DKCERT
Trendrapport
2014

Status på informations-sikkerheden i Danmark

DeiC DANISH e-INFRASTRUCTURE COOPERATION

DKCERT Trendrapport 2014

Redaktion: Shehzad Ahmad, Tonny Bjørn og Torben B. Sørensen

Eksterne bidragydere: Henrik Jensen, Roskilde Universitet, Niels Madelung, Dansk Standard,
Ole Boulund, Aarhus Universitet, Kim Aarenstrup, Deloitte

Grafik og layout: Torben B. Sørensen

Forsidefoto: Colourbox.com

DKCERT, DeIC
DTU, Centrifugevej, Bygn. 356
2800 Kgs. Lyngby

DeIC-journalnr.: DeIC JS 2014-3

Om DKCERT

Det er DKCERTs mission at skabe øget fokus på informationssikkerhed 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.

DKCERT bygger på en vision om at skabe samfundsmæssig værdi 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.

Denne viden benytter DKCERT til at udvikle services, der skaber merværdi for DKCERTs kunder og øvrige interessenter og sætter dem i stand til bedre at sikre deres it-systemer.

DKCERT, det danske Computer Emergency Response Team, blev oprettet i 1991 som en afdeling af UNI-C, Danmarks it-center for uddannelse og forskning, der er en styrelse under Ministeriet for Børn og Undervisning.

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 Danmark. DKCERT er medlem af FIRST (Forum of Incident Response and Security Teams).

Indholdsfortegnelse

1. Forord

Velkommen til DKCERT Trendrapport 2014. I denne årlige rapport tager vi temperaturen på informationssikkerheden i Danmark. Og den er høj grænsende til feber.

DKCERT behandler stadig flere it-sikkerhedshændelser. Og vi hører det samme fra vore samarbejdspartnere, kunder og kolleger: Der kommer flere angreb, og de er sværere at forsvare sig mod.

Resultatet af et angreb kan være, at organisationens websted bliver sat ud af drift, uvedkommende får fat i fortrolige data, eller organisationen mister penge.

Når det sker, går jagten på den ansvarlige for sikkerhedsbruddet ind. Og alt for ofte giver man den it-sikkerhedsansvarlige skylden for, at det gik galt.

Men den sikkerhedsansvarlige er ofte kun en syndebuk. Rigtig mange gange har vedkommende nemlig hyppigt bedt sin ledelse om ressourcer til at beskytte mod angreb: Flere medarbejdere, specialiseret hardware eller software, eller uddannelse af medarbejderstaben.

De ønsker har ledelsen sagt nej til. Den har barberet budgettet til it-sikkerhed ud fra en ide om, at det ikke er et profitcenter.

Derfor er det ledelsens ansvar, når en organisation ikke er ordentligt rustet til at modstå angreb på it-sikkerheden. Hvis den sikkerhedsansvarlige ikke får de nødvendige redskaber stillet til rådighed, kan vedkommende ikke udføre sit arbejde tilfredsstillende.

En konsekvens er, at sikkerhedsfolk bliver frustrerede. De bliver stressede, når de kan se, hvad der skal til, men samtidig ikke får lov til at gøre det. På internationale konferencer for it-sikkerhedsfolk er kurser i mindfulness og håndtering af stress begyndt at dukke op. Det er et tegn på, at her er et reelt problem, som vi skal gøre noget ved.

1.1. ISO 27001 er den røde tråd

I årets trendrapport optræder ISO 27001 mange gange. Vi har valgt at lade den internationale standard for it-sikkerhed fungere som rød tråd gennem rapporten.

Vi opfatter ISO 27001 som et middel til at opnå et mål: Bedre informationssikkerhed. Båden på trendrapportens forsidebillede kan opfattes som symbol på ISO 27001: Den kan hjælpe os frem til vores mål. Men det sker kun, hvis kaptajnen tager roret og sætter kursen. Og kaptajnen skal være ledelsen, ikke en underordnet sikkerhedsansvarlig.

Det gør ISO 27001 helt klart:: Ansvaret for informationssikkerheden ligger hos ledelsen, og standarden giver et konkret bud på, hvordan det ansvar kan forankres i hverdagen.

Hvordan det kan foregå i praksis, fortæller den it-sikkerhedsansvarlige fra Roskilde Universitet i et af de fire indlæg fra eksterne skribenter, der indgår i denne trendrapport. RUC har blandt andet erfaret, at auditeringsprocessen kan udnyttes aktivt til at forbedre det løbende arbejde med sikkerheden.

Som tidligere år ser denne trendrapport både bagud og fremad. Vi analyserer tal fra DKCERTs aktiviteter i 2013 og kommer med bud på, hvilke udfordringer vi vil møde i år.

En af dem hedder Windows XP. Microsoft trækker stikket og lukker for sikkerhedsopdateringer til det aldrende operativsystem.

Her er en konkret anledning til at vise, at man tager sikkerheden alvorligt: Enhver dansk virksomhed eller organisation bør for længst have lagt en plan for, hvordan man udfaser Windows XP. Er det ikke tilfældet, er det på høje tid at tage fat på opgaven.

God fornøjelse med læsningen!

Shehzad Ahmad
Chef, DKCERT

DKCERT mener:

Alt for mange organisationer ser it-sikkerhed som noget sekundært, de kan uddelegere til en underordnet sikkerhedsansvarlig i it-afdelingen. Informationssikkerhed er ledelsens ansvar, og ledelsen skal afsætte den fornødne tid, penge og ressourcer til området. På den måde bliver den sikkerhedsansvarlig et aktiv for organisationen i stedet for en syndebuk, man trækker frem, når det går galt.

2.Resumé

Tidligere trendrapporter fik navn efter det år, de handlede om. Således udkom Trendrapport 2012 i foråret 2013. Den praksis har vi ændret, så årets udgivelse hedder Trendrapport 2014. Den dækker udviklingen i 2013 og analyserer tendenser, der får betydning i 2014.

I 2013 behandlede DKCERT 18.640 sikkerhedshændelser, hvilket udgør en stigning på 20 procent i forhold til 2012. Den største enkeltkategori af hændelser var piratkopiering, der tegnede sig for 29 procent af henvendelserne.

Der var næsten dobbelt så mange tilfælde af webservere, der blev brugt til at sprede skadelige programmer med, end året før. Der var også stigning i mængden af servere, der blev brugt til phishing.

På internationalt plan blev der fundet 5.186 nye sårbarheder i it-systemer. Det er på niveau med året før. DKCERTs scanninger af computere på Forskningsnettet, som DeIC driver, fandt sårbarheder på 21 procent af de IP-adresser, der svarede på scanningen. Langt hovedparten af sårbarhederne findes i web-software.

2.1. Borgernes datasikkerhed

Sikringen af borgernes personlige data var i fokus i 2013. Det skyldes især afsløringen af, hvordan NSA og andre efterretningstjenester overvåger og aflytter kommunikation på nettet. Men også kinesisk industrispionage, der ser ud til at være statsstyret, kom for dagens lys.

I Danmark kom nogle borgeres data i de forkerte hænder efter et hackerangreb på politiets kørekortregister. Senere blev afhængigheden af en enkelt teknologi tydelig, da en Java-opdatering gav problemer for NemID. Derved fik borgerne problemer med at kommunikere digitalt med det offentlige og bruge deres netbank.

2.2. ISO 27001

I september udkom den seneste revision af den internationale standard ISO 27001. Den beskriver, hvordan man opbygger og driver et ledelsessystem til informationssikkerhed. Roskilde Universitet er som det første universitet i Danmark blevet certificeret efter standarden. De skete i et tæt samarbejde mellem ledelsen, den informationssikkerhedsansvarlige og medarbejderne.

Dansk Standard anbefaler, at man husker forretningsmæssige parametre som kundetilfredshed og produktivitet, når man indfører ISO 27001. Det er ikke nok at tænke på den tekniske del af sikkerheden. Kommunikation og information skal også med. Aarhus Universitet har haft succes med at informere de studerende om passwordsikkerhed via små web-videoer.

2.3. Udfordringer i 2014

I 2014 venter DKCERT fortsat stor opmærksomhed om statslig overvågning og dens konsekvenser for informationssikkerheden. Det kan få betydning for, i hvor høj grad danske virksomheder ønsker at lægge tjenester ud til cloud-udbydere – især amerikanske.

Derudover opstår der en konkret udfordring, når Microsoft holder op med at udsende sikkerhedsrettelser til Windows XP. Det sker den 8. april.

Ransomware, der kræver løsesum for at frigive offerets filer, var i vækst i 2013. Det ventes at fortsætte, og også virksomheder og offentlige institutioner må være forberedt på at blive forsøgt afpresset.

Tingenes internet, hvor andet end traditionelle computere er på nettet, er i vækst. Det er truslerne mod det også. Angribere vil udnytte, at forbrugerne sjældent er opmærksomme på, at der også kommer sikkerhedsrettelser til routere, medieafspillere, fjernsyn og andet udstyr med indbygget computerkraft.

2.4. Mobilbetaling og borgernes it-sikkerhed

Som noget nyt indeholder årets trendrapport en analyse af sikkerheden ved mobilbetaling. Analysen dækker de udbredte betalingsmetoder i Danmark og gennemgår de sikkerhedsmæssige konsekvenser for hver enkelt metode.

En anden nyhed er en statistisk undersøgelse, som Danmarks Statistik har gennemført på vegne af DKCERT og Digitaliseringsstyrelsen. Den undersøger, hvilke sikkerhedshændelser borgerne har været udsat for, og hvad de ved om it-sikkerhed. Konklusionen er, at borgerne især rammes af virusangreb, men at de også ved, hvordan de kan forsvare sig mod dem. Derimod har halvdelen ikke styr på sikkerhedskopiering.

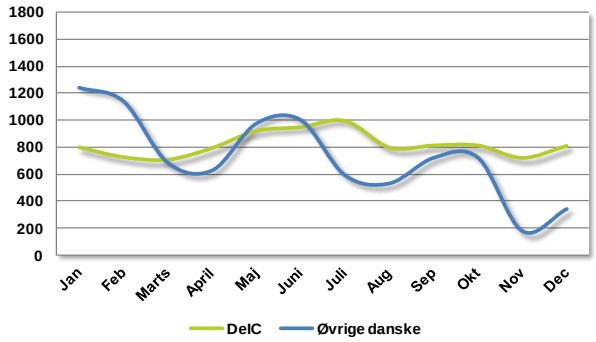
3.2013 – året i tal

3.1. Årets sikkerhedshændelser

I 2013 behandlede DKCERT 18.640 sikkerhedshændelser. Det er 20 procent flere end året før. Dermed afspejler tallet en global tendens inden for it-sikkerhed: Hvert år opstår der flere sikkerhedshændelser end det foregående år.

Lidt over halvdelen af sagerne havde tilknytning til Forskningsnettet, der drives af DeIC (Danish e-Infrastructure Cooperation). De øvrige hændelser stammer fra andre netværk, som DKCERT behandler sikkerhedshændelser for.

På grund af tekniske problemer mangler DKCERTs sagsstyringssystem statistik for perioden fra 1. september til 8. november. Derfor er tallene i denne trendrapport estimeret for den periode.

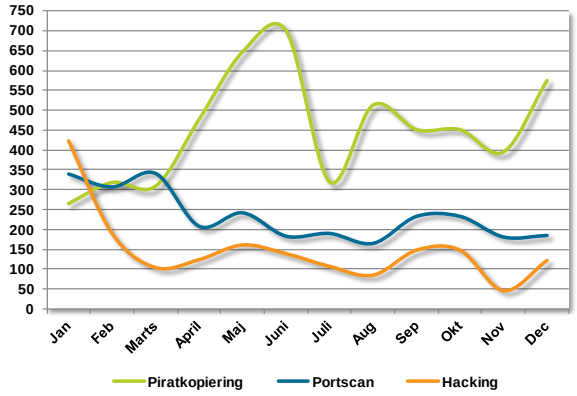


Figur 1: Hændelser på Forskningsnettet (DeIC) og øvrige sikkerhedshændelser i 2013.

DKCERT opdeler sikkerhedshændelserne i kategorier. I 2013 var den hyppigst forekommende kategori piratkopiering: 29 procent af alle hændelser handlede om brud på ophavsretslovgivningen. Mange af disse hændelser finder sted på kollegier, hvis netværk er på Forskningsnettet. Derfor ser vi ofte sæsonmæssige udsving – således er der ikke mange sager i juli, når de studerende er på ferie.

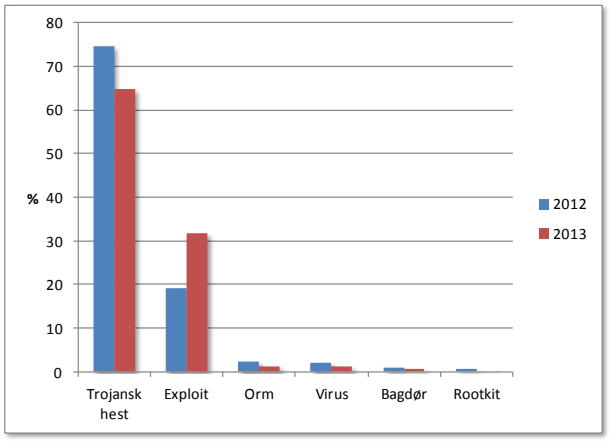
Som nummer to på hitlisten kom websteder, der blev brugt til at sprede skadelige programmer (malware). Dem var der godt 15 procent af. Næsten lige så mange hændelser var portscanninger, hvor hackere eller malware undersøger, om computere på nettet svarer på henvendelser.

Hacking udgjorde 10 procent. Det er næsten en fordobling i forhold til 2012. Kategorien er dog en blandet landhandel, så ikke alle hændelser her er reelt af typen, hvor en hacker angriber en computer og får adgang til den.



Figur 2: Sikkerhedshændelser inden for piratkopiering, portscanninger og hacking.

3.2. Malware-udviklingen

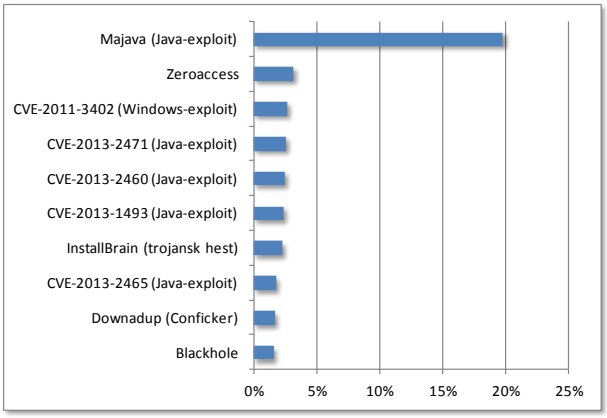


Figur 3: Udviklingen i skadelig software 2012-2013 i Danmark. Kilde: F-Secure

Sikkerhedsfirmaet F-Secure fangede omkring en halv million skadelige programmer (malware) hos firmaets danske kunder i 2013. Den mest udbredte type malware var ligesom året før trojanske heste. De spredes typisk på to måder: Inficerede websteder og e-mail. Trojanske heste udgjorde to tredjedele af alle opdagede malware-trusler.

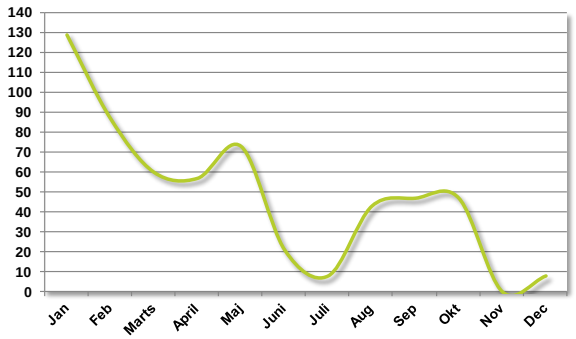
Det er imidlertid en mindre andel end i 2012. Til gengæld er mængden af exploits stigende. Et exploit er et angrebsprogram, der udnytter en bestemt sårbarhed. Exploits udgjorde 32 procent af truslerne mod 19 procent året før.

Det var især exploits, der udnyttede sårbarheder i Java, som blev spredt i 2013. Næsten 30 procent af malware-truslerne var således Java-exploits.



Figur 4: De ti mest udbredte malware-trusler i 2013 i Danmark. Kilde: F-Secure.

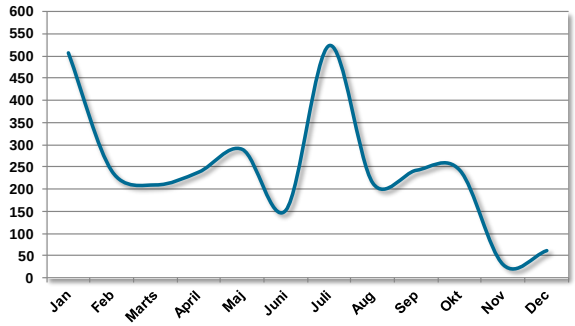
DKCERT modtager sjældent henvendelser om computere, der er inficeret med skadelige programmer. Når det sker, er det som regel fordi, computeren indgår i et botnet. Det vil sige, at bagmænd kan udnytte det skadelige program på computeren til at fjernstyre den ved at sende kommandoer til programmet. I 2013 behandlede vi 580 hændelser, hvor pc'er indgik i botnet. Det er et lille fald i forhold til 2012.



Figur 5: Danske pc'er inficeret med botnet-programmer.

Som regel er det personlige computere, der bliver inficeret med skadelige programmer. Men det sker også, at en webserver bliver inficeret. Her er formålet ofte at udnytte den til at inficere de computere, der besøger den. Det sker gerne ved, at bagmændene får webserveren til at sende de besøgende videre til en anden server, hvorpå der kører et såkaldt exploit kit. Det er et automatiseret angrebsprogram, der afprøver en række angreb på udbredte sårbarheder. Har den besøgende computer blot en af sårbarhederne, bliver den inficeret. Derfor er det vigtigt at opdage og rense inficerede webservere hurtigt, da de kan føre til store udbrud af infektioner, hvis mange besøger dem.

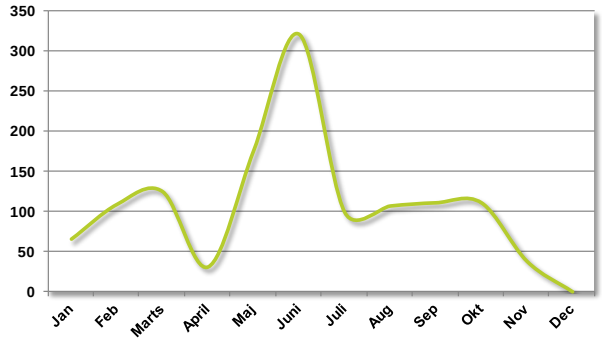
I 2013 behandlede DCKERT næsten 3.000 af den type hændelser – det er tæt på en fordobling i forhold til året før.



Figur 6: Danske websteder der spredte malware.

3.3. Spam og phishing

Vi modtog 1.364 henvendelser om e-mails med spam eller phishing i 2013. Det er et fald på 45 procent i forhold til året før. Faldet er nok udtryk for, at færre vælger at henvende sig til os om den slags mails. Årsagen er næppe, at mængden af spam og phishing-mails er faldet.

