DK•CERT

Trendrapport 2011

It-kriminalitet og sikkerhed i året der gik

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Jens Borup Pedersen og Tonny Bjørn, DK•CERT

Grafisk arbejde: Kirsten Tobine Hougaard, UNI•C

Foto: colourbox.com

ISBN 978-878703673-3

Om DK•CERT

Det er DK•CERTs mission at skabe øget fokus på informationssikkerhed ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DK•CERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DK•CERT 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 DK•CERT til at udvikle services, der skaber merværdi for DK•CERTs kunder og øvrige interessenter og sætter dem i stand til bedre at sikre deres it-systemer.

DK•CERT, 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.

DK•CERT 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 DK•CERT om informationssikkerhed i Danmark.

DK•CERT samarbejder med GovCERT (Government Computer Emergency Response Team), der er den danske stats internetvarslingstjeneste. DK•CERT bidrager med information rettet mod borgerne og mindre virksomheder om aktuelle trusler og sikkerhedshændelser.

Forord

"Temaet for DK•CERTs Trendrapport 2011 er: "Har vi råd til ikke at samarbejde?" Mit svar er et klart nej! "

Konkurrence er en god ting. Men når konkurrence direkte medfører dårlig sikkerhed, er der noget galt.

Det ser jeg desværre flere eksempler på i mit virke som chef for DK•CERT. Visse sikkerhedsfirmaer går så meget op i at være først ude med nyheden om et nyt angreb, at de ikke deler informationen – hverken med os eller med deres kommercielle konkurrenter.

På internationalt plan findes der ellers et forbilledligt samarbejde. Det handler om skadelige programmer: Når en ny trussel dukker op, er antivirusfirmaerne flinke til at sende programkoden til hinanden, så de alle kan sørge for, at deres kunder er beskyttet. Men her i landet er det flere gange sket, at vi først hører om et nyt angreb, når vi læser om det i pressen.

Det kan selvfølgelig give god mening på kort sigt for det sikkerhedsfirma, der får medieomtalen. Men på langt sigt er den slags egoisme dårlig for dem selv og deres kunder: Hvis vi alle holder kortene tæt ind til kroppen, kommer de heller ikke til at høre om, hvad vi og de andre i branchen observerer. Derved bliver det samlede trusselsbillede mindre dækkende. Den udvikling vil jeg ikke støtte.

Jeg opfordrer derfor alle firmaer og andre interessenter til åbent at dele information om nye sikkerhedshændelser med DK•CERT og resten af sikkerhedsbranchen. Vi har ikke råd til at lade være.

Danmark er velsignet med en række af råd og udvalg, der beskæftiger sig med it-sikkerhed. De har hver deres indgang til området. Det er fint. Men det er mindre godt, når de ikke taler sammen. Et råd gik for eksempel ud med en sikkerhedsadvarsel i medierne, hvor det viste sig, at de ikke havde styr på det tekniske indhold. Det kunne de have undgået, hvis de havde samarbejdet med specialister med viden om emnet.

Så jeg opfordrer også alle råd og udvalg inden for it-sikkerhed til at samarbejde åbent og konstruktivt.

Godt samarbejde fører til konkrete resultater. I Danmark er internetudbyderne rigtig gode til at samarbejde om it-sikkerhed. Det sker i regi af ISP-sikkerhedsforum. I 2011 udvidede vi samarbejdet til også at omfatte en koordineret bekæmpelse af botnet – i øvrigt i samarbejde med GovCERT.

På et mere overordnet plan efterlyser jeg en national it-strategi, der omfatter både det offentlige, det private erhvervsliv og borgerne. En vigtig del af det samarbejde bliver at udvikle en strategi for informationssikkerhed. Læs mere i afsnittet med anbefalinger til beslutningstagere.

Temaet for DK•CERTs Trendrapport 2011 er: "Har vi råd til ikke at samarbejde?" Mit svar er et klart nej! God fornøjelse med læsningen.

Shehzad Ahmad, chef for DK•CERT

Indholdsfortegnelse

1. Resume

For første gang siden 2007 steg antallet af sikkerhedshændelser i 2011. Vi registrerede 44.829 sikkerhedshændelser, hvilket er en stigning på 25 procent i forhold til 2010. Det skyldes flere hændelser, der blev kategoriseret som scanninger, brute force-angreb, malware og phishing.

I 2011 var der dobbelt så mange malware- eller phishing-sider i forhold til 2010. Ved et avanceret phishing-angreb mistede otte af Nordeas netbank-kunder i alt 62.400 kr. De blev ledt til en phishing-side, hvor man omgik sikkerheden i NemID i form af et man-in-the-middle-angreb.

Igen i 2011 var der en stigning i mængden af ny malware der var rettet mod flere platforme, og undgik detektering af antimalware-softwaren. Trojanske heste udgjorde den største andel. De blev spredt som e-mails, over sociale medier og ved hjælp af kompromitterede hjemmesider.

Den samlede mængde af spam-mail faldt herhjemme fra 80 procent til under 70 procent i slutningen af året. Det kan hænge sammen med, at flere spam-botnet er blevet lukket. Modsat steg andelen af phishing-mails i samme periode.

Der blev i 2011 offentliggjort færre CVE-nummererede sårbarheder. Det skal måles op mod, at der blev offentliggjort flere exploits, der udnyttede sårbarhederne. For at imødegå dette indførte vi nye procedurer og værktøjer til scanning af vores kunders it-systemer.

I 2011 scannede DK•CERT 50.000 forskellige IP-adresser på Forskningsnettet. Af dem svarede 3.200, hvoraf 735 havde sårbarheder. Med Anonymous-bevægelsens trusler mod blandt andet danske universiteter, er det positivt, at andelen af sårbare IP-adresser er faldet.

