infrastructure-initiative

19 **Wikipedia:** Shellshock (software bug), https://en.wikipedia.org/wiki/Shellshock_%28software_bug%29

20 **Bodo Möller, Thai Duong og Krzysztof Kotowicz:** This POODLE Bites
Exploiting The SSL3.0 Fallback, https://www.openssl.org/~bodo/ssl-poodle.pdf

21 **Gabor Szappanos:** VBA Is not dead, https://www.virusbtn.com/virusbulletin/archive/2014/07/vb201407-VBA

22 **Microsoft Malware Protection Center:** Before you enable those macros... http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx

23 **Finans.dk:** Frygt for hacking skaber nye it-virksomheder, http://finans.dk/artikel/ECE6636192/frygt_for_hacking_skaber_nye_it-virksomheder/

24 **DI's skabelon for Privacy Impact Assessment:** http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Trusler%20og%20loesninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

25 **Wendy Nather:** The hierarchy of IT needs, http://informationsecurity.451research.com/?p=5679

26 **Glenda Rotvold:** How to Create a Security Culture in Your Organization, http://content.arma.org/IMM/NovDec2008/How_to_Create_a_Security_Culture.aspx

27 **Wired:** Researchers Uncover Government Spy Tool Used to Hack Telecoms and Belgian Cryptographer, http://www.wired.com/2014/11/mysteries-of-the-malware-regin/

28 **Digitaliseringsstyrelsen/DKCERT:** Borgernes informationssikkerhed 2014, https://www.cert.dk/borgersikkerhed2014/Borgernes_informationssikkerhed_2014.pdf

29 **Digitaliseringsstyrelsen:** Strategi for cyber- og informationssikkerhed, http://www.digst.dk/Arkitektur-og-standarder/Cyber-og-informationssikkerhed

30 **Lett:** Opdatering – EU's persondataforordning, http://www.lett.dk/viden/faglige-nyheder/nyt-fra-persondataret-oktober-2014/opdatering-%E2%80%93-eu%E2%80%99s-persondataforordning

31 **Microsoft:** Windows lifecycle fact sheet, http://windows.microsoft.com/en-us/windows/lifecycle

DKCERT

DeiC DANISH e-INFRASTRUCTURE COOPERATION

DTU
Asmussens Allé
Bygning 305
DK-2800 Kgs. Lyngby

t +45 35 88 82 55
e cert@cert.dk
w www.cert.dk

DKCERT

DeiC DANISH e-INFRASTRUCTURE COOPERATION

TRENDRAPPORT

Status på informationssikkerheden i året der gik

15