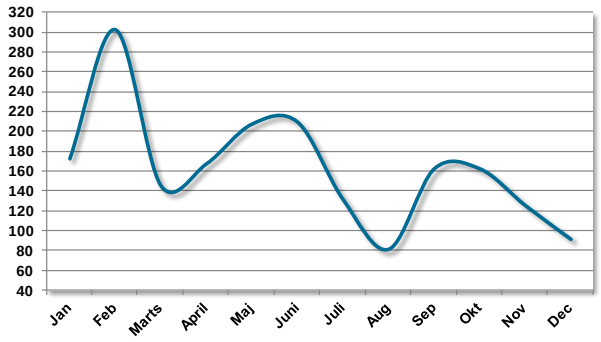


Figur 7: Spam og phishing-mails meldt til DKCERT.

Internationalt udgjorde spam i årets løb to tredjedele af alle e-mails. Andelen var højest i april, men faldt siden lidt. Det fremgår af statistikker fra Symantec[1].

Samme kilde taler om en positiv udvikling i årets løb, når det gælder phishing. I februar var godt en ud af 466 e-mails en phishing-mail. I november var den andel faldet til en ud af 1.311 mails.

[1] Symantec november 2013

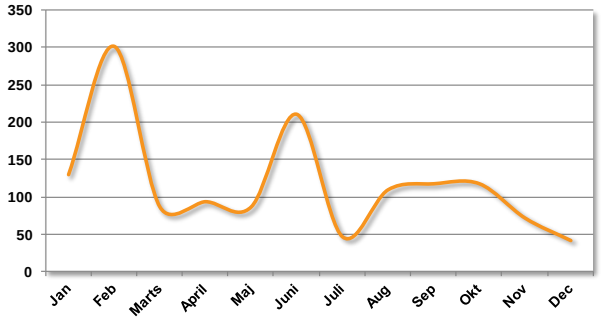


Figur 8: Danske websteder med phishing-sider.

Ud over henvendelser om phishing-mails støder DKCERT også på phishing ved en anden type sikkerhedshændelser: Når en webserver indeholder sider, som svindlere bruger til at narre fortrolige oplysninger fra deres ofre. En phishing-mail har gerne et link til sådan en side, der fx giver sig ud for at være en bank eller en online-butik.

I 2013 behandlede DKCERT 1.966 hændelser med websteder, der indeholdt phishingsider. Typisk skyldes det, at de er blevet hacket – webserverens ejer er næsten aldrig vidende om, at der ligger svindelsider på den. Bagmændene skjuler ofte siderne ved at lægge dem i undermapper, som ejeren ikke kender til. Truslen vokser, der var 62 procent flere hændelser af den type i forhold til 2012.

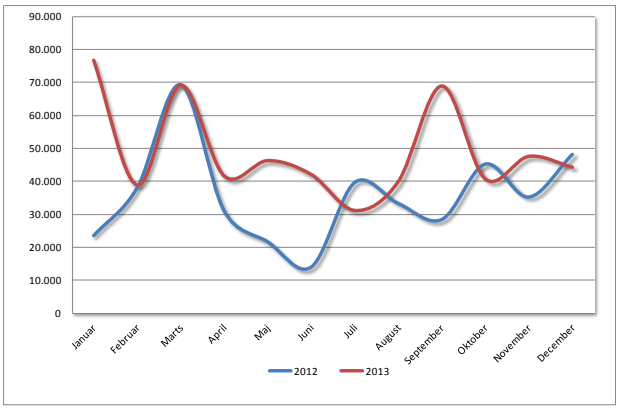
3.4. Øvrige hændelser



Figur 9: Brute force-angreb på danske IP-adresser.

Vi registrerede godt 1.400 brute force-angreb. Det er angreb, hvor en hacker eller et angrebsprogram afprøver en række kombinationer af brugernavne og password i forsøg på at få adgang. Ofte sker det ved tjenesten SSH (Secure Shell). Antallet er halveret i forhold til året før, hvilket dog ikke ser ud til at passe med de internationale tendenser. For eksempel registrerede SANS Internet Storm Center 80 procent flere angreb på SSH i 2013 end året før. For danske forhold er tallene fra DKCERTs honeynet (se nedenfor) sandsynligvis mere retvisende for tendensen.

3.5. Honeynet om angreb på SSH



Figur 10: Data fra DKCERT honeynet om forsøg på brute force-angreb på SSH-tjenesten.

DKCERT driver et såkaldt honeynet. Det er netværk af computere, der kan sammenlignes med en myrelokkedåse: Formålet er at lokke angribere til at prøve at angribe dem, så vi kan lære noget om, hvad de går efter. Honeynettet har været i drift i over to år.

SSH er en af de tjenester, vi indbyder til at angribe. Og angrebet bliver den: Hver måned er der mellem 30.000 og 70.000 forsøg på at gætte sig til brugernavne og passwords. Gennemsnitligt var der i 2013 13.000 flere angreb hver måned i forhold til 2012. Det er en stigning på 37 procent.

Angrebene kommer primært fra Kina med 43 procent af de angribende IP-adresser.

Angriberne er ikke særlig opfindsomme, når de skal afprøve kombinationer af brugernavne og passwords. Det mest populære brugernavn er "root" med "admin" som nummer to. Det mest forsøgte password er "123456" med "password" på andenpladsen.

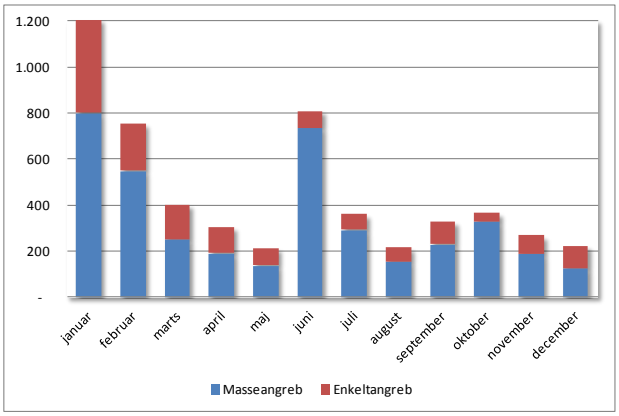
3.6. Færre defacements

Web defacement går ud på, at en hacker placerer sine egne sider på en webserver, han har hacket sig ind på. Den slags angreb var der færre af i 2013. Det fremgår af webstedet Zone-H, der fører international statistik over defacements[2]. Zone-H registrerede 5.429 angreb på danske domæner. Det er otte procent færre end i 2012.

De fleste angreb var masseangreb, hvor flere websteder på en enkelt IP-adresse overtages på én gang. Årsagen er ofte, at et webhotel er konfigureret sådan, at det er muligt at nå ind på flere kunders sider, hvis blot en enkelt af dem har et svagt password. En anden

[2] Zone-H

årsag kan være sårbarheder i den software, der kører på webhotellet.



Figur 11: Defacements på danske websteder.

Defacements ser generelt ud til at være på tilbagetog. I 2011 var der over 12.000 angreb, men siden har der været halvt så mange om året.

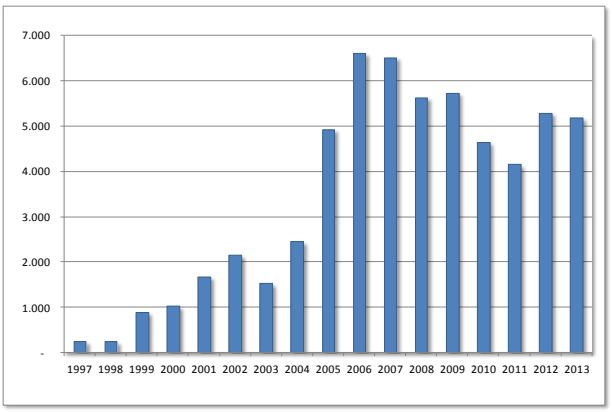
Tidligere blev defacements oftest placeret på indgangssiden, så besøgende blev mødt med hackerens budskab. Men i 2013 blev mange defacements placeret på undersider, som man kun finder, hvis man kender den præcise adresse. Det gør angrebet sværere at opdage. Til gengæld bliver genen mindre for webstedets ejer, da besøgende ikke opdager angrebet.

Årsagen er nok, at hackerne ikke længere er så interesserede i at udbrede et politisk budskab, men i højere grad er optaget af at konkurrere med andre defacement-hackere. Så er det mindre vigtigt, hvor mange der ser en defacement – ligesindede kan finde dem via tjenester som Zone-H.

3.7. Årets sårbarheder

De fleste angreb på it-systemer udnytter sårbarheder. Såkaldte sikkerhedshuller tillader hackere eller angrebsprogrammer at komme indenfor. I 2013 blev der på verdensplan registreret 5.186 nye sårbarheder ifølge den amerikanske National Vulnerability Database[3]. Det svarer til niveauet i 2012.

I løbet af året kom producenterne da også med rettelser til en lang række sårbarheder. Flere har fulgt Microsofts eksempel og har indført en fast plan for, hvornår de udsender rettelser. Således udsender Microsoft og Adobe rettelser den anden tirsdag i hver måned.



Figur 12: Sårbarheder i it-systemer ifølge National Vulnerability Database.

Oracle udsender rettelser hvert kvartal. En af dem gav problemer i Danmark: En rettelse til Java 7 medførte i oktober, at NemID ikke kunne anvendes[4].

Sårbarheder i netop Java er blandt dem, som angribere oftest udnytter. En analyse fra sikkerhedsfirmaet Kaspersky viste således en stigning i 33 procent af angreb på Java fra 2012 til 2013[5].

3.8. Statistik fra DKCERTs scanninger

I løbet af året har DKCERT foretaget 59 sårbarhedsscanninger på Forskningsnettet. Scanningerne anvender samme type værktøjer som dem, hackerne anvender. Formålet er at finde frem til sårbare systemer, så deres sikkerhedshuller kan blive lukket, før angribere udnytter dem.

I alt forsøgte vi at forbinde os til 44.768 IP-adresser. Heraf svarede 4.545. Dem scannede vi for sårbarheder. Vi fandt sårbarheder på 965 af dem eller 21 procent af de IP-adresser, der svarede. I alt var der 7.820 sårbarheder.

I gennemsnit var der 8,1 sårbarheder på hver af de sårbare IP-adresser. Det er en forbedring i forhold til 2012, hvor der var 9,4.

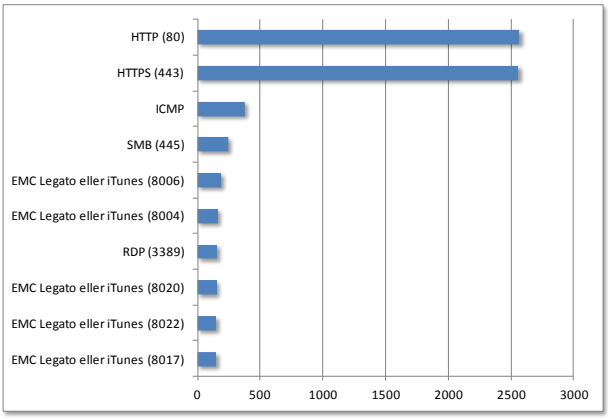
Langt de fleste sårbarheder blev fundet i websoftware. Det er tjenester, der kører på TCP-portene 80 (HTTP) og 443 (HTTPS). I alt udgjorde de to tredjedele af alle sårbarhederne.

Som nummer tre på topti-listen over fundne sårbarheder lå ICMP (Internet Control Message Protocol), der anvendes til signalering på internettet.

[3] NVD Statistics

[4] DKCERT, 16-10-2013

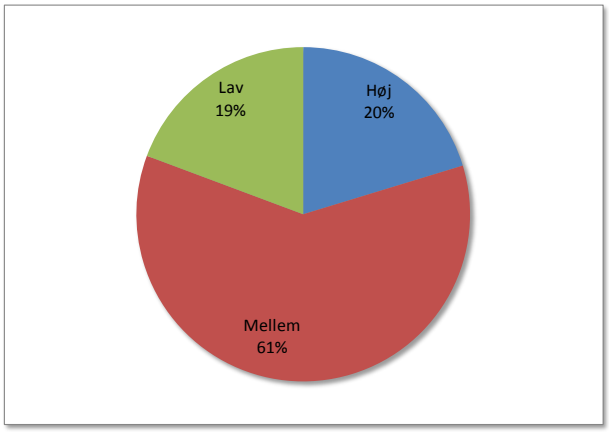
[5] Kaspersky, Java under attack



Figur 13: Topti over porte med flest sårbarheder.

Derefter fulgte SMB (Server Message Block), som Windows bruger til fil- og printerdeling. Blandt de øvrige sårbare porte var en række i området fra 8004-8022. De kan være tildelt EMC Legato Networker eller Apples iTunes – eller noget helt tredje. Endelig var der også en del sårbarheder tilknyttet RDP (Remote Desktop Protocol), som bruges til terminaladgang til Windows-computere.

20 procent af de sårbarheder, vi fandt ved scanningerne, er alvorlige. 61 procent har fået en mellemhøj risikovurdering, mens de sidste 19 procent er vurderet lavt. I forhold til 2012 er mængden af alvorlige sårbarheder uændret, mens der er kommet lidt flere med lav risikovurdering.



Figur 14: Risikovurdering af de sårbarheder, DKCERT fandt ved scanning i 2013.

Samlet set viser statistikken en lille forbedring af sikkerheden på Forskningsnettet. Der blev fundet færre sårbare maskiner (21 procent mod 24 procent i 2012). Og en større andel af de fundne sårbarheder udgør en mindre risiko. Men tallene viser også, at der fortsat er behov for at få bedre styr på processen med at installere sikkerhedsrettelser.

4.2013 – året i ord

4.1. Årets tendenser

Inden for it-sikkerhed var der et emne, der overskyggede alle andre i 2013: Efterretningstjenesters og andre statslige organisationers overvågning af borgerne. Det fyldte også meget i den danske debat, hvor fremtiden for NemID også var til diskussion. I staten kigger stadig flere på ISO 27001 som en metode til at få styr på informationssikkerheden. Standarden kom i en ny version.

4.1.1. Statslig overvågning

Statslige organisationer overvåger egne og andre borgere – og det sker også ved hjælp af teknikker kendt fra den kriminelle underverden. I februar udgav det amerikanske sikkerhedsfirma Mandiant en rapport, der sandsynliggjorde, at den kinesiske hær står bag en stor hackerbande. Banden, som firmaet kalder APT1, står bag avancerede angreb på amerikanske virksomheder[6].

Rapporten vakte megen opmærksomhed. Men den blev fuldstændig overskygget af de afsløringer, som en tidligere ansat i NSA (National Security Agency), Edward Snowden, kom med i juni. Han afdækkede en global overvågning, hvor NSA samarbejder med efterretningstjenester i en række andre lande.

Ifølge Snowdens oplysninger havde NSA indsamlet metadata om 120 millioner amerikaneres telefonsamtaler. Organisationen har i samarbejde med andre efterretningstjenester spioneret mod ambassader og opsamlet data om brug af e-mail og internet. Siden de første afsløringer er der løbende kommet detaljer frem om nye aflytninger og spionage.

Blandt afsløringerne er også, at NSA har udviklet en række programmer og værktøjer til at opsnappe og analysere information med. Blandt andet har de forsøgt at inficere computere, der bruger anonymiseringsnetværket Tor, med programmer til at aflytte kommunikationen.[7]

For it-sikkerhed betyder afsløringerne, at nye risici er dukket op. For eksempel ser det ud til, at NSA har påvirket sikkerhedsfirmaet RSA til at indføje en svag krypteringsalgoritme i et udbredt produkt. Det lader også til, at NSA har aflyttet den interne kommunikation mellem datacentre hos firmaer som Google. Derfor er de blevet nødt til at indføre kryptering ikke kun ud mod internettet, men også mellem deres datacentre.

4.1.2. Borgernes sikkerhed

I Danmark handlede it-sikkerhed i 2013 i høj grad om sikring af borgernes data. I juni kom det frem, at hackere havde været inde i politiets kørekortregister fra april til august 2012. En dansker og en svensker blev sigtet i sagen. Hackerne havde downloadet cpr-numre og oplysninger om efterlyste personer i Schengen-registre.

Systemet kørte på mainframes hos driftsleverandøren CSC. En redegørelse viser, at CSC undlod at installere to vigtige opdateringer til mainframesoftwaren, som IBM udsendte i december 2012. Det opdagede CSC først i begyndelsen af marts 2013[8].

Som resultat af angrebet kan uvedkommende have fået adgang til danske borgeres cpr-numre.

Borgernes indgang til det offentlige samt til finansverdenens systemer hedder NemID. Denne teknologi fik problemer i oktober, da login-programmet var inkompatibelt med en ny version af Java, som Oracle udsendte. Der gik fire dage, før Nets DanID fik rettet fejlen, så borgerne igen kunne komme på netbank eller logge ind på offentlige selvbetjeningsløsninger.

Parterne bag NemID vedtog at foretage en teknisk videreudvikling af løsningen: Den bliver skrevet om i Javascript, hvor den i dag er skrevet i Java[9]. Det betyder, at NemID vil kunne bruges på flere platforme. En række smartphones og andre enheder understøtter ikke Java. Men alle browsere understøtter Javascript.

Den nye Javascript-baserede NemID ventes klar i andet kvartal 2014.

Sikkerhedsmæssigt betyder det, at sikkerhedsproblemer i Java ikke længere får betydning for NemID. I stedet er det sikkerheden i browserens afvikling af Javascript, der bliver relevant. Dermed flytter fokus fra Oracle, som vedligeholder Java, til de forskellige producenter af browsere: Microsoft, Google, Mozilla, Apple, Opera og andre.

---

[6] Mandiant: APT1
[7] Wikipedia: Global surveillance disclosures
[8] Version2, 8-1-2014
[9] NemID, 2-7-2013

DKCERT mener:

Nogle få angreb mod NemID er lykkedes. De har været af typen real-time-phishing, hvor angriberne har anvendt skadelige programmer på offerets computer til at opsnappe engangskoder. Ingen af angrebene skyldes sårbarheder i Java.

Overgangen til en Javascript-baseret NemID er en sikkerhedsmæssig udfordring, fordi data i Javascript ikke er indkapslet på samme måde som i en Java-applet. Uvedkommende kan ikke gå ind og ændre i NemID's Java-applet, men enhver vil kunne ændre på de data, der sendes fra en webside til en server. Javascript er et åbent miljø, så det er let at angribe, men til gengæld ser vi sjældent sårbarheder i implementeringen af Javascript – de er derimod hyppige ved Java.

4.1.3. Beskyttelse mod DDoS

På globalt plan var der flere angreb af typen DDoS (Distributed Denial of Service). Det er overbelastningsangreb, hvor en stor mængde computere bombarderer offerets netværk med datapakker, så det bliver utilgængeligt. Angrebene kommer som regel fra botnet, hvor inficerede pc'er bliver fjernstyret til at angribe et mål, uden at deres ejere er klar over det.

Forskningsnettet var mål for flere DDoS-angreb i 2013. Nogle computere på Forskningsnettet var også med til at udføre angreb – ikke fordi deres ejere ønskede det, men fordi de var inficeret med botnetprogrammer, så it-kriminelle kunne fjernstyre dem til at udføre angreb.

Flere internetudbydere indførte i 2013 bedre beskyttelse mod DDoS-angreb. Det sker typisk ved en kombination af overvågning og handling. Overvågningen viser, hvad det normale trafikmønster er på det netværk, der beskyttes. Hvis grænseværdier bliver overskredet, kan internetudbyderen tilbyde at filtrere angrebspakker fra, øge båndbredden eller på anden måde mindske konsekvenserne af angrebet.

Den øgede opmærksomhed om problemet fremgår også af, at Center for Cybersikkerhed under Forsvarsministeriet udsendte en vejledning i, hvordan man kan imødegå et DDoS-angreb[10].

[10] Center for cybersikkerhed, 9-4-2013

DKCERT mener:

Det er godt, at danske organisationer har fået bedre midler til at beskytte sig mod DDoS-angreb. Vi venter flere angreb med endnu større båndbredde i fremtiden.

4.1.4. ISO 27001 i ny version

Familien af ISO 27000-standarder for informationssikkerhed fik en væsentlig opdatering i 2013: Den 25. september blev ISO 27001:2013 officielt frigivet.

ISO 27001 er en standard, der beskriver, hvordan man opbygger og driver et ledelsessystem til informationssikkerhed. Sådan et ledelsessystem består af politikker og processer, der skal sikre, at man har styr på de risici, organisationens it-aktiver er udsat for.

Den nye version afløser forgængeren fra 2005[11]. En væsentlig forskel er, at 2013-versionen ikke lægger så meget vægt på plan-do-check-act-cyklussen. I stedet lægger den sig mere op ad andre standarder for ledelsessystemer såsom ISO 9000 til kvalitetsstyring og ISO 20000 for it service management.

En anden nyhed er et afsnit om outsourcing. Endvidere lægger 2013-udgaven mere vægt på at måle og vurdere, hvor godt ledelsessystemet fungerer i praksis.

Den største del af standarden er Annex A, der indeholder en liste over konkrete kontroller, man kan indføre for at opnå et bestemt sikkerhedsniveau. 2005-udgaven havde 133 kontroller fordelt på 11 emnegrupper. Den nye har 114 kontroller fordelt på 14 grupper.

[11] Wikipedia, ISO 27001

5. Det eksterne perspektiv

I dette kapitel fortæller fire personer uden for DKCERT om deres erfaringer med aktuelle emner inden for informationssikkerhed. Henrik Jensen fra Roskilde Universitet fortæller, hvordan universitetet som det første i Danmark blev ISO 27001-certificeret. Niels Madelung fra Dansk Standard beskriver de konkrete, sikkerhedsmæssige fordele, sådan en certificering kan medføre. Ole Boulund fra Aarhus Universitet gennemgår, hvordan universitetet planlægger og gennemfører en awareness-kampagne. Endelig fortæller Kim Aarenstrup fra Deloitte om, hvor afhængig man bliver af leverandørens sikkerhed, når man lægger drift og andre it-opgaver ud i byen.

5.1. Sådan blev RUC ISO-certificeret

Af Henrik Jensen, it-sikkerhedskonsulent, Roskilde Universitet (RUC)

Alle statslige organisationer skal gå over til at styre deres informationssikkerhed ud fra ISO 27001. På Roskilde Universitet kendte vi allerede statens krav til indførelse af et ISMS (Information Security Management System) tilbage i slutningen af 2009: Staten ønskede indført en mindre rigid og mere "forretningsorienteret" måde at styre informationssikkerheden i de statslige institutioner. Det passede som fod i hose til vores tanker om de sikkerhedsmæssige implementeringer, universitetet foretager.

Det var væsentligt for os, at den daglige ledelse af universitetet blev gjort opmærksom på de risici, de stod over for ved valget af it til understøttelse af langt de fleste daglige processer på universitetet.

Vi finder det rimeligt, at den daglige ledelse også selv bestemmer beskyttelsesniveauet for det samlede it-miljø; selvfølgelig på et oplyst og sagligt grundlag. Vi valgte som den første statslige institution at blive certificeret efter ISO 27001.

At blive certificeret i henhold til en standard er ikke nogen triviel opgave, men nu havde ledelsen på RUC besluttet sig. Et af de mere essentielle områder i certificeringsprocessen er at få beslutningen forankret på ledelsesniveau.

5.1.1. Det tog et år

Vi undersøgte i første omgang, hvem der havde de rette kompetencer til at foretage certificeringen. Vi fandt Dansk Standard (DS) og Norsk Veritas som de mest seriøse i relation til at hjælpe os sikkert i havn.

Valget faldt af praktiske årsager på DS. De udarbejdede en fornuftig køreplan for, hvordan processen omkring certificeringen kunne forløbe optimalt. Processen forløb over et år og foregik i korte træk som følger:

1) RUC gennemgik vores interne kontroller (gjorde vi egentlig det, vi sagde, at vi gjorde?) – et halvt år.
2) DS kom og foretog et tjek af vores parathed til at blive certificeret med udgangspunkt i vores egne kontroller. Tjekket forløb i tre dage. DS leverede en screeningsrapport.
3) RUC fik fire måneder til at rette op på eventuelle forbedringstiltag fundet i punkt 2.
4) DS foretog et præaudit-forløb dels for at kontrollere, at forbedringstiltagene fra punkt 3 var implementeret og dels for at se, om vi var klar til det egentlige certificeringsforløb. Tjekket forløb i to dage. DS leverede en præauditrapport med yderligere forbedringstiltag inden certificeringen.
5) To måneder senere kom DS igen og foretog selve certificeringen. Certificeringen forløb over fem dage. Under certificeringen måtte der ikke forekomme afvigelser i forhold til standardens krav, egne krav (politikker etc.) samt lov- og myndighedskrav.

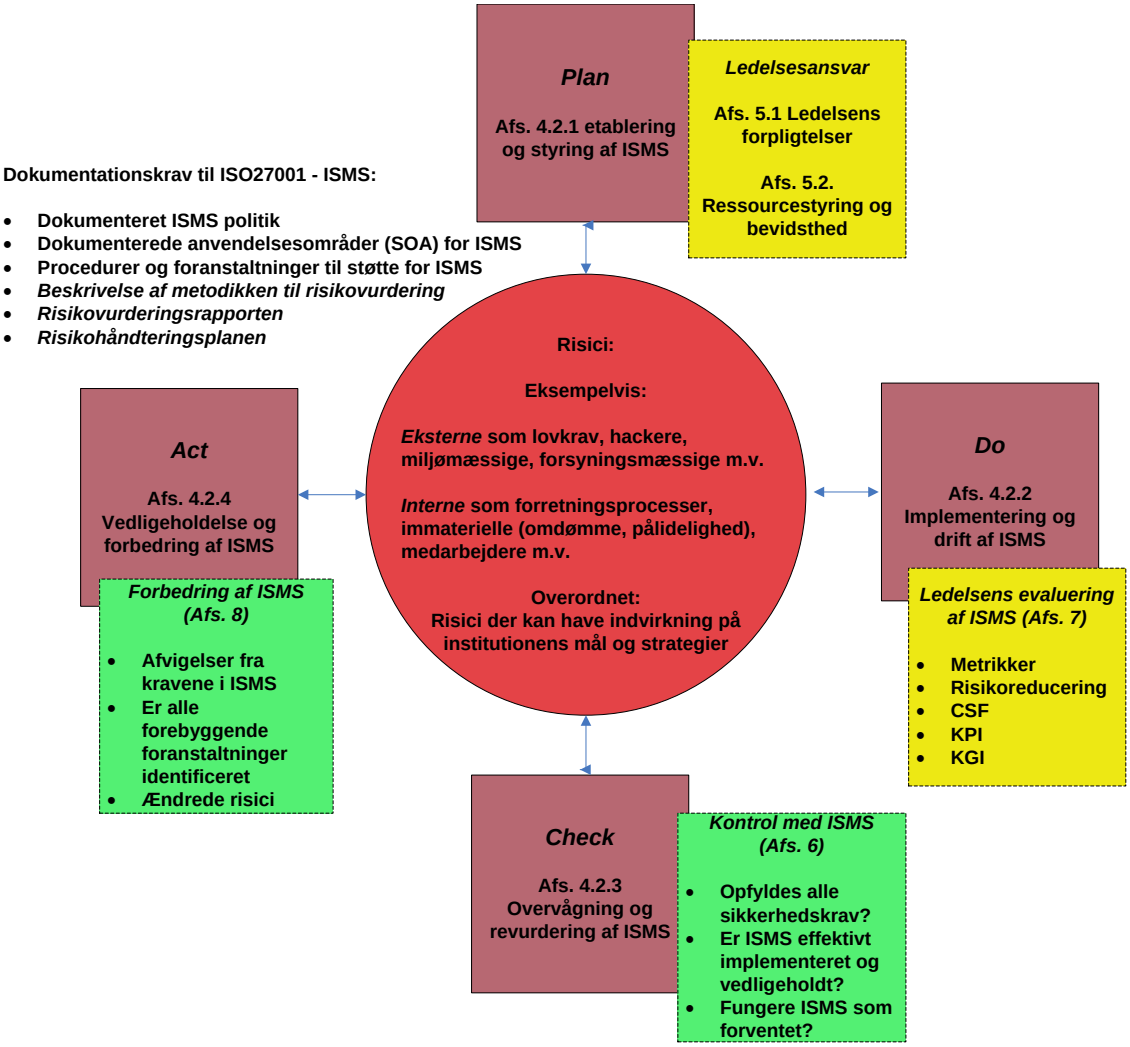
I ovenstående proces var det væsentligt, at RUC i forvejen efterlevede DS484, da en meget stor del af certificeringen går på de sikkerhedsmæssige implementeringer, institutionen har foretaget. Da implementeringskravene i ISO 27001 Annex A i høj grad læner sig op ad de sikkerhedsimplementeringer, der er krav om i DS484, har det været en stor hjælp i certificeringsprocessen at overholde DS484.

Figur 15 viser, hvordan vi fortolker ISO 27001:2007.

5.1.2. De blev involveret

RUC betragter informationssikkerhed som et fælles ansvar. Derfor har hele organisationen været involveret i processen. De væsentligste aktører på RUC var:

a) Ledelsen
b) Informationssikkerhedsansvarlig (tovholder)
c) Tværorganisatorisk informationssikkerhedsudvalg
d) Interne auditører
e) Systemejere (forretningsdelen)
f) Teknikejere (driftsansvarlige)



Figur 15: RUC's fortolkning af ISO 27001 ud fra PDCA-cyklussen (Plan-Do-Check-Act).

5.1.3. Ledelsen

Det overordnede ansvar for informationssikkerheden ligger hos den øverste ledelse. Det skyldes, at information i dag bliver behandlet i store dele af RUC. Adgangen til og brugen af informationer er oftest en kritisk forretningsproces for organisationen. Derfor er det nødvendigt for ledelsen at styre, hvordan disse informationer bliver sikret.

5.1.4. Informationssikkerhedsansvarlig

Den informationssikkerhedsansvarlige skal tilse, at RUC's samlede informationssikkerhedsniveau er i overensstemmelse med forretningens krav og behov. Vedkommende skal sikre fokus, fremdrift, og at den nødvendige informationssikkerhedsinformation når ud til alle medarbejdere i organisationen. Den informationssikkerhedsansvarlige varetager opgaven i tæt samarbejde med den øverste ledelse, informationssikkerhedsudvalget, systemejere og teknikejere.

5.1.5. Informationssikkerhedsudvalget

Udvalget koordinerer og støtter implementeringen af sikkerheden på tværs af universitetet, herunder institutterne. Det tilser, at nedenstående opgaver udføres:

1) Vurderer, om informationssikkerhedsniveauet er tilfredsstillende i forhold til forretningsførelsen og det aktuelle risikobillede.
2) Indstiller ISMS og it-sikkerhedspolitikker, som ledelsen godkender.
3) Godkender efter behov dispensationer fra it-sikkerhedspolitikken og it-sikkerhedsretningslinjer, og holder ledelsen orienteret.
4) Tilser, at de tilknyttede regler gennemføres, herunder om de lever op til de eksterne forpligtelser i lovgivning og kontrakter/aftaler.
5) Tilser, at handlingsplaner for it-sikkerheden udføres i overensstemmelse med risikovurdering/konsekvensanalyse.

6) Indstiller til ledelsen om større investeringer til foranstaltninger vedrørende informationssikkerhed.
7) Indstiller til ledelsen om prioriterede sikkerhedsmæssige implementeringer i henhold til handlingsplanerne fra risikovurderinger.
8) Styrer handlingsplaner for etablering af et ISMS.

5.1.6. Interne auditører

Intern audit af RUC's ISMS udføres for at sikre, at styringsmål, sikringsforanstaltninger samt processer og procedurer i forbindelse med RUC's ISMS til stadighed opfylder kravene i ISO 27001 samt lov- og myndighedskrav og kontraktlige forpligtigelser. Desuden sikrer audit, at vi overholder vores egen informationssikkerhedspolitik, og at ISMS fungerer som forventet.

Hovedaktiviteterne for de interne auditører er:

1) Intern audit gennemføres årligt af de interne auditører. De er hverken repræsenteret i informationssikkerhedsudvalget eller har interesse i forhold til it-afdelingen eller sikkerhedsfunktionen.
2) Resultatet af den interne audit forelægges ledelsen på RUC. Ledelsen gennemgår resultatet af den interne gennemgang sammen med den informationssikkerhedsansvarlige. Med baggrund i gennemgangen udarbejder den informationssikkerhedsansvarlige en handlingsplan for gennemførelse af identificerede afvigelser i forbindelse med den interne audit.
3) Planlægningen af den interne kontrol registreres i RUC's system til styring af universitetets ISMS. Afvigelser i forhold til kontrolplanen foretages ved udarbejdelse af gap-analyser. Gennemførelsen af den interne kontrol og resultatet af den registreres i selvstændige rapporter for de enkelte organisatoriske enheder.

Når alle aktiviteter i handlingsplanen er gennemført, rapporteres det til ledelsen, som kvitterer for auditeringens gennemførelse.

5.1.7. Systemejere

Systemejer har det forretningsmæssige eller forvaltningsmæssige ansvar for et it-system, fx. økonomisystemet. En systemejer repræsenterer en afdeling eller et institut, som anvender et givent system mest i den daglige forretningsgang. Vedkommende er dermed også den, der har det største kendskab til systemet, både når det gælder den funktionelle og den forretningsmæssige betydning.

Systemejeren definerer blandt andet det ønskede sikkerhedsniveau.

5.1.8. Teknikejere

Teknikejeren har det driftsmæssige ansvar for de forretningsmæssige informationsaktiver (systemer og data). For de tekniske informationsaktiver såsom systemsoftware, netværk, servere og andet it-udstyr har den driftsansvarlige ofte samme ansvar som systemejerne.

Den driftsansvarlige er særligt ansvarlig for at sikre, at de tekniske aktiver som minimum understøtter systemejerens krav til sikkerhedsniveau for det forretningsmæssige system med underliggende data og informationer.

5.1.9. Fordel: Vi bliver holdt til ilden

Umiddelbart kan det virke lidt ambitiøst sådan at lade sig certificere i henhold til en af de største (læs: værste) standarder, men det har selvfølgelig også nogle fordele at lade sig certificere.

En af de væsentligste fordele er, at vi konstant har en tredjepart til at holde os til ilden i forhold til vores ISMS. Certificeringen indbefatter et årligt kontrolbesøg fra DS for at sikre, at vi stadig kan beholde vores certificering, samt en re-certificering efter tre år. Vi har altså sikret den kontinuerlige tilgang til informationssikkerhedsniveauet, som vi oprindelig ønskede.

Ud over det har vi konstateret at certificeringen gennem vores risikostyring hverken giver os for lidt eller for meget sikkerhed. Vi har fokus på risici i processerne, f.eks. ændringsstyring, der giver mindre brandslukning. Vi arbejder med risici i forbindelse med services, processerne og projekterne, så vi kommer hurtigere i mål med aktiviteterne.

Endelig vælger eller fravælger vi vores implementeringer ud fra et sikkerhedsmæssigt perspektiv. Altså ingen investering i sikkerhed, uden at den er forretningsmæssigt begrundet. Det vil sige, at det vi beskytter, har større værdi end den sikkerhedsmæssige investering.

5.1.10. Udfordring: Hvad er rollerne?

Det var ikke en triviel opgave at komme igennem certificeringsforløbet på RUC. Vi havde godt nok defineret de forskellige roller og deres ansvar i forbindelse med vores ISMS. Men vi havde ikke været gode nok til at forklare, hvad disse roller indebærer.

Det er derfor essentielt at sikre sig, at rollerne og deres ansvar bliver ordentligt forankret på de respektive positioner i organisationen. Vi har efterfølgende snakket om, at de forskellige roller og deres ansvar bør ligge som en del af jobbeskrivelsen.

Certificeringsprocessen er lang og ressourcekrævende. De ressourcer, man beslaglægger til certificeringen, går fra varetagelsen af de daglige opgaver. Det var især mærkbart i en lille it-organisation som RUC's.

Institutionen bør udnævne en gennemgående tovholder for certificeringsprocessen. Ellers risikerer man, at auditør drøner rundt i organisationen og kommer til at snakke med de forkerte kolleger. Sørg for, at auditør "holdes i kort snor", og at tovholderen navigerer auditør gennem organisationen og sikrer, at auditør kun snakker med relevante medarbejdere.

5.1.11. Gode råd til andre uddannelsesinstitutioner

Vi på RUC anbefaler, at før man går i gang med en certificeringsproces, skal institutionen sikre sig følgende:

1) Få ledelsens "buy-in" til projektet. Få dem til at melde projektets start ud i organisationen. Det har en god signalværdi.
2) Sæt jer grundigt ind i standardens krav. Få evt. afstemt forventningerne med en tredjepart.
3) Vi blev certificeret i henhold til ISO 27001:2007 og blev derfor opmærksomme på den kvalitetsstyringsmekanisme, der også ligger i ISO 27001, nemlig Plan-Do-Check-ACT-cyklussen (PDCA). Sørg for, at den cyklus er gennemlevet mindst en gang i organisationen, da den hænger meget nøje sammen (procesorienteret).
4) Undervurder ikke ressourcetrækket i forbindelse med certificeringen.
5) Definer scopet for certificeringen så snævert som muligt, så certificeringen kun dækker det mest forretningskritiske.
6) Kend din organisation og ikke mindst processerne i din organisation. De gør mange af tingene i forvejen, det er bare ikke beskrevet.
7) Sørg for kun at beskrive det, de faktisk gør i organisationen – ikke så meget hvordan det virker rigtigst at gøre tingene.
8) Når auditør kommer forbi, så husk altid at fortælle sandheden. Men I behøver ikke nødvendigvis at rutte med den (svar kun på det, der spørges om).

Generelt kan vi kun anbefale at blive certificeret i henhold til standarden. Det sikrer, at man med god samvittighed kan sige, at man efterlever ISO 27001.

Desuden vil man altid holde kæden stram i forhold til de sikkerhedsmæssige implementeringer, der er foretaget i organisationen. Man foretager altså implementeringer ud fra et væsentlighedsprincip frem for sikkerhed for sikkerhedens skyld. Dermed undgår organisationen også falsk sikkerhed.

5.2. Sådan får du konkrete sikkerhedsmæssige gevinster ud af din ISO 27001-certificering

Af Niels Madelung, Dansk Standard

Den nye ISO/IEC 27001:2013 ansporer i endnu højere grad end den tidligere version virksomheder til at se på informationssikkerhed som en del af den overordnede forretningsstabilitet. Der er to kritiske forudsætninger for at få størst mulig udbytte af standarden:

- Tag udgangspunkt i virksomhedens interessenter.
- Ansku potentielle risici ud fra virksomhedens forretningsprocesser.

Det øger sandsynligheden for, at informationssikkerheden bliver præventiv, relevant og relativ i forhold til virksomhedens sårbarhed som helhed.

5.2.1. Husk forretningsparametre

Alt for mange virksomheders sikkerhed begrænser sig til at fokusere på adgangskontrollen til serverrummet, UPS'ens kapacitet eller antivirus og lignende. Forretningsstrategiske/kritiske nøgleparametre som kundetilfredshed og produktivitet ryger i glemmebogen.

Det vil i praksis sige, at man glemmer betydningen af og forudsætningerne for, at fru Hansen kan få sin dagpleje eller virksomhedens kunder kan få deres varer eller services leveret.

Fokus på interessenter og produktivitet harmonerer imidlertid med ledelsens fokus og vil derfor skærpe deres engagement, som er essentielt for at lykkes med informationssikkerhedsledelse.

Derfor er den første forudsætning for at opnå gevinster ved brug af ISO/IEC 27001 at gennemføre en forretningsrettet risikoanalyse, dvs. ud fra en outside-in og ikke inside-out tankegang. Risikoanalysen skal afdække de kritiske informationsaktiver (for forretningen) og de potentielle trusler, der kan ramme dem.

5.2.2. Forebyg konsekvenser

Behandlingen af disse trusler bør primært fokusere på forebyggelse af konsekvenser og sekundært på at fjerne sandsynligheden. Man kan ikke fjerne sandsynligheden for regn, men en paraply mindsker konsekvensen. En overdreven indsats på at fjerne sandsynligheden vil uundgåeligt underminere rentabiliteten i informationssikkerheden og virksomhedens effektivitet og konkurrencedygtighed.

Uagtet at brugerne udgør den største enkeltstående informationssikkerhedstrussel, er de også et stærkt middel mod sandsynligheder og de bedst egnede til at forebygge konsekvenser.

En effektiv og rentabel forebyggelse af konsekvenser og fjernelse af sandsynligheder skal være grundlaget for virksomhedens procedurer, retningslinjer og interne audits. Formuleringen og struktureringen (læs: anvendeligheden) af disse er derfor den næste forudsætning for at opnå gevinster ved brug af ISO/IEC 27001.

5.2.3. Involver brugerne

Hvis brugerne involveres i udarbejdelsen af procedurerne, vil de være langt mere tilbøjelige til at efterleve dem. Derved kommer deres uvurderlige viden virksomheden til gavn. Brugerne vil tage ejerskab og agere som ambassadører over for resten af virksomheden. Men det er afgørende, at procedurerne afspejler "fornuft" og ikke rigide "krav".

Hidtil har kundekrav eller konkurrencefordele været de primære årsager til, at virksomheder har ladet sig certificere.

I dag og fremover bliver det et spørgsmål om at trimme informationssikkerheden løbende som følge af interne og eksterne forandringer. Det vil i sidste ende være mest økonomisk rentabelt i modsætning til en "hit-and-run" tilgang. Det sikrer nemlig, at informationssikkerheden forbliver relevant og ikke ender som en hæmsko, der resulterer i, at procedurerne ikke længere efterleves og sikkerhedshuller opstår.

5.2.4. På linje med kvalitet

Arbejdet med informationssikkerhed bør placeres eller organiseres sammen med områder som kvalitet og effektivitet. Sådanne områder skal være i harmoni, ellers vil de uvilkårligt modarbejde hinanden i stedet for at understøtte hinanden.

Ligesom ledelsen følger op på økonomiske nøgletal fra driften, bør den også følge op på indikatorerne for kvalitet, effektivitet og informationssikkerhed.

ISO/IEC 27001 er en rentabel løsning til at undgå ineffektivitet, produktionstab, frustration, dårlig omtale og meget andet – afhængig af den konkrete virksomhed og dens forretning.

5.3. Sådan laver man en effektiv awareness-kampagne

Af Ole Boulund Knudsen, Chief Information Security Officer, Aarhus Universitet

Aarhus Universitet er i gang med at udarbejde en awareness-kampagne rettet mod de studerende. Målet med kampagnen er at gøre de studerende mere bevidste om informationssikkerhed og om de konsekvenser, manglende sikkerhed kan medføre.

Materialet til kampagnen er udarbejdet i samarbejde med de øvrige danske universiteter. Det består indtil videre af to videoklip, som har en logisk kobling, men som kan bruges hver for sig.

Det første vi gjorde, var at identificere målgruppen; i det konkrete tilfælde de studerende – både danske og internationale. Næste skridt var at identificere relevante problemstillinger. Her indgik egne erfaringer og tilbagemeldinger fra studenterorganisationer og it-afdelingens helpdesk.

Emnerne for kampagnen er henholdsvis håndtering af passwords og deling af materiale. Begge områder har betydning for både universitetets og de studerendes informationssikkerhed. På begge områder er der brug for at løfte bevidstheden om, hvor vigtigt det er.

5.3.1. Valgte hurtigt video

Næste skridt var at vælge medie. Her faldt valget ret hurtigt på levende billeder i form af video-klip.

Vi har tidligere prøvet med plakater, men desværre er effekten ikke så stor, når det kommer til studerende. Vi drukner formentlig lidt i mængden af informationer, som kommer ud til de studerende den vej. Vi må erkende, at en plakat med programmet i fredagsbaren er mere interessant end en plakat om, at man skal skifte sit password.

Da målgruppen også omfattede de internationale studerende, skulle materialet være tilgængeligt på både dansk og engelsk. Det har vi løst ved, at videoerne har dansk tale, men engelske tekster og undertekster (se figur 16). Det har i øvrigt den fordel, at video-materialet også kan bruges på infoskærme uden lyd.

Figur 16: Videoen har dansk tale og engelske undertekster. Foto: iambic intermedia

Selve video-materialet har vi haft andre til at producere, men i tæt samspil med os. Vi har dels holdt fælles brainstorms for at få gode ideer på bordet, og dels arbejdet iterativt, hvor materialet jævnligt har være til review hos både sikkerhedsfolkene ved universiteterne og udvalgte studerende for at få feedback. Det sidste vil vi nok udnytte i højere grad fremover, da konstruktiv feedback fra målgruppen er vigtig for det færdige produkt. Alternativt skal vi hyre et professionelt reklame-firma til denne del, men så bliver det væsentligt dyrere end det materiale, vi har i dag.

5.3.2. Det virker

En awareness-kampagne har en effekt. Det viser både tidligere erfaringer fra Aarhus Universitet og erfaringerne fra de universiteter, som har benyttet ovenstående materiale. Man kan således måle en markant fremgang på password-området blandt de studerende.

Det svære er at fastholde denne effekt over tid. Man skal derfor være indstillet på at gentage budskabet med jævne mellemrum.

Vi har disse gode råd til andre, der skal udvikle awareness-kampagner:

- Brug god tid på planlægningsfasen, det betaler sig ind i den sidste ende.
- Tag andre med på råd, både interessenter fra målgruppen og kollegaer fra fx kommunikationsafdelingen.
- Find eventuelt sammen med andre om at producere materialet – det kan holde budgettet i ro, hvis man kan deles om den del af omkostningerne.

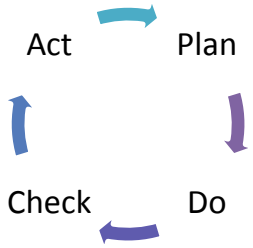
Aarhus Universitets råd om awareness-kampagner

- Start i god tid.
- Fastlæg din målgruppe.
- Identificer relevante problemstillinger.
- Involver andre i arbejdet.
- Brug humor.
- Brug flere kanaler.
- Lav et iterativt forløb.

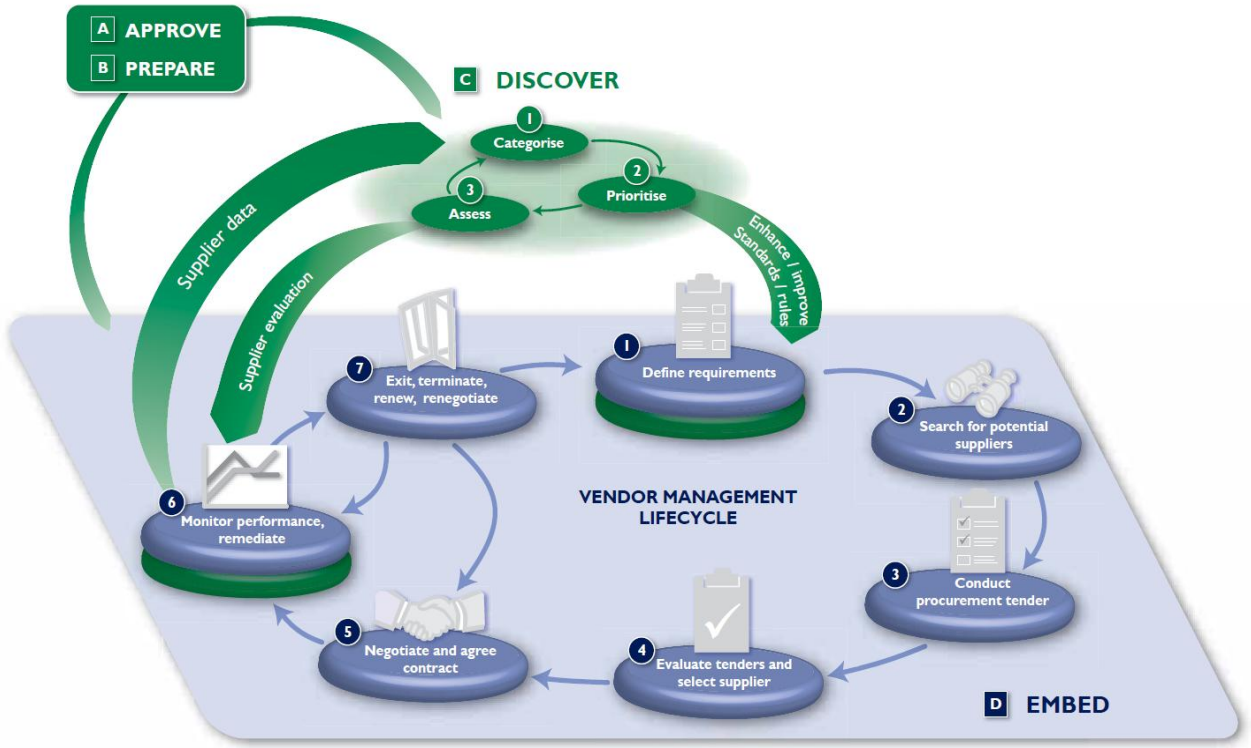
5.3.3. Brug PDCA-cyklussen

En effektiv awareness-kampagne kan planlægges ud fra den klassiske PDCA-model (se figur 17):

1. Plan: Fastlæg din målgruppe og identificer relevante problemstillinger. Vælg medie og planlæg kommunikationen. Fastlæg mål for ønsket resultat. Lav materialet.
2. Do: Sæt kampagnen i gang. Følg kommunikationsplanen. Lav målinger og indsaml feedback.
3. Check: Sammenlign målingerne med det ønskede resultat.
4. Act: Analyser kampagnen: Nåede vi vores mål? Hvad gik godt? Hvad gik mindre godt? Brug resultaterne til næste kampagne.



Figur 17: Brug Plan-Do-Check-Act-cyklussen til awareness-kampagner.



Figur 18: Supply Chain Information Risk Assurance Process.

5.4. Er din leverandør din ven eller ubevidste fjende?

Af Kim Aarenstrup, Deloitte

For de fleste organisationer spiller eksterne leverandører en vital rolle ved den digitale sikkerhed. Det gælder derfor om at have en god og velstruktureret proces om brugen af eksterne leverandører.

Ofte er leverandørerne stærkt forskellige i deres evne til reelt at passe på kundernes digitale informationer. Eksempelvis vil mange store cloud-leverandører have ret godt styr på sikkerheden, mens mindre leverandører af fx. marketingløsninger kan være udfordret omkring, hvordan man reelt løser den digitale sikkerhed for kundernes data.

5.4.1. Tænk digital sikkerhed før du indgår en samarbejdsaftale

Derfor er det vitalt, at man gør sig en række overvejelser, inden man indgår et samarbejde med en konkret ekstern leverandør. Der skal stilles de korrekte krav, og udførelsen skal kontrolleres.

Information Security Forum (ISF) har forsket i emnet, hvilket der kommet en såkaldt SCIRAP ud af (Supply Chain Information Risk Assurance Process)[12].

Processen er overordnet illustreret i figur 18. Den handler om, at man sørger for at gennemløbe fire konkrete proces-forløb:

1. Godkend (approve)
2. Forbered (prepare)
3. Afdæk (discover)
4. Indbyg (imbed)

Der er tale om en livscyklus, som skal holdes løbende i gang.

Man bør overveje at tage de sikkerhedsmæssige krav op for eksempel en gang årligt i de kontrakter, der er indgået. Det skal være skrevet ind i kontrakten som en betingelse for aftalen. Dette åbner også op for genforhandling af prisen, såfremt der er "materielle ændringer" i kontraktindholdet.

De blå farver illustrerer de processer, som indkøbsafdelingen typisk står for uden indblanding fra sikkerhed.

---

[12] ISF: SCIRAP
Securing the Supply Chain,
https://www.securityforum.org/shop/product.asp?P_ID=160

I områderne hvor farverne er blandet, er det stadig indkøb, der leder forløbet, men her støttes de eventuelt af en sikkerhedsfunktion.

Derimod leder sikkerhedsfunktionen de grønne områder (discover-processerne), ligesom den også bør godkende en leverandør, inden man underskriver eller fornyer kontrakten.

Når det er en cyklus, så skyldes det, at truslerne forandrer sig. Derfor skal sikkerhed genovervejes, såfremt der er problemer med sikkerheden i leverancen, eller hvis der opstår nye trusler mod de leverede ydelser/tjenester.

5.4.2. Kontrollér leverandøren og stil krav

I kontrakten med leverandøren bør man således også forholde sig til, hvorledes man foretager denne afdækning af sikkerhedskvaliteten i leverancen (discover).

Der er mange måder, det kan gøres på. Kundens virksomhed har måske sin egen sikkerhedsfunktion, som også kontrollerer leverandørernes sikkerhed for eksempel med scanninger.

Dette er dog blevet mindre almindeligt. Langt de fleste læner sig op ad de it-revisionserklæringer, som leverandørerne ofte får udført med en bestemt frekvens netop til dette formål.

På virksomhedens egen side handler det ofte om at gøre en konkret person ansvarlig for dette område. Så lader man vedkommende følge en struktur som ovennævnte med henblik på at skabe gennemsigtighed og kvalitet i sikkerhedssamarbejdet med leverandørerne.

Det er herunder vigtigt, at man sikrer sig, at eventuelle revisionsrapporter dækker de specifikke områder, der er vigtige for ens egen virksomhed eller institution, og at de ikke bliver alt for overordnede.

Det er vigtigt, at man stiller de rette krav til leverandøren og sikrer sig, at deres it og processer er i orden og i rimeligt omfang beskytter deres kunders data mod digitale trusler. Det er en god idé at få fagfolk til at hjælpe med at formulere disse krav, da det kan være vanskeligt for lægmand at definere. Kan en leverandør ikke indfri ønskerne, må man overveje, om de er de rigtige til opgaven.

Leverandøren skal stille med gode og trygge garantier for, at der leves op til disse krav. Det gøres rigtig fint gennem de førnævnte revisionsrapporter.

5.4.3. Når det er gået galt, hvad så?

Uanset hvor godt man beskytter sig, vil det kunne gå galt. Netop dette er det også vigtigt at forholde sig til inden indgåelsen af en leverandøraftale.

Har leverandøren eventuelt en erstatningspligt op til et vist beløb, eller har man fraskrevet sig ethvert ansvar via juridiske formuleringer? Den slags skal være helt klart, inden man underskriver.

Hvis en leverandør svigter, så er det jo din virksomheds data, der måske er kompromitteret. Derfor er det også vigtigt, at du forholder dig til, hvem der gør hvad i tilfælde af et digitalt uheld eller et angreb.

6.Trends og trusler

6.1. Trusler mod informationssikkerheden i 2014

Fremtiden vil bringe flere trusler mod informationssikkerheden. I dette kapitel har vi udvalgt nogle tendenser og forudsigelser for året. Vi har undladt nogle af de velkendte trusler, der igen vil være store, men som vi har beskæftiget os mere indgående med i tidligere års trendrapporter.

6.1.1. Windows XP udgår

Efter den 8. april udsender Microsoft ikke længere sikkerhedsrettelser til styresystemet Windows XP og kontorpakken Office 2003. Hvis der bliver fundet sårbarheder i programmerne efter den dato, vil de altså ikke blive fjernet.

Sikkerhedseksperter mener, at nogle kriminelle grupper sidder inde med viden om sårbarheder, som de ikke anvender. De venter til efter den 8. april. Til den tid vil brugerne nemlig få sværere ved at beskytte sig mod nye sårbarheder.

Problemet øges af, at næsten hver fjerde pc på verdensplan stadig kører Windows XP.

DKCERT mener:

Danske it-ansvarlige skal hurtigst muligt identificere de computere med Windows XP, de stadig har i drift, og lægge en plan for at udfase dem.

6.1.2. Afpresning

Angreb med ransomware voksede i 2013. Ofrene blev mødt med en besked om, at data på harddisken var krypteret. For at få adgang til filerne igen, skulle de købe en nøgle. I forhold til tidligere år er teknikken forbedret: Krypteringen er så stærk, at den er næsten umulig at knække.

Vi venter, at væksten fortsætter. Hvor den type angreb hidtil mest er gået ud over private, venter DKCERT, at også virksomheder og myndigheder vil blive ofre.

Ud over ransomware kan afpresning også have form af trusler om DDoS-angreb. Bagmændene kræver betaling, hvis de ikke skal iværksætte et DDoS-angreb på offerets systemer.

6.1.3. Overvågning

Truslen fra store aktører som efterretningstjenester og organiserede bander er forskellig, alt efter hvem man er. For nogle danske organisationer går overvågningen udelukkende ud over privatlivets fred: Uvedkommende kan følge med i, hvad deres brugere foretager sig på nettet. For andre er truslen økonomisk: Industrispionage kan medføre, at konkurrenter reagerer hurtigere på nye produkter eller saboterer lanceringen af dem. Og for andre er det et spørgsmål om liv eller død: Hvis de forkerte finder ud af, hvor bestemte mennesker befinder sig hvornår, kan deres liv være i fare.

Vi venter, at året vil bringe endnu flere afsløringer i stil med dem, som Edward Snowden offentliggjorde i 2013. Vi anbefaler, at danske organisationer behandler al datakommunikation ud fra en formodning om, at den kan blive aflyttet.

DKCERT mener:

Nationale efterretningstjenester har så store ressourcer, at det i praksis er umuligt at modgå et målrettet angreb. Derfor må danske organisationer tage udgangspunkt i en konkret risikovurdering for de aktiver, de vil beskytte.

Hvis aktivet kan interessere en efterretningstjeneste, kan det få betydning for, om det kan placeres på en cloud-tjeneste, om det skal beskyttes med kryptering eller eventuelt holdes helt væk fra internettet.

6.1.4. Tingenes internet

Din computer er selvfølgelig på nettet. Og din smartphone. Men hvad med bilen? Fjernsynet?

Internet of things kaldes den udvikling, hvor andet end computere udstyres med en IP-adresse. Det giver nye sikkerhedsudfordringer. Vi ved allerede i dag, hvor svært det er at holde softwaren på computere opdateret med de seneste sikkerhedsrettelser. Udfordringen mangedobles, når også fjernsyn, køkkenudstyr og armbåndsure skal opdateres løbende.

Vi venter flere angreb på udstyr, der ikke er decideredede computere. For eksempel er der allerede set angreb, der udnytter sårbarheder i trådløse routere.

DKCERT mener:

Strategier for it-sikkerhed skal udvides med planer for, hvordan man beskytter andet en traditionelt computerudstyr mod angreb fra nettet.

6.1.5. Sårbarheder bliver udnyttet

Langt de fleste af de angreb, der lykkes, udnytter sårbarheder i it-systemer. Og det er oftest sårbarheder, som der findes sikkerhedsrettelser til.

Derfor er det afgørende at have styr på processen med at holde it-systemerne opdateret. Det er vanskeligt, fordi de fleste anvender mange programmer fra forskellige leverandører.

DKCERT mener:

It-organisationer skal opbygge en dokumenteret proces for, hvordan de holder deres systemer opdateret. Og de skal undersøge mulighederne for at automatisere processen og anvende værktøjer, der gør arbejdet lettere.

6.1.6. Cloud lokker

Gevinsterne ved at lægge it-systemer ud i skyen er åbenbare: Cloud computing tilbyder mere fleksible og skalerbare løsninger, samtidig med at man slipper for selv at have besværet med at købe og drive hardware og software. Sikkerheden er på nogle punkter også bedre: Det er mere sandsynligt, at en stor cloud-leverandør holder sine systemer opdateret, end at små it-organisationer med mange daglige opgaver selv gør det. Det er også i cloud-leverandørens interesse at beskytte sine systemer: Går det galt, giver det dårlig omtale og dermed risiko for, at kunderne bliver væk.

Men cloud medfører også sikkerhedsmæssige udfordringer. Især persondatalovgivningen kan give problemer, når leverandøren fx ikke kan garantere, at data opbevares i et EU-land.

Sagerne om statslig overvågning gav i 2013 øget fokus på sikkerheden i cloud. De store cloud-systemer er naturligt i efterretningstjenesternes søgelys.

DKCERT mener:

It-organisationer bør undersøge muligheden af at bruge cloud computing. Men sikkerheden skal være et væsentligt kriterium for valget af løsning.

6.1.7. Virtuelle valutaer

Gennem 2013 steg værdien af den virtuelle valuta Bitcoin voldsomt. Det førte til flere angreb, hvor brugere fik stjålet deres digitale penge. Nogle skadelige programmer bruger offerets computer til de beregninger, der danner nye Bitcoins.

Vi forventer en stigning i angreb på Bitcoins og andre virtuelle valutaer. Hvor mange der kommer, afhænger af, hvor mange brugere der tager valutaerne til sig. For nogle år siden var det et rent nichefænomen, men de voldsomme værdistigninger har gjort flere interesserede – både legitime brugere og underverdenen.

6.2. ISO 27001

ISO 27001 er den vigtigste standard inden for informationssikkerhed i Danmark. Det skyldes, at den er valgt til standard i staten. Den seneste revision, ISO 27001:2013, forventer vi sætter yderligere skub i aktiviteterne. De firmaer, der tilbyder certificering, vil markedsføre den nye version. Og hvis nogen har ventet på revisionen, kan de nu gå i gang med at indføre den.

Vi venter, at flere universiteter vil følge Roskilde Universitets eksempel og blive certificeret efter ISO 27001. Det er en naturlig konsekvens af, at det er den officielle standard i staten – med en certificering kan man bevise, at man lever op til den. Og samtidig giver certificeringen en uafhængig ekstern kildes syn på organisationens informationssikkerhed. Det kan medføre, at man opdager fejl eller uhensigtsmæssigheder i den måde, man har tilrettelagt sikkerhedsarbejdet på.

DKCERT mener:

ISO 27001 bygger på tanken om, at sikkerhed er ledelsens ansvar. Det er fornuftigt. Men det indebærer også en risiko for, at sikkerhed ender med at være et sæt ringbind på chefens kontor, der ikke afspejler den reelle virkelighed. Det er afgørende for værdien af ISO 27001, at den anvendes som et praktisk værktøj i dagligdagen.

Det er ikke nok at investere i en certificering. Der skal også afsættes den nødvendige tid, penge og ressourcer til at gennemføre sikkerhedspolitikken i praksis.

7.Anbefalinger

I dette kapitel kommer DKCERT med anbefalinger, der har til formål at øge it-sikkerheden. De er ligesom tidligere år rettet mod tre målgrupper: Borgere, it-ansvarlige og beslutningstagere.

7.1. Anbefalinger til borgerne

DKCERT anbefaler, at du følger nedenstående råd og i øvrigt bruger din sunde fornuft. Så mindsker du risikoen for at blive offer for it-sikkerhedsproblemer.

1. Beskyt din mobiltelefon eller tablet med en kode.
2. Brug kun trådløse netværk (Wi-Fi) med kryptering.
3. Hvis du bruger et ubeskyttet trådløst netværk, så indstil telefonen eller computeren til at glemme det, når du er færdig.
4. Hold alle programmer opdateret.
5. Anvend sikkerhedsprogrammer (antivirus, anti-spyware, firewall).
6. Vær forsigtig med vedhæftede filer eller links, du får tilsendt uopfordret.
7. Tag jævnligt sikkerhedskopi af dine data.
8. Brug sikre passwords på mindst otte tegn. De skal bestå af store og små bogstaver, tal og gerne specialtegn.
9. Brug ikke samme password til forskellige tjenester.
10. Følg ikke links i mails, der beder om fortrolige oplysninger.
11. Hent kun apps og andre programmer fra kilder, du har tillid til.
12. Overvej en forsikring mod identitetstyveri.

7.2. Anbefalinger til it-ansvarlige

DKCERT anbefaler, at it-ansvarlige udfører 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 arbejdsformål (BYOD).
2. Forlang ledelsens aktive involvering i informationssikkerhedsarbejdet.
3. Udarbejd beredskabsplaner for kritiske hændelser.
4. Ajourfør og vedligehold informationssikkerhedspolitikken.
5. Begræns adgangen til data og beskyt dem med kryptering.
6. Hold de ansatte eller studerende informeret om informationssikkerhedspolitikken og aktuelle problemer.
7. Hav øget fokus på organisationens webapplikationer.
8. Gennemfør en passwordpolitik, der forhindrer svage passwords.
9. Tænk sikkerhed ind i relationen til leverandører, kunder og samarbejdspartnere.
10. Overvej forsikringer mod tab ved hacking af netbank eller DDoS-angreb.

7.3. Anbefalinger til beslutningstagere

Informationssikkerhed er ledelsens ansvar. Brud på sikkerheden kan koste dyrt i form af økonomisk tab, mistede ordrer, dårlig omtale og udgifter til oprydning. DKCERT anbefaler, at ledelsen afsætter de fornødne ressourcer til at løfte opgaven.

1. Se informationssikkerhed som et konkurrenceparameter på linje med kvalitet.
2. Inkluder informationssikkerhed i den langsigtede strategiske planlægning.
3. Tænk sikkerhed ind fra starten i udviklingen af produkter og tjenester.
4. Gør det tydeligt, at ledelsen er aktivt involveret i informationssikkerheden.
5. Prioriter og synliggør risikostyring.
6. Afsæt ressourcer til uddannelse.
7. Arbejd sammen med andre virksomheder eller interessenter om informationssikkerhed.
8. Udarbejd og vedligehold en beredskabsplan for kritiske hændelser.
9. Afsæt ressourcer i form af tid, penge og personale, før der opstår et alvorligt it-sikkerhedsproblem.

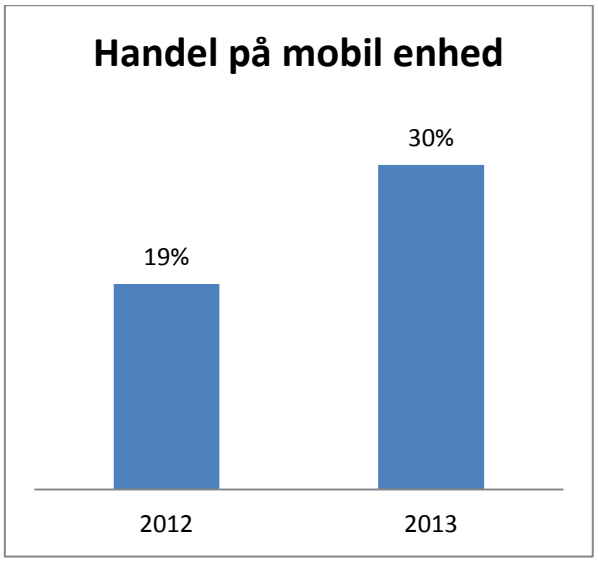
8.Sikkerhedsrisici ved mobilbetaling

Dette afsnit gennemgår de sikkerhedsrisici, som borgerne udsætter sig for, når de betaler med mobilen. Da analysen er udarbejdet ved årsskiftet, dækker den ikke teleselskabernes løsning Paii, der blev lanceret i februar 2014.

8.1. Indledning

I 2013 tog danskerne for alvor muligheden for at betale med mobiltelefonen til sig. Betalingsformidleren DIBS (Dansk Internet Betalings System) registrerede, at 423.000 nye forbrugere anvendte smartphones eller tablets til at foretage indkøb[13]. Dermed har næsten hver tredje danske forbruger handlet via en mobil enhed (se Figur 1). Undersøgelsen omfatter alle former for mobil handel, fx betaling med kreditkort i browseren på en tablet eller køb af busbillet via en app. Også Danske Bank melder om stor interesse for bankens MobilePay-løsning til overførsel af penge mellem smartphones.

For forbrugeren er der tale om en mobilbetaling, når betalingen foregår ved hjælp af mobiltelefonen. Finanssektoren har en mere begrænset definition, hvor man for eksempel ikke regner det for en mobilbetaling, når brugeren indtaster sit betalingskortnummer på en mobil webside.



Figur 1: 30 procent af forbrugerne svarer ja til, at de har handlet med en smartphone eller tablet. Kilde: DIBS E-handel 2013.

[13] DIBS, 1-12-2013

I denne rapport anvender vi den brugerorienterede definition, hvor en mobilbetaling er enhver betaling, som brugeren foretager ved hjælp af telefonen eller en tablet-computer.

Som ved andre finansielle transaktioner er sikkerhed afgørende ved mobile betalinger. De involverede parter i transaktionen skal have sikkerhed for, at betalingen når frem. Og løsningerne skal være sikret, så uvedkommende ikke kan misbruge dem til at overføre penge til sig selv.

I det følgende beskriver vi først det generelle forløb, når en kunde køber en vare, der betales med et betalingskort. Det skyldes, at mange mobilbetalinger reelt er kortbetalinger, selvom kunden ikke fysisk anvender sit betalingskort. Derefter gennemgår vi de sikkerhedsaspekter, der er fælles for alle former for mobilbetaling, før vi kommer ind på de forskellige løsninger.

8.1.1. Online betaling med betalingskort

Der indgår typisk mindst fire parter i et køb med betalingskort: En kunde, en butik, en payment service provider (PSP) og en indløser. Forløbet er gerne således:

1. Kunden vælger sin vare i en online butik. Det foregår i butikkens it-system via en webside.
2. Kunden går til betaling. Nu åbnes en webside hos PSP'en.
3. Kunden indtaster kortnummer, udløbsdato og sikkerhedskode hos PSP'en.
4. PSP'en kontrollerer strukturen af kortdata og sender transaktionen til validering hos indløseren.
5. I de fleste tilfælde sender indløseren transaktionen til kundens bank for kontrol af fx dækning eller spærring.
6. PSP'en sender besked til butikken om, at dataene og dermed betalingen er godkendt.
7. Kunden får bekræftelse på, at købet er gennemført.
8. Forretningen anmoder via PSP'en sin indløser om udbetaling, når forretningen har afsendt varen til kunden.

Forløbet er det samme, hvad enten købet foregår hjemme foran skærmen eller ude med en smartphone. Dermed er reglerne for erstatningsansvar og tilbageføring af betalinger de samme for mobilhan-

del som ved internethandel, når betalingskort er involveret.

8.1.2. Generelle risici ved mobile betalinger

Uanset løsningen er der en række risici, som gælder for alle metoder til mobilbetaling:

1. Enheden kan blive stjålet.
2. Uvedkommende kan bruge enheden.
3. Uvedkommende kan aflure indtastninger.
4. Uvedkommende kan opsnappe data trådløst.
5. Uvedkommende kan inficere enheden med skadelige programmer.

Risikoen for at enheden bliver stjålet, er højere, jo mere mobil en enhed er. Tyveri af en stationær computer kræver som regel, at tyven bryder ind hos offeret og fjerner pc'en. En bærbar pc kan blive stjålet sammen med den taske, den ligger i. Men på grund af størrelsen er risikoen for tyveri endnu større ved mobiltelefoner – en telefon kan stjæles fra en lomme eller taske i et ubevogtet øjeblik.

Hvis telefonen bliver efterladt, risikerer man, at uvedkommende bruger den. Hvis en app til pengeoverførsler er åben, kan personen overføre penge til sig selv.

Selv når brugeren har telefonen i hånden, er der risiko for, at andre kan kigge over skulderen. På den måde kan en angriber se passwords og andre koder, som brugeren indtaster. Dem kan angriberen udnytte, hvis han senere stjæler telefonen.

Angribere kan opsnappe den trådløse kommunikation, hvis smartphonen anvender Wi-Fi på et netværk uden kryptering.

Skadelige apps kan som regel kun installeres, hvis det lykkes angriberen at narre sit offer til at gøre det. Det sker som oftest ved at forklæde det skadelige program som en app, kunden er interesseret i. Skadelige apps kan for eksempel sende sms'er fra den inficerede smartphone, opsnappe fortrolige data eller bruge mikrofon og kamera til at optage offerets samtaler. I udlandet er der observeret flere skadelige apps, der angriber to faktor-autentifikation via sms: Appen kan opsnappe en sms, som indeholder en kode, brugeren skal indtaste i netbank på computeren for at godkende en transaktion[14]. Da bankerne i Danmark anvender NemID, som ikke bruger sms-autentifikation, udgør det ikke en risiko for traditionelle netbanker – men kan gøre det for mobilbanker, se afsnit 8.2.6.

8.1.3. Generelle forholdsregler

De følgende forholdsregler kan bruges til at mindske de generelle risici ved mobilbetaling.

1. Opbevar enheden sikkert, for eksempel i en inderlomme med lynlås.
2. Lås enheden med en kode, der skal indtastes eller angives på anden måde, før man får adgang til at bruge den.
3. Installer sikkerhedssoftware, der gør det muligt at slette data på afstand, hvis enheden bortkommer eller bliver stjålet. Den type program kan også hjælpe med at lokalisere enheden.
4. Gem kvitteringer og tjek kontoudtog. Gør indsigelse, når der optræder en transaktion, der ikke kan genkendes.
5. Betal med et internationalt betalingskort for at opnå den bedst mulige forbrugerbeskyttelse.
6. Hent kun apps fra de reglementerede app stores.
7. Installer sikkerhedssoftware, der beskytter mod skadelige apps.
8. Mister man enheden, skal man hurtigst muligt få spærret de betalingsløsninger, der er knyttet til den. Man skal også spærre selve mobilabonnementet.

8.2. Løsninger til mobilbetaling

Mobile betalinger bygger på teknologier, der i forvejen er kendt fra især webverdenen. Men når det bliver muligt at betale med mobilen, opstår der nye sikkerhedsudfordringer. I det følgende gennemgår vi nogle af de mobile betalingsmuligheder på det danske marked ud fra en sikkerhedsvinkel.

DKCERT har identificeret følgende metoder til betaling med en mobiltelefon/smartphone eller tablet. Listen bygger blandt andet på Betalingsrådets Rapport om nye betalingsformer[15]. Der findes utvivlsomt flere metoder, men de vil ofte være varianter af følgende teknologiske løsninger.

1. Betaling af en ydelse med en app til formålet.
2. Overtakserede sms'er.
3. Mobilpenge.
4. Pengeoverførsel mellem to smartphones (Swipp/MobilePay).

[14] NSS 11-12-2013

[15] Betalingsrådet, november 2013

5. Betaling på mobil-tilpassede websider.
6. Pengeoverførsel i mobil netbank.
7. Digitale tegnebøger som apps.
8. Kortbetaling med smartphones med NFC.

Alle ovenstående metoder anvendes i Danmark i dag bortset fra nummer 8. Da det er en oplagt mulighed i fremtiden, har vi valgt også at gennemgå dens sikkerhedsaspekter.

8.2.1. Betaling af en ydelse med en app

Bilen er parkeret, og nu skal der betales for parkeringen. Brugeren finder sin smartphone frem, åbner parkeringsselskabets app og betaler. Det er et eksempel på en app, der er målrettet til betaling af en enkeltydelse. Andre eksempler er apps til køb af billetter til bus eller tog.

Der findes to typer apps til smartphones og tablets: Native apps og hybride apps. En native app er programmeret til den enkelte platform (for eksempel Android eller iOS). En hybrid app er en app, hvor dele er skrevet til platformen, men hvor meget af indholdet vises som websider inde i appen. Endelig taler nogle også om web-apps, men i praksis er de ikke apps, men websteder skræddersyet til mobilbrug. Dem gennemgår vi nedenfor under punkt 8.2.5.

Betalingen i en hybrid app foregår ligesom en kortbetaling på et almindeligt websted (se afsnit 8.1.1). Dermed er den også omfattet af de gængse regler for internethandel.

Hvis betalingen foregår i en native app, har udviklerne indlejret en betalingsfunktion. Det kan ske på flere måder: Udviklerne kan anvende et programmeringsbibliotek, der håndterer betalingsdelen, eller de kan sende betalingsoplysningerne til en webside hos en PSP. I det førstnævnte tilfælde kan systemet udarbejdes, så det lever op til de krav, de internationale kortudstedere stiller. Disse krav er formuleret i specifikationen Payment Card Industry Data Security Standard (PCI DSS)[16]. Det handler blandt andet om, at butikken ikke ser brugerens kortnummer og sikkerhedskode. Kun PSP'en har adgang til de data.

Den danske PSP DIBS oplyser til DKCERT[17], at der er et sikkerhedsproblem i en række betalingsapps på det danske marked: Hvis appen sender betalingsdataene til PSP'ens webside i stedet for at modtage dem via funktionerne i et programmeringsbibliotek, kan det indebære, at brugeren først indtaster dataene i appen. Så befinder dataene sig i en periode i butikkens app. Dermed overholder appen ikke kravene i PCI-DSS.

Det kan give problemer for butikken, hvis den bliver udsat for audit fra indløserens side. Hvis butikken bliver udsat for et hackerangreb, risikerer den at miste data om kundernes betalingskort. Det kan i sidste ende give kunderne problemer. Foreløbig har denne risiko kun været teoretisk i Danmark, der kendes ikke til eksempler på misbrug.

8.2.1.1. Forholdsregler

Man kan anbefale kunder kun at betale i apps, der er hybride eller udviklet i henhold til PCI DSS. I praksis er det dog ikke muligt for den almindelige bruger at afgøre, hvordan betalingen foregår. Da risikoen for at miste data på den måde foreløbig må anses for ret teoretisk, har DKCERT valgt ikke at anbefale den forholdsregel. Men brugere bør altid være opmærksomme på, hvem der står bag de apps, de installerer.

Det er vigtigt, at apps anvender krypteret kommunikation (HTTPS/SSL). Men også det kan være svært for forbrugeren at afgøre. Her må man trække på evalueringer fra tredjeparter, der for eksempel undersøger appens kommunikation og lagring af fortrolige data.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

8.2.2. Overtakserede sms'er

Betaling med en sms er nok den ældste og mest afprøvede metode til mobilbetaling. Kunden sender en sms til et telefonnummer, som butikken oplyser. Butikken sender en sms retur til kunden. Først når kunden besvarer den, gennemføres betalingen.

Det er som regel et teleselskab, der står for betalingsløsningen. Dermed foregår afregningen over teleregningen. Ud over kunde, butik og teleselskab kan der også indgå en såkaldt indholdsaggregator i løsningen. Det er en virksomhed, der står for grænseflade og applikationer til brug ved betalingen.

En risiko ved sms-betaling er, at en angriber kan bestille varer i en andens navn. DKCERT vurderer, at metoden med at kræve en bekræftelse, før beta-

[16] PCI DSS
[17] DIBS, 3-12-2013

lingen gennemføres, normalt er tilstrækkelig til at forhindre den type misbrug.

Skadelige programmer (malware) udgør en særlig risiko i forbindelse med sms-betalinger. Bagmænd kan oprette overtakserede telefonnumre. Derefter inficerer de offerets smartphone med malware. Bagmændene fjernstyrer det skadelige program til at sende sms'er uden brugerens vidende. Først når teleregningen skal betales, opdager offeret misbruget.

Den type malware er primært observeret i Østeuropa. Det skyldes, at det i de lande er forholdsvis let at oprette et overtakseret nummer. Samtidig er brugerne her også mere tilbøjelige til at hente apps fra andre steder end de reglementerede app stores[18]. Derimod kender DKCERT ikke til angreb rettet specifikt mod danske kunder med overtakserede numre oprettet i Danmark.

8.2.2.1. Forholdsregler

Brugerne skal kun bekræfte sms-køb, de selv har taget initiativ til. DKCERT anbefaler, at man beskytter sin smartphone mod skadelige programmer ved kun at hente apps fra reglementerede app stores, vurdere apps kritisk og eventuelt installere antivirus på smartphonen.

Hvis telefonen bliver stjålet eller bortkommer, skal man lukke for mobilabonnementet, så uvedkommende ikke kan misbruge telefonen til sms-betaling.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

8.2.3. Mobilpenge

Mobilpenge er et betalingsmiddel, hvor brugeren med sms eller via en app kan betale for varer eller tjenesteydelser. Det betalte beløb trækkes fra den bankkonto, som er tilknyttet ordningen. Her adskiller Mobilpenge sig fra traditionelle overtakserede sms'er, hvor beløbet trækkes fra teleregningen. Mobilpenge er udviklet af Nets og de danske pengeinstitutter. Foreløbig understøtter kun få butikker systemet.

Kunden kan højst bruge Mobilpenge for 1.500 kroner pr. dag. Dette maksimum er med til at begrænse risikoen for misbrug – gevinsten er forholdsvis lille for en angriber. I øvrigt skal enhver butik, der tager mod Mobilpenge, modtage en separat bekræftelse, før den må opkræve beløbet.

Risiciene ved Mobilpenge, når det anvendes til sms-betaling, er de samme som ved sms-betaling (se afsnit 8.2.2).

Når det gælder Mobilpenge som app, er der de samme risici som ved andre apps (se afsnit 8.2.1).

8.2.3.1. Forholdsregler

Hvis enheden bliver stjålet eller forsvinder, skal man spærre mobilnummerets tilknytning til bankkontoen hurtigst muligt. Det sker hos pengeinstituttet[19].

Kunden kan overveje at sætte et lavere dagligt maksimumbeløb, der må hæves via Mobilpenge.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

8.2.4. Pengeoverførsel mellem to smartphones (Swipp/MobilePay)

I 2013 lancerede danske pengeinstitutter to tjenester til mobilbetaling: Danske Bank kom med MobilePay, mens de øvrige pengeinstitutter står bag Swipp. Løsningerne fungerer stort set på samme måde: Betaleren åbner appen og indtaster en personlig kode for at få adgang til den. Derefter indtastes beløbet samt modtagerens mobilnummer. Der kræves kun, at begge parter har appen, de får ikke oplyst hinandens kontonumre eller betalingskortnumre.

I MobilePay hæves beløbet på betalerens betalingskort. Derfor skal der være et betalingskort tilknyttet ordningen. Pengene overføres til modtageren som en konto til konto-overførsel. Brugeren kan overføre op til 1.500 kroner dagligt, dog højst 50.000 kroner om året.

I Swipp foregår betalingen som en ren konto til konto-overførsel. Kunden kan maksimalt overføre 3.000 kroner pr. dag, men kan aftale et lavere beløb med pengeinstituttet.

MobilePay er den mest brugte af de to løsninger. I starten af december blev der hver dag i gennemsnit gennemført 35.000 overførsler med MobilePay.

[18] CSO Online, 7-09-2012

[19] Nets, 26-11-2013

Siden åbningen har danskerne overført over 550 millioner kroner med løsningen – typisk ved mindre overførsler på i snit 225 kroner[20].

I dag er løsningen beregnet til overførsel mellem private. Danske Bank er i gang med at udvikle en egentlig betalingsløsning. Den kan få form af en app målrettet til virksomheder, der vil tage betaling ad den vej.

Den største risiko ved løsningerne er, at en angriber får fat i telefonen og misbruger den til betalinger. Her er beløbsbegrænsningen med til at mindske risikoen for misbrug. Danske Bank oplyser, at banken har haft meget lidt svindel med løsningen, og at den svindel, der har været, ikke har været som led i noget, der ligner organiseret kriminalitet[21].

I tilfælde af misbrug er forbrugeren dækket på samme måde, som hvis der var tale om et køb med kort. Hvis der er tale om misbrug, kan det fulde beløb derfor blive refunderet.

8.2.4.1. Forholdsregler

Betaleren skal indtaste en firecifret kode for at komme ind i MobilePay. DKCERT anbefaler, at denne kode ikke er den samme som den, man anvender til at låse telefonen op med.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

Figur 2: Swipp-funktionen er her indbygget i en mobilbank-applikation fra Finansnetbanken.

8.2.5. Betaling på mobil-tilpassede websider

En betaling på en webside, der vises på mobilen, svarer fuldstændig til en betaling på en webside, der vises på en computer. Derfor er risiciene de samme: Man risikerer at købe hos en fupbutik, der aldrig leverer varen, eller at butikken trækker et større beløb, end man har indtastet. Her er forbrugeren dækket på samme måde som ved anden internethandel.

Når indtastningen foregår på en smartphone eller tablet, er der nogle ekstra risici. Hvis det foregår på et offentligt sted, for eksempel på en café, risikerer man, at uvedkommende aflurer dataene ved at kigge over skulderen på betaleren. Der er også risiko for, at de trådløse data opsnappes, hvis der anvendes et åbent trådløst netværk.

8.2.5.1. Forholdsregler

Borgerne bør følge gængse anbefalinger for sikker internethandel. Man skal være ekstra opmærksom på, at websteder som modtager data om betalingskort, altid bør anvende krypteret kommunikation (HTTPS). Det forhindrer, at aflytning af data via trådløse netværk kan misbruges. Det kan dog i mange mobilbrowsere være svært at se, om en forbindelse er krypteret.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

8.2.6. Pengeoverførsel i mobil netbank

En mobil netbank er en app, der tilbyder nogle af de samme faciliteter, som forbrugerne kender fra netbank på computeren. Her kan man se sin saldo og overføre store beløb. Mobil netbank er blevet populær: Den 31. oktober registrerede BEC således flere besøg i banken via mobilløsningen end via netbank på computeren[22].

Den mobile netbank giver direkte adgang til kontoen. Derfor indebærer den en større risiko for tab end specialiserede apps som Swipp og MobilePay. Hvis en hacker får adgang til netbank-appen, kan han overføre store beløb til sine egne konti.

Mobilbankløsningerne anvender typisk en form for to faktor-autentifikation, hvor brugeren skal indtaste en engangskode, før der kan overføres penge. I

[20] Danske Bank, 11-12-2013
[21] Danske Bank, 4-12-2013
[22] BEC, 11-11-2013

nogle tilfælde står koden på et nøglekort, som man kender det fra NemID. Andre løsninger sender en kode via sms. Men det beskytter ikke mod misbrug, hvis smartphonen er blevet stjålet – så har tyven også adgang til de sms'er, der sendes til den.

Endnu har vi ikke set skadelige apps rettet direkte mod danske mobilbanker. I udlandet er derimod observeret en app, der giver sig ud for at være en mobilbankløsning til en række koreanske banker[23]. Hvis offeret installerer den og prøver at logge ind, får bagmændene adgang til vedkommendes loginoplysninger.

8.2.6.1. Forholdsregler

De fleste netbank-apps er beskyttet med en kode, der skal indtastes, før appen kan startes. Her er det vigtigt at vælge en anden kode end den, der bruges til at låse mobilen op med. Så er der mindre risiko for, at en tyv kan aflure koden, inden han stjæler telefonen.

Engangskoder sendt via sms er en mangelfuld sikring: Hvis telefonen er i tyvens hænder, har han også adgang til den sms, der har koden, som bruges til at godkende en overførsel. Endvidere kan sms'er opsnappes via skadelige apps som fx Zitmo (Zeus in the mobile)[24]. DKCERT vurderer derfor, at der er brug for en mere sikker løsning, fx med koder på et separat nøglekort.

For øjeblikket er det ikke muligt at anvende NemID til login på smartphones. Det ventes løst i 2014, hvor der kommer en Javascript-baseret NemID-løsning. Det muliggør to faktor-autentifikation, hvor brugeren både oplyser sin adgangskode og en engangskode fra et nøglekort. Sikkerheden i sådan en løsning kan dog først vurderes, når vi kender detaljerne om implementeringen. Nogle skadelige apps har fuld kontrol med smartphonen, så her kræves der særlige forholdsregler i designet af løsningen14.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

8.2.7. Digitale tegnebøger som apps

En digital tegnebog er en elektronisk pung, der opbevarer data om forbrugerens betalingskort eller andre betalingsløsninger. Et eksempel er Google Wallet. Når brugeren skal betale, åbnes appen og brugeren vælger det betalingsmiddel, der skal betales med. Foreløbig er fænomenet stort set ukendt i Danmark, fx er det ikke muligt at bruge Google Wallet i fysiske butikker, men kun på nettet.

Det vil dog ændre sig. Teleselskaberne TDC, Telia, Telenor og 3 har dannet det fælles selskab 4T Mobile Payments, der er ved at udvikle en app til mobilbetaling. Her vil beløbet blive trukket fra teleregningen. Appen ventes at få form af en digital tegnebog[15]. Nets arbejder på en digital tegnebog, som danske banker vil kunne udbyde[25]. Danske Bank venter også, at erfaringerne fra MobilePay med tiden kan føre til en form for digital tegnebog[20].

Da en digital tegnebog kan indeholde en række betalingsmidler, er det afgørende at beskytte den mod misbrug, hvis telefonen bliver stjålet. Skadelige programmer udgør også en risiko.

8.2.7.1. Forholdsregler

Brugeren bør beskytte sin digitale tegnebog med en kode, der er en anden end den, der bruges til at låse telefonen op. Endvidere skal det være muligt at lukke tegnebogen fra en computer, hvis telefonen bortkommer.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 8.1.3.

8.2.8. Kortbetaling med NFC

Nogle smartphones er udstyret med NFC (Near Field Communication). Det er en kontaktløs teknologi, der gør det muligt at overføre data trådløst på op til 10 centimeters afstand. NFC kan også indbygges direkte i et kort, det kendes fra Rejsekortet. Når en smartphone har NFC, kan det kombineres med en digital tegnebog, som sender kortinformation ud via NFC. Teknologien er endnu ikke i brug i Danmark. Der er ikke nogen teknisk hindring for, at man kan lægge dankortet ind i en digital tegnebog og bruge det som kontaktløst kort. Men der er ingen konkrete planer om det.

Risikoen her er den samme som ved digitale tegnebøger. Derudover foregår der en trådløs kommunikation, som i teorien kan opsnappes. Den er dog krypteret, og en angriber skal placere sig ganske tæt på for at kunne få fat i data fra NFC-kommunikationen. Derfor anser DKCERT den risiko for meget lille.

[23] FireEye, 26-11-2013
[24] DKCERT, 2011
[25] Nets, 22-8-2013

8.2.8.1. Forholdsregler

Forholdsreglerne er de samme som ved digitale tegnebøger.

8.3. Konklusion og anbefalinger

Mobilbetaling er et område i vækst. Det tog for alvor fart i 2013, dels med et stigende antal transaktioner på mobile websider, dels med introduktionen af MobilePay og Swipp.

Når flere penge udveksles mobilt, bliver området interessant for de kriminelle. Derfor er det vigtigt for borgerne at vide, hvilke nye risici mobilbetaling medfører.

Ud fra ovenstående gennemgang kan det måske se ud som om, der er store risici ved de forskellige former for mobilbetaling. Men en risiko skal altid afvejes i forhold til det tab, man risikerer at lide. De fleste af teknologierne skal ikke sammenlignes med, hvad man kan i sin netbank – de skal ses som en afløser for pengepungen.

Med en digital tegnebog kan man opbevare sine betalingskort i smartphonen. Har man dem i sin fysiske pung, er de lige til at misbruge, hvis pungen bliver tabt eller stjålet. Misbruget er dog begrænset til situationer, hvor brugeren ikke skal indtaste sin pinkode. I smartphonen skal tyven først gætte den rette kode, før han kan bruge de lagrede oplysninger. Så her er sikkerheden faktisk lidt bedre i smartphonen i forhold til den gammeldags portemonnæ.

Løsninger som Swipp og MobilePay minder også mere om en pung end en netbank: Her kan man kun overføre et begrænset beløb pr. dag. Måske er 1.500 kroner lidt mere, end de fleste går rundt med i kontanter. Til gengæld bliver beløbet dækket, hvis der sker misbrug, fordi der teknisk set er tale om en kortbetaling. Så også her er forbrugeren bedre stillet, end hvis en pung med 1.500 kroner bliver stjålet.

En anden fremtidsmulighed er virtuelle valutaer. Der har i 2013 været megen opmærksomhed omkring Bitcoin, der er en virtuel valuta. Det er muligt at veksle Bitcoins til andre valutaer, men kursen er ikke låst fast. I fremtiden kan man forestille sig, at Bitcoins kan opbevares i brugerens digitale tegnebog. Det er endnu for tidligt at sige, hvilken rolle den type valuta vil spille på betalingsmarkedet, herunder mobilbetalinger. Men det er et område, som skal følges i de kommende år.

DKCERT ser ikke mobilbetalinger som en forestående sikkerhedsmæssig katastrofe. Men vi ser samme mønster som ved tidligere nye teknologier: Først tager forbrugerne dem til sig. Derefter opdager de teknologiens uheldige sider. Derfor er der brug for at opstille en række anbefalinger, der kan sikre, at teknologiens sikkerhedsrisici undgås.

8.3.1. Anbefalinger

Efterhånden som mobiltelefonen bliver et betalingsinstrument, er der brug for anbefalinger om sikker omgang med den. Brugerne skal passe lige så godt på mobilen som på deres pengepung.

DKCERT anbefaler følgende forholdsregler:

1. Opbevar enheden sikkert, for eksempel i en inderlomme med lynlås.
2. Lås enheden med en kode, der skal indtastes eller angives på anden måde, før man får adgang til at bruge den.
3. Installer sikkerhedssoftware, der gør det muligt at slette data på afstand, hvis enheden bortkommer eller bliver stjålet. Den type program kan også hjælpe med at lokalisere enheden.
4. Gem kvitteringer og tjek kontoudtog. Gør indsigelse, når der optræder en transaktion, der ikke kan genkendes.
5. Betal med et internationalt betalingskort for at opnå den bedst mulige forbrugerbeskyttelse.
6. Hent kun apps fra de reglementerede app stores.
7. Installer sikkerhedssoftware, der beskytter mod skadelige apps.
8. Mister man enheden, skal man hurtigst muligt få spærret de betalingsløsninger, der er knyttet til den. Man skal også spærre selve mobilabonnementet.

Anbefalingerne skal opdateres, når teknologierne udvikles. For eksempel skal NemID indgå, når det bliver muligt at bruge det på smartphones.

9. Borgernes it-sikkerhed

9.1. Indledning

Formålet med dette kapitel er at afdække, om borgerne har oplevet sikkerhedshændelser. En sikkerhedshændelse kan for eksempel være et virusangreb, tab af data som følge af en smadret harddisk eller svindel via e-mails.

Har borgerne oplevet sikkerhedshændelser, undersøger vi, hvilke konsekvenser det fik for borgernes videre kontakt med det offentlige. Endelig ser vi på, hvad borgerne generelt ved om informationssikkerhed.

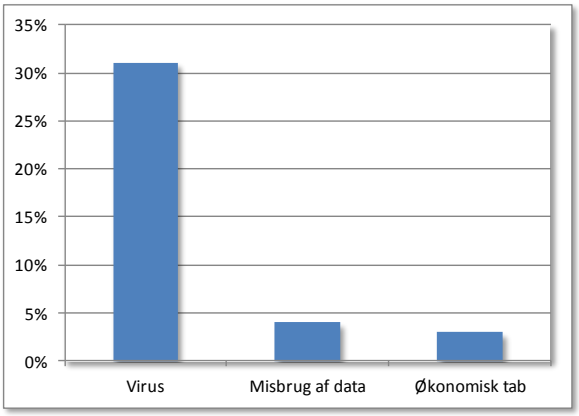
Den primære kilde til oplysningerne er en kvantitativ undersøgelse, som Danmarks Statistik foretog i januar 2014 på vegne af DKCERT. Undersøgelsen er udført i samarbejde med Digitaliseringsstyrelsen.

Undersøgelsen bygger på svar fra 981 personer, der udgør et repræsentativt udsnit af den voksne befolkning (16-74 år) i Danmark. Lidt over halvdelen af svarene blev indhentet via telefon, resten er fra spørgeskemaer på web.

Svarene fra undersøgelsen er suppleret med data indsamlet i forbindelse med rapporten It-anvendelse i befolkningen 2013 fra Danmarks Statistik[26] samt øvrige kilder.

Efter en gennemgang af undersøgelsens resultater opstiller vi en række konkrete anbefalinger til sikker adfærd på nettet og computeren og til håndtering af sikkerhedshændelser.

9.2. Oplevede sikkerhedshændelser



Figur 3: Tre typer trusler borgerne har oplevet.

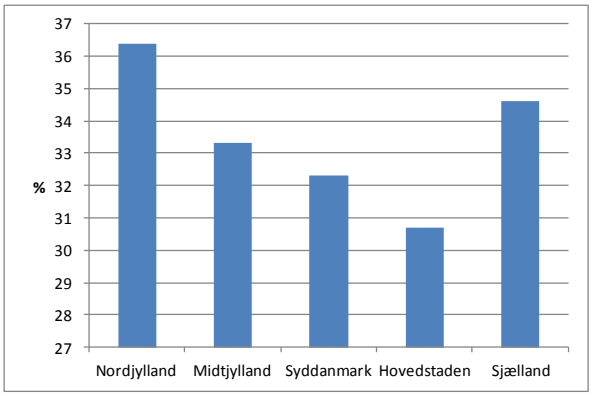
Vi har spurgt borgerne, om de har oplevet tre konkrete trusler mod deres informationssikkerhed: Virus eller anden skadelig software, misbrug af personlige oplysninger og økonomisk tab som følge af it-sikkerhedsproblemer.

Virus er den mest udbredte af de tre trusler: 31 procent har haft virus eller andre former for skadelige programmer på deres computer. Det svarer til resultatet fra undersøgelsen "It-anvendelse i befolkningen 2013", hvor 28 procent af internetbrugerne havde haft virus inden for de sidste 12 måneder.

Kun fire procent af deltagerne i undersøgelsen oplevede misbrug af personlige oplysninger. Tre procent har haft et økonomisk tab som følge af it-sikkerhedsproblemer. De tal svarer ganske godt til resultaterne i forskningsrapporten "Kriminalitet i en digitaliseret verden" fra oktober 2013[27] . Ifølge den har fire procent af danskerne inden for en 12 måneders periode været udsat for identitetstyveri, betalingskortmisbrug eller handelsbedrageri på nettet.

Generelt viser svarene kun, hvad borgerne har opdaget. Flere kan således have haft virus eller have fået misbrugt personlige data uden at være klar over det. DKCERT anslår derfor, at der reelt er flere borgere, der har haft virus eller fået misbrugt personlige data.

Tallet om økonomisk tab antages at være mere retvisende – hvis man mister penge, skal man nok opdage det.



Figur 4: Nordjyder oplever oftere sikkerhedsproblemer.

[26] Danmarks Statistik, november 2013

[27] Kriminalitet i en digitaliseret verden, 2013

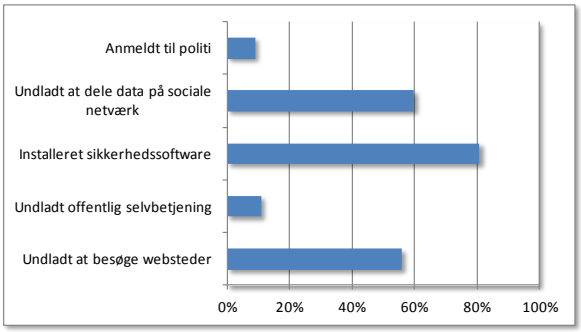
Ifølge undersøgelsen "It-anvendelse i befolkningen 2013" er det dog et stigende antal danskere, der lider økonomisk tab på grund af it-trusler. Så selvom andelen er lille, er mængden stigende.

Vi har ikke spurgt om spam, der traditionelt har været den mest udbredte gene for internetbrugerne. Det skyldes, at spam i sig selv ikke udgør et sikkerhedsproblem.

Samlet set svarer 33 procent, at de har oplevet et eller flere af de tre sikkerhedsproblemer.

Der er nogle mindre udsving i svarene, når vi opdeler dem på geografi. Således har over 36 procent af borgerne i Nordjylland oplevet it-sikkerhedsproblemer. DKCERT har ikke en forklaring på fænomenet, men bemærker, at nordjyderne også er dårligst til at tage sikkerhedskopi: Kun 28 procent sikkerhedskopierer dataene på deres pc.

9.3. Konsekvenser af sikkerhedshændelser



Figur 5: Handlinger, borgerne har udført som konsekvens af de trusler, de oplevede.

Hvad gør man, når man er udsat for en sikkerhedshændelse? Langt de fleste installerer sikkerhedssoftware. Det svarer 81 procent af dem, der var udsat for en af de tre trusler, at de har gjort.

Seks ud af ti ramte blev mere forsigtige med, hvilke data de delte på sociale netværk som fx Facebook.

Trusler kan være så skræmmende, at de direkte afholder borgerne fra at bruge tjenester på nettet. Vi har spurgt, om borgerne har holdt sig fra to slags tjenester: Dels bestemte websteder, dels specifikt offentlige selvbetjeningsløsninger (som fx Skat Tastselv). Lidt over halvdelen undlod at besøge bestemte websteder efter sikkerhedshændelsen. 11 procent afholdt sig fra at bruge offentlig digital selvbetjening.

Det giver god mening at holde sig fra at besøge bestemte websteder, hvis man har fået virus efter at have været på fx et pornowebsted eller et med piratkopier. Derimod er det sværere at argumentere for, at man skal undlade at bruge offentlig selvbetjening efter en sikkerhedshændelse.

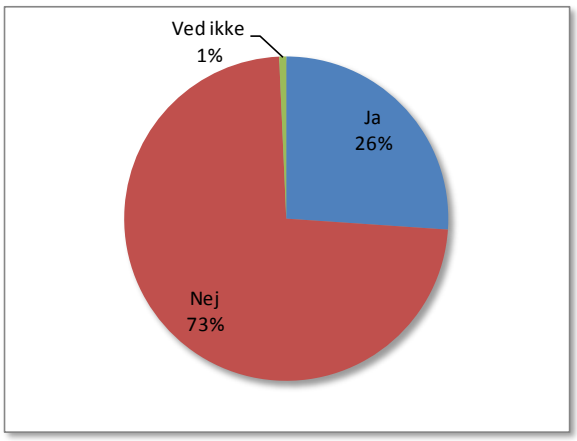
Tallene viser derfor, at nogle borgere har brug for at forstå, hvad der udgør risikoadfærd på nettet, og hvad der ikke er det.

Ni procent har anmeldt sikkerhedshændelsen til politiet eller andre instanser.

I alt har 95 procent af de borgere, der blev udsat for en it-sikkerhedshændelse, ændret adfærd eller taget forholdsregler for at undgå, at det sker igen.

9.4. Viden om informationssikkerhed

Ud over at spørge til de sikkerhedshændelser borgerne har været udsat for, har vi også undersøgt deres viden om it-sikkerhed.

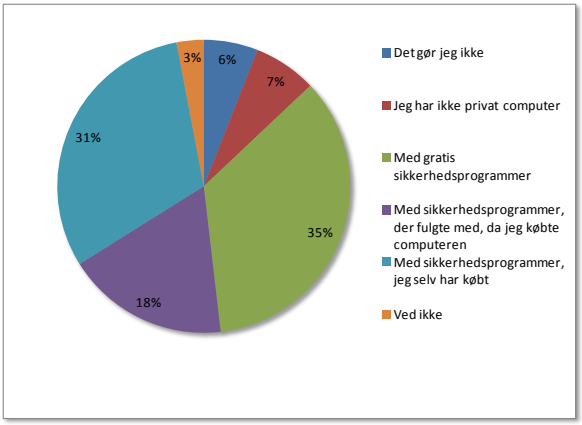


Figur 6: 26 procent sender følsomme data som ukrypterede e-mails.

Datatilsynet anser personnumre som en oplysning af fortrolig karakter. Derfor anbefaler tilsynet, at personnumre sendes krypteret over nettet. Men 26 procent af borgerne svarer, at de har sendt cpr-nummer eller andre personlige oplysninger i e-mail til det offentlige. Da krypteret e-mail er meget lidt udbredt, er det efter DKCERTs vurdering sandsynligt, at disse følsomme data er sendt ubeskyttet.

"It-anvendelse i befolkningen 2013" viste, at 86 procent af internetbrugerne anvender sikkerhedssoftware. Vores undersøgelse giver nærmere detaljer om valget af produkter. Således viser det sig, at en tredjedel vælger at beskytte sig med gratis programmer. 18 procent bruger de sikkerhedsprogrammer, der fulgte med ved køb af pc'en. Det er ofte tidsbegrænsede programmer: Efter en periode skal man betale for at

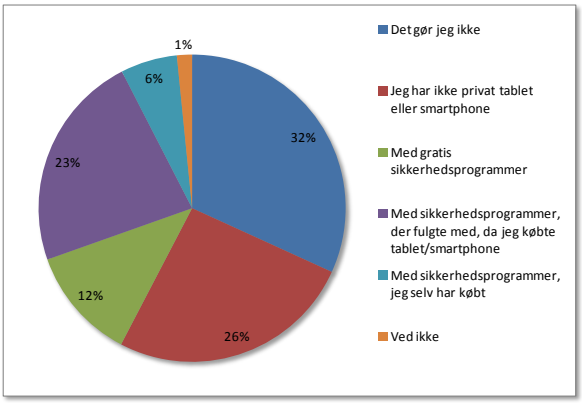
fortsætte med at modtage opdateringer af virusdefinitioner.



Figur 7: Langt de fleste beskytter deres computer.

Knap en tredjedel af brugerne har selv investeret i sikkerhedssoftware ud over det, der fulgte med ved købet af computeren. Kun seks procent svarer, at de ikke beskytter deres computer med antivirus eller lignende.

Svarene illustrerer, at pc-teknologien er gammel og moden. Folk har hørt om antivirus de sidste 20 år, så de er klar over, at det er nødvendigt. For at sætte emnet i perspektiv stillede vi de samme spørgsmål om sikkerhedssoftware til smartphones og tablets.



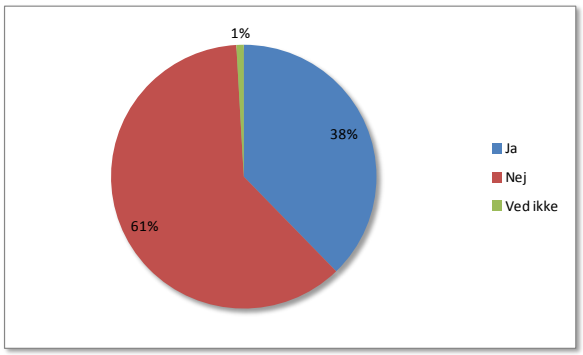
Figur 8: Mere end hver tredje beskytter ikke data på sin smartphone eller tablet.

Her svarer næsten hver tredje, at de ikke beskytter enheden og dataene på den. Hvis man udelader de 26 procent, der ikke har smartphone eller tablet, er det 43 procent af brugerne, der ikke beskytter deres udstyr.

Af de resterende har de fleste valgt at bruge den sikkerhedssoftware, der fulgte med, da de købte enheden.

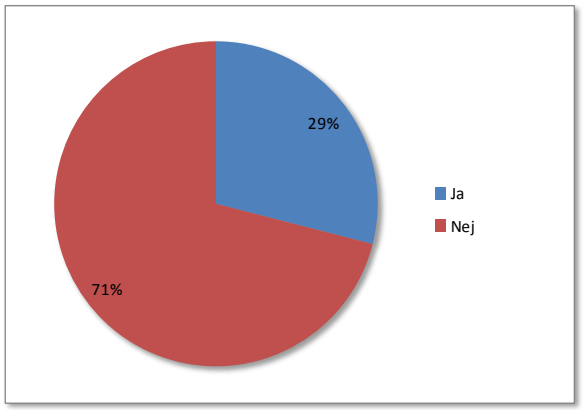
Tallene kan være udtryk for, at mange stadig opfatter en smartphone som en telefon. De tænker ikke på den som en lille computer, der indeholder en lang række personlige data: Familiebilleder, kontaktinformationer, sms'er, e-mails og passwords til en række onlinetjenester.

Sikkerhedssoftware som antivirus, firewall og antispyware beskytter computeren eller smartphonen mod angreb. Men der er også brug for at beskytte data mod at gå tabt. Det kan fx ske, hvis enheden går i stykker eller bliver stjålet. Så er det vigtigt at have en sikkerhedskopi.



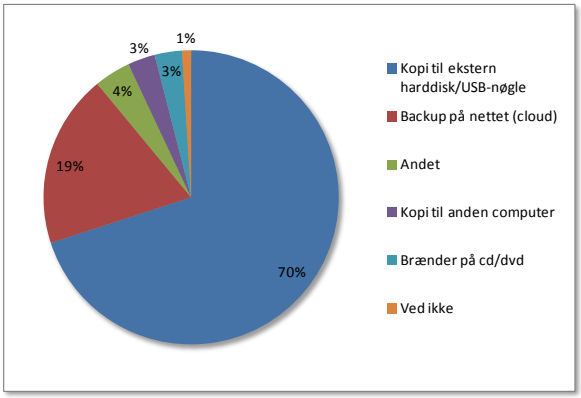
Figur 9: 38 procent tager sikkerhedskopi af data på deres private computer.

38 procent af de borgere, der har en computer, tager sikkerhedskopi af data. 61 procent gør det ikke.



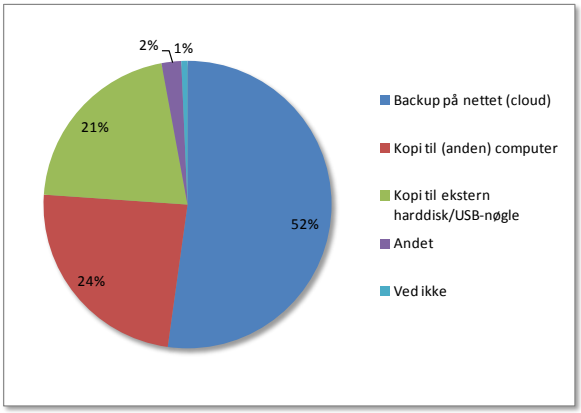
Figur 10: 29 procent tager sikkerhedskopi af data på deres smartphone eller tablet.

Men kun 29 procent af dem, der har en smartphone eller tablet, tager sikkerhedskopi.



Figur 11: Ekstern harddisk er den mest populære metode til sikkerhedskopiering af computer.

To tredjedele af de brugere, der tager sikkerhedskopi af deres computer, bruger en ekstern harddisk eller USB-nøgle. Den næstmest populære metode er cloud-backup, hvor data kopieres ud på en server på internettet.

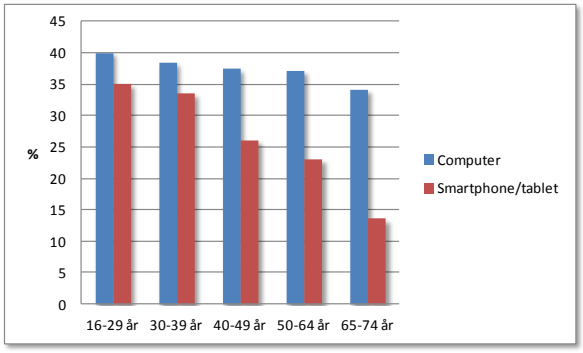


Figur 12: Cloud fører, når man skal sikkerhedskopiere data på en smartphone.

Også her er billedet anderledes for smartphones: Godt halvdelen af dem, der tager sikkerhedskopi, gør det via en cloud-tjeneste. Resten er nogenlunde ligeligt fordelt mellem kopi til en computer og ekstern disk.

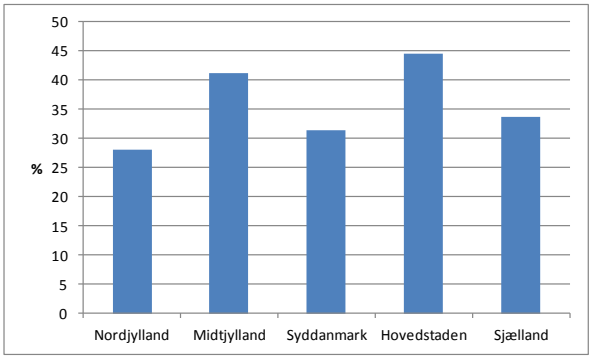
Svarene om sikkerhedskopier viser, at her er et alvorligt problem for borgerne: De risikerer at miste deres private data, fordi de ikke har styr på sikkerhedskopieringen.

Men de viser også noget interessant, når det gælder fremtiden: De unge er nemlig bedre til at tage sikkerhedskopi end de ældre. Blandt de 16-29-årige er der således 40 procent, der sikkerhedskopierer deres computerdata. Smartphone-brugere under 40 år er væsentligt bedre til at tage sikkerhedskopi end de ældre brugere.



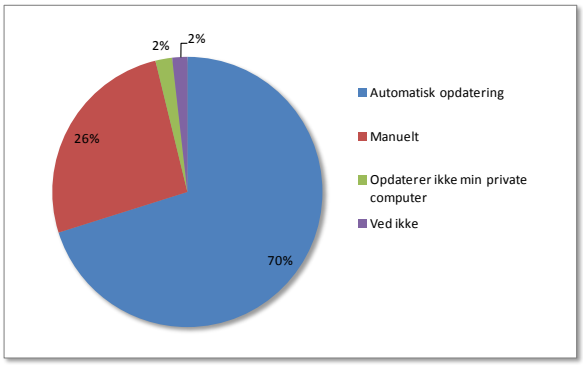
Figur 13: Procent der tager sikkerhedskopi fordelt på alder.

Københavnerne er bedst til at sikkerhedskopiere deres data. 45 procent tager jævnligt sikkerhedskopi af data på deres computer. I Nordjylland er andelen nede på 28 procent.



Figur 14: Borgere i hovedstaden sikkerhedskopierer mere end andre.

De fleste vellykkede angreb udnytter sårbarheder i software. Derfor er det afgørende for sikkerheden, at software på borgernes computere og andre enheder holdes opdateret. På den måde bliver sikkerhedshuller lukket, så snart softwareproducenten har udsendt en rettelse.



Figur 15: 70 procent bruger automatisk opdatering.

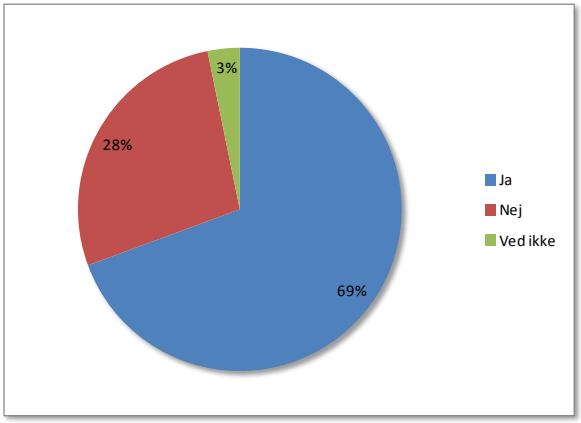
70 procent holder deres computer opdateret ved hjælp af automatisk opdatering. Det vil typisk sige, at

de har slået funktionen automatiske opdateringer til under Windows Update.

26 procent foretrækker at opdatere software manuelt, mens kun tre procent svarer, at de ikke holder computeren opdateret.

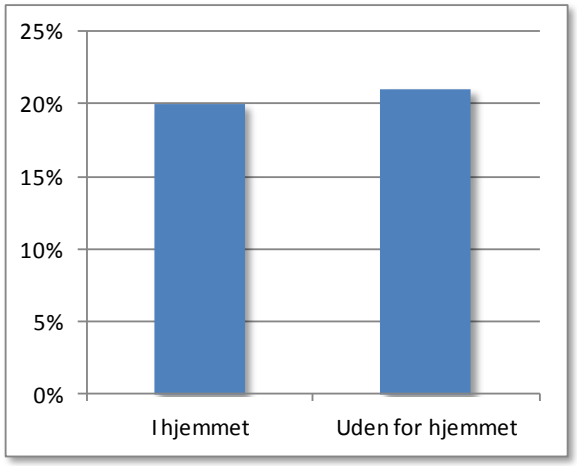
Automatisk opdatering er en nyttig funktion. Men den kan give en falsk tryghed. Funktionen dækker nemlig ikke alle programmer. Windows Update sørger således kun for at opdatere Microsoft-programmer. Andre programmer har deres egne automatiske opdateringsfunktioner, mens nogle stadig skal opdateres manuelt.

En del borgere er klar over, at automatiske opdateringer ikke nødvendigvis sikrer, at alt er opdateret. 28 procent føler sig ikke sikre på, at alle programmer der skal opdateres, rent faktisk også bliver det.



Figur 16: Føler borgerne sig sikre på, at alt der skal opdateres, bliver det?

Spørgsmålet er både stillet til dem, der anvender automatisk opdatering, og de øvrige.

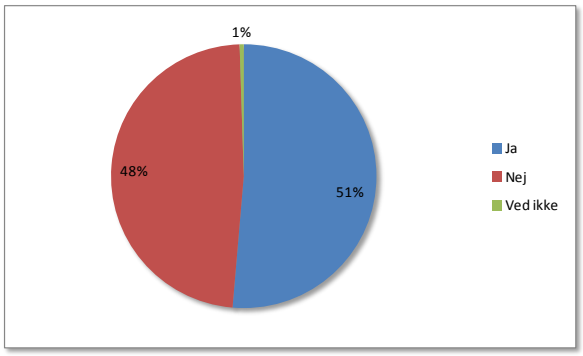


Figur 17: Hver femte bruger trådløse netværk, som ikke kræver adgangskode.

Når man bruger et trådløst netværk, skal man nogle gange indtaste en adgangskode. Det betyder som regel, at kommunikationen er krypteret. Er den ikke det, kan enhver der er inden for netværkets radiorækkevidde aflytte kommunikationen. Derfor er adgangsbeskyttelsen en vigtig sikkerhedsfunktion på trådløse netværk.

Hver femte anvender trådløse netværk uden kryptering. Andelen er stort set den samme, hvad enten det gælder bopælens eget netværk eller trådløse net ude i byen.

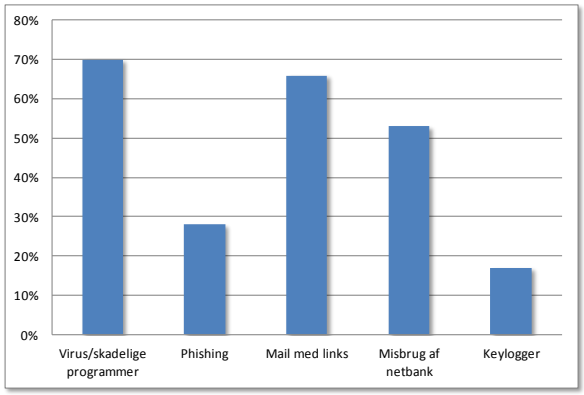
Ud over risikoen for aflytning på det pågældende netværk indebærer det også en anden risiko. Når en enhed en gang har været på et trådløst net, husker den det ofte. Når den senere ikke er på et net, søger den efter de netværk, som den har brugt før. Det kan hackere udnytte ved at opsnappe, hvilke netværk der søges efter. Derefter lader deres udstyr som om, det er det pågældende netværk. Ofte vil offerets enhed slutte sig til netværket uden videre. Det kan man beskytte sig mod ved at sætte sin enhed til at glemme netværket, når man er færdig med at bruge det.



Figur 18: Bruger samme adgangskode til flere tjenester.

Mere end halvdelen af borgerne anvender den samme adgangskode til flere forskellige tjenester. Det kan fx være deres netbank, webmail, Facebook og andre onlinetjenester.

Det udgør en sikkerhedsrisiko. Hvis angribere får fat i brugernavn og password til en enkelt tjeneste, kan de hurtigt afprøve kombinationen på andre tjenester. På den måde kan et brud på sikkerheden på en onlinebutik, hvor man en enkelt gang har købt noget, føre til, at fremmede får fat i ens mails eller andre fortrolige oplysninger.



Figur 19: Borgere der ved, hvordan de skal beskytte sig mod bestemte trusler.

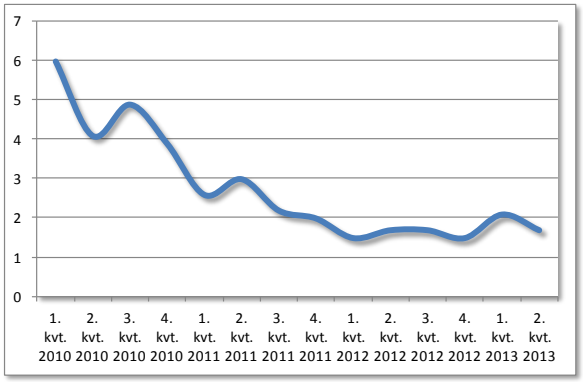
Endelig har vi spurgt borgerne, om de føler sig i stand til at beskytte sig mod fem konkrete trusler: Virus og andre skadelige programmer, phishing, e-mails med vedhæftede filer eller links, misbrug af netbank og keyloggere. For virus og e-mails ved over to ud af tre, hvad de skal gøre. Derimod kan kun 28 procent beskytte sig mod phishing.

Det er dog ikke nødvendigvis korrekt. 47 procent svarer nemlig, at de ikke ved, hvad phishing er. Så det er muligt, at de godt kan genkende en svindel-mail og undlade at reagere på den, selvom de ikke kender begrebet phishing.

Kun 17 procent kan beskytte sig mod keyloggere, der opsnapper tastetryk. Men også her er det nok tegn på uvidenhed: 61 procent ved ikke, hvad en keylogger er. Da en keylogger oftest installeres af et skadeligt program, vil de som regel være beskyttet i kraft af deres antivirusløsning. Det samme gælder for misbrug af netbank – også her foregår misbruget som regel via skadelig software på offerets computer.

9.5. Internationalt perspektiv

For at sætte tallene i perspektiv inddrager vi her statistikker fra Microsofts Security Intelligence Report[28]. Rapporten fører statistik over mængden af computere, som firmaets "Værktøj til fjernelse af skadelig software" renser for infektioner. Værktøjet er et program, der kører hver måned på de pc'er, hvor automatiske opdateringer er slået til. Programmet kan fjerne en række af de mest udbredte virus og andre skadelige programmer.



Figur 20: Computere renset pr. 1.000 computere i Danmark 2010-2013.

Tallet angives som antallet af computere pr. 1.000 computere, der blev renset for skadelig software. I den seneste rapport, der dækker andet kvartal 2013, var tallet for Danmark 1,7.

Til sammenligning var gennemsnittet på verdensplan 5,8. Der er imidlertid store udsving: fra 31,5 i Irak til 1,1 i Japan. Men Danmark ligger blandt landene med den laveste mængde infektioner.

9.6. Konklusion på undersøgelsen

Virus og andre skadelige programmer er den trussel, borgerne i vores undersøgelse hyppigst er udsat for. Derimod har kun få borgere fået misbrugt personlige oplysninger eller haft økonomisk tab som følge af it-sikkerhedshændelser.

Det passer godt til de forholdsregler, som borgerne tager: Kun fem procent oplyser, at de ikke bruger en form for antivirus eller anden sikkerhedssoftware. At de så alligevel kan blive ramt, kan skyldes, at sikkerhedssoftware ikke beskytter mod alt. Desuden kan nogle af de ramte være dem, der ikke anvender sikkerhedssoftware, eller hvor den ikke bliver opdateret.

Skønt 31 procent borgere med virusangreb kan lyde højt, ligger Danmark internationalt blandt de seks lande med færrest tilfælde af skadelig software.

Hvor danskerne er gode til at beskytte deres computere mod virus, er de dårligere til at beskytte sig selv. Halvdelen bruger således samme password til flere tjenester. Dermed udsætter de sig for risiko for, at uvedkommende får adgang til deres data.

Et andet eksempel på dårlig beskyttelse af personlige data er, at 26 procent sender fortrolige oplysninger med e-mail til det offentlige. Hvis det sker på et usikkert netværk, kan uvedkommende opsnappe dataene.

[28] Microsoft Security Intelligence Report

61 procent af borgerne vil miste data, hvis deres computer bliver stjålet eller går i stykker. De tager nemlig ikke jævnligt sikkerhedskopi af deres data. Procentsatsen svarer til, at 2,3 millioner danskeres private data ikke er sikret med sikkerhedskopiering.

Endnu værre ser det ud for smartphones og tablets: Her er det 71 procent, der ikke sikkerhedskopierer. I nogle tilfælde kan der dog være en sikkerhedskopi, som brugeren ikke kender til. For eksempel kan en telefon være sat op til at anvende et adressekartotek på en server i skyen. Så er navne og telefonnumre stadig tilgængelige, selvom telefonen går tabt.

Geografisk set tyder undersøgelsen på, at borgere i hovedstadsområdet har bedre styr på it-sikkerheden end borgere i resten af landet. Især Nordjylland stikker ud, når det gælder mængden af sikkerhedsproblemer – og de er tilsvarende dårligst til at tage sikkerhedskopi.

Samlet er det DKCERTs opfattelse, at danskerne har ganske godt styr på skadelig software og hvordan man beskytter sig imod den. Derimod er der alvorlige problemer med sikringen af data via sikkerhedskopiering. Og borgerne savner også viden om, hvordan de beskytter og behandler fortrolige data. Sikkerheden er bedre på computere end på nye enheder som smartphones og tablets.

9.7. Anbefalinger

Vores undersøgelse har afdækket et behov for bedre beskyttelse af data på mobile enheder. Men også de traditionelle computere giver sikkerhedsmæssige udfordringer, primært inden for sikkerhedskopiering.

Vi har her samlet nogle anbefalinger til borgerne om, hvordan de kan forbedre deres it-sikkerhed. Vi har opdelt dem i to grupper: Råd om sikkerhed på mobile enheder og generelle råd.

9.7.1. Sikkerhed på mobilen

DKCERT anbefaler følgende forholdsregler i forbindelse med borgernes anvendelse af mobile enheder:

1. Beskyt din telefon med en kode.
2. Brug kun trådløse netværk (Wi-Fi) med kryptering.
3. Hvis du bruger et ubeskyttet trådløst netværk, så indstil telefonen til at glemme det, når du er færdig.
4. Luk for abonnementet og tilknyttede betalingstjenester, så snart telefonen bliver stjålet eller tabt.
5. Tag sikkerhedskopi af data på mobile enheder.

9.7.2. Generel sikkerhed

Derudover anbefaler DKCERT følgende grundlæggende forholdsregler til sikker adfærd på nettet og computeren.

6. Hold alle programmer opdateret.
7. Anvend sikkerhedsprogrammer (antivirus, antispyware, firewall).
8. Vær forsigtig med vedhæftede filer eller links, du får tilsendt uopfordret.
9. Tag jævnligt sikkerhedskopi af dine data.
10. Brug sikre passwords på mindst otte tegn. De skal bestå af store og små bogstaver, tal og gerne specialtegn.
11. Brug ikke samme password til forskellige tjenester.
12. Følg ikke links i mails, der beder om fortrolige oplysninger.
13. Hent kun apps og andre programmer fra kilder, du har tillid til.

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 dens modstand mod Scientology Kirken og for sin støtte til Wikileaks og The Pirate Bay. Gruppen stod også bag operation AntiSec i foråret 2011.

Awareness: Betegnelse for tiltag eller aktiviteter, der skaber opmærksomhed og påvirker ansattes eller borgeres viden og adfærd i forhold til it-sikkerhed.

BYOD. Bring Your Own Device, dækker over at et stigende antal organisationer lader de ansatte selv stå for indkøb og drift af deres eget udstyr. Det giver på den ene side større fleksibilitet, men på den anden side introducerer det en række problemstillinger i forhold til informationssikkerheden.

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 vil ofte være 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: 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 til det enkelte site.

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, forkortet CVE, 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, der ikke er i distribution, såsom de fleste webapplikationer.

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 DS 484, 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: Defacement eller web-graffiti, betegner et angreb, hvor websider tagges (overskrives) med angriberens signatur og ofte også et politisk budskab.

DeIC: Danish e-Infrastructure Cooperation (DeIC) blev dannet i april 2012 ved en sammenlægning af Forskningsnettet og Dansk Center for Scientfiic 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 er 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 program 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, på dansk god selskabsledelse, opstod som følge af en række erhvervsskandaler i England og USA og bredte sig op gennem 1990'erne til resten af Europa. God selskabsledelse skal sikre en hensigtsmæssig rolle- og ansvarsfordeling i forbindelse med kontrol og styring af organisationen. Et væsentligt element af god selskabsledelse omhandler risikostyring og revision. It governance er en integreret del af corporate governance, der har til formål at sikre strategisk udnyttelse af brugen af it, således at it både understøtter organisationens effektivitet og medvirker til at udvikle organisationen.

GovCERT: GovCERT-funktionen (Government Computer Emergency Response Team), der i Danmark er placeret under Forsvarsministeriet, 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 it-sikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler.

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: Sammentræning af hack og aktivisme, eller på dansk "politisk motiveret hacking." Det vil sige forfølgelse af politiske mål gennem brugen af midler som defacement, DDoS-angreb, informationstyveri og lignende.

Identitetstyveri: Identitetstyveri betegner brugen 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, der i staten helt skal erstatte brugen af DS 484. 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.

MAM: Mobile Application Management beskriver software, der benyttes til central kontrol og godkendelse af tilgængelige mobil applikationer.

Malware, skadelig kode: Sammentrækning af malicious software eller på dansk ondsindede programmer. Malware er en samlebetegnelse for virus, orme, trojanske heste, keyloggere, spyware, adware, botnetprogrammer og lignende.

Man-in-the-browser: Et angreb relateret til Man-in-the-middle angreb, hvor en trojansk hest kan modificerer websider og indhold af transaktioner uden brugerens viden. Man-in-the-browser funktioner kan være at overtage sessionen til netbanken, overføre penge fra brugerens konto og herefter ændre indholdet i brow-

seren, således at overførelsen ikke fremgår af kontooversigten.

Man-in-the-Middle: En angrebsform, hvor kommunikationen mellem to parter uden parternes vidende, videresendes gennem en mellemmand, der aktivt kan kontrollere kommunikationen. I praksis kan et Man-in-the-middle-angreb for eksempel foregå ved en ændring af DNS-registrering på enten DNS-serveren eller ved ændring af hosts-filen.

MDM: Mobile Device Management er software, der benyttes til centralt 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, som består af en personlig adgangskode og et nøglekort, kan benyttes fra en hvilken som helst computer uden foregående installation af software. 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 kode, 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. Brugen af firewalls vil som udgangspunkt lukke for adgangen til maskinens åbne porte.

Social engineering: Manipulation, der har til formål at få folk til at bidrage med informationer eller at udfører 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: 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 blandt de hidtil mest avancerede orme. Ormen 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.

Trojansk hest: Et program, der har andre, ofte ondartede, funktioner end dem, som det foregiver at have. Trojanske heste indeholder ofte dialer-, bagdørs- eller keylogger-funktionalitet, eller benyttes til installation af virus, botnetprogrammer og lignende. Trojanske heste identificeres ofte af antivirus- og antispywareprogrammer.

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. Virus spredes ofte som mail vedlagt en trojansk hest, der indeholder virussen selv.

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

BEC, 11-11-2013: Nye tal og tendenser i mobilbanken, http://www.bec.dk/bec/presse/nyheder/tal-og-tendenser-i-mobilbanken.aspx?PID=4143&M=NewsV2&Action=1

Betalingsrådet, november 2013: Rapport om nye betalingsløsninger, http://nationalbanken.dk/C1256B730054214F/sysOakFil/Betalingsraadets_rapport_nye_betalingsloesninger_nov2013/$File/Betalingsraadet_Rapport_om_nye_betalingsloesninger.pdf

Center for cybersikkerhed, 9-4-2013: Sådan kan DDoS-angreb imødegås, http://fe-ddis.dk/cfcs/nyheder/arkiv/2013/Pages/S%C3%A5danim%C3%B8deg%C3%A5rduDDoS-angreb.aspx

CSO Online, 07-09-2012: Mobile malware shifting to SMS fraud, http://www.csoonline.com/article/715700/mobile-malware-shifting-to-sms-fraud

Danmarks Statistik, november 2013: It-anvendelse i befolkningen 2013, http://www.dst.dk/pubpdf/18685/itanv

Danske Bank, 4-12-2013: Telefoninterview med Jesper Nielsen, Danske Bank.

Danske Bank, 11-12-2013: Telefoninterview med Peter Kjærgaard Nielsen, Danske Bank.

DIBS, 1-12-2013: Dansk E-handel 2013 - E-handlen boomer fortsat, http://www.dibs.dk/news/dibs-e-handel-2013

DIBS, 3-12-2013: Telefoninterview med Lars Juul Dalsted, DIBS.

DKCERT, 2011: Smartphones – ulven er ankommet, https://www.cert.dk/pdf/indsigtsmartphones.pdf

DKCERT, 16-10-2013: Ny Java giver problemer med NemID, https://www.cert.dk/nyheder/nyheder.shtml?13-10-16-11-27-01

EPN, 29-11-2013: Danskerne shopper løs med mobilen, http://epn.dk/brancher/detail/ECE6293187/danskerne-shopper-loes-med-mobilen/

FireEye, 26-11-2013: Dissecting Android KorBanker, http://www.fireeye.com/blog/technical/targeted-attack/2013/11/dissecting-android-korbanker.html

Kaspersky, Java under attack: Kaspersky Lab Report: Java under attack – the evolution of exploits in 2012-2013, http://www.securelist.com/en/analysis/204792310/Kaspersky_Lab_Report_Java_under_attack_the_evolution_of_exploits_in_2012_2013

Kriminalitet i en digitaliseret verden, 2013: Samlet rapport, Peter Kruize, Det Juridiske Fakultet, Københavns Universitet, http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Kriminalitet%20i%20en%20digitaliseret%20verden%20samlet%20rapport.pdf

Mandiant: APT1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Microsoft Security Intelligence Report, http://www.microsoft.com/security/sir/default.aspx

NemID, 2-7-2013: NemID i ny og mere mobil udgave på vej, https://www.nemid.nu/dk-da/om_nemid/videreudvikling_af_nemid/nemid_til_mobile_platforme/

Nets, 22-8-2013: Nets indgår aftaler om udviklingen af fremtidens mobilbetaling, http://www.nets.eu/dk-da/Om/nyheder-og-presse/Pages/Nets-indg%C3%A5r-aftaler-om-udviklingen-af-fremtidens-mobilbetaling.aspx

Nets, 26-11-2013: Mail med besvarelse af spørgsmål stillet af DKCERT om Mobilpenge og andre løsninger til mobilbetaling.

NSS 11-12-2013: NSS Labs: View From the Precipice - Mobile Financial Malware, https://www.nsslabs.com/reports/view-precipice-mobile-financial-malware

NVD Statistics: National Vulnerability Database CVE Statistics, http://web.nvd.nist.gov/view/vuln/statistics

PCI DSS: PCI Security Standards Council, https://www.pcisecuritystandards.org/

Symantec november 2013: Symantec Intelligence Report, november 2013, http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_11-2013.en-us.pdf

Version2, 8-1-2014: Dokumentation: CSC overså kritiske opdateringer til politiets mainframe i tre måneder, www.version2.dk/55656

Wikipedia: Global surveillance disclosures (2013–present), http://en.wikipedia.org/wiki/2013_Global_surveillance_disclosure

Wikipedia, ISO 27001: ISO/IEC 27001:2013, http://en.wikipedia.org/wiki/ISO/IEC_27001:2013

Zone-H: Zone-H Archive, http://zone-h.org/archive