Blandt de væsentligste tendenser for informationssikkerhed i 2011 var:

- En eksplosion i aktivitet, der relaterer sig til hacktivisme.
- Avanceret malware ramte alle platforme, benyttede stjålne certifikater og undgik sikkerhedssoftwaren.

For de kommende år forventer vi, at udviklingen vil være præget af:

- Stigende hacktivisme, som vil have danske organisationer i fokus.
- Mere brug af informationer om medarbejderne til målrettede angreb.
- Malware som er målrettet den enkelte organisation og dennes systemer.

Rapportens konklusioner medfører udfordringer for hele samfundet. Nogle kan løses teknisk og ved kommunikation og samarbejde. Men overordnet set mener vi, at der mangler faste rammer for, i hvilken retning vi ønsker at trække udviklingen af informationssamfundet.

Med EU-formandskabet er der fokus på Danmark. Set i lyset af Anonymous-bevægelsens trusler mod danske interesser, springer det i øjnene, at vi ikke har en national it-strategi, som omfatter informationssikkerhed for både det offentlige, erhvervslivet og borgerne.

2. Indledning

Vi har i år valgt at ændre strukturen på vores årlige Trendrapport, så den i højere grad afspejler hele årets begivenheder. Herved gives et samlet kronologisk overblik over de væsentlige historier i 2011. Du kan derfor i afsnit 9–11 læse eller genlæse artikler fra årets tre første kvartalsvise Trendrapporter.

Vi indleder årets trendrapport med at beskrive internetkriminalitetens udvikling, som vi kan måle den fra vores data. At internetkriminalitet er et problem, vi i stigende grad både som samfund, organisationer og borgere bliver nødt til at forholde os til, skitseres ved nedenstående citat fra Interpols fakta-blad om emnet:

"Cybercrime is one of the fastest growing areas of crime, as more and more criminals exploit the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of crimes."

At truslen er nærværende understreges af en undersøgelse foretaget af sikkerhedsfirmaet Symantecs Norton-division. Den viser, at 27 procent af danskerne har været udsat for internetkriminalitet mod 11 procent i den virkelige verden. Tallene siger dermed, at chancen for at blive ramt af internetkriminalitet er 2,5 gange større.

Det er den virkelighed vi forsøger at skitsere i rapportens afsnit 3. Her tager vi udgangspunkt i tal og statistikker fra 2011, som primært dækker hændelser på de netværk, som DK•CERT overvåger. Afsnittet er suppleret og perspektiveret med eksterne data og statistikker, hvorfor vi mener, at konklusionerne er dækkende for udviklingen på hele den danske del af internettet.

I afsnit 4 samler vi op på nogle af de historier, vi fandt væsentlige i fjerde kvartal 2011. Her kan du læse om forskellige forsøg på svindel, fremkomsten af et nyt botnet, yderliggående politiske fraktioner, som i stigende grad benytter sig af teknologiens gråzoner, samt nogle af de risici, som overskygges af teknologiens nye muligheder. Afsnittet skal ses i relation til historierne fra de tre øvrige kvartaler.

Rapportens afsnit 5 giver opsummerende refleksioner over den udvikling, vi har set i 2011. Refleksioner som peger fremad og er med til at tegne de udfordringer, vi i fremtiden står over for, når det handler om informationssikkerhed.

Vi har herefter ladet en række eksterne parter beskrive deres perspektiv på informationssikkerhed i året der gik og årene der kommer. Du kan her læse, hvordan internetudbyderen (Forskningsnettet) og kunden (Københavns Universitet) betragter de udfordringer, de står over for når det drejer sig om informationssikkerhed. Til sidst i afsnittet har vi givet ordet til den hedengangne IT & Telestyrelse, som i sin tid søsatte NemID-løsningen.

Det efterfølgende afsnit bruger vi til at samle op på rapportens delkonklusioner. Det gør vi ved at liste de vigtigste tendenser for året der gik og de tendenser, som vil præge informationssikkerhedsarbejdet de kommende år. Vi forsøger her, at åbne perspektivet på de udfordringer, trusselsbilledet og brugen af ny teknologi i fremtiden vil afstedkomme.

Det er vores håb at du vil finde det efterfølgende afsnits anbefalinger til

henholdsvis borgerne, organisationerne og beslutningstagerne brugbare. I modsætning til tidligere år har vi holdt os til 10 anbefalinger til hver gruppe.

Selv om det primært er truslerne, der har denne rapports fokus, har erfaringen vist, at vi i samarbejde kan minimere dem. Eller som lederen og talsmanden for vores irske søsterorganisation IRISS-CERT, Brian Honan, den 23. november udtalte på organisationens konference i Dublin:

"*We can no longer afford to treat information security as an afterthought and need to ensure we take the appropriate steps to secure our systems. Criminals are sharing information and working together so they can exploit our systems and steal our money. Businesses need to better share information with the community so we all can learn.*"

Spørgsmålet er derfor, om vi har råd til ikke at samarbejde.

Interpol, 2011; "*Cybercrime fact sheet*".
Scmagazineuk.com; "*IRISSCERT conference kicks off, as statistics reveal level of cyber crime against Irish websites*".
Symantec, 2011; "*Nortons rapport om cyberkriminalitet 2011*".

3. 2011 - året i tal

Nærværende afsnit beskriver året 2011 med baggrund i de tal og statistikker, som er tilgængelige for DK•CERT. Fokus er vores forretning og de data, som herved er tilgængelige for os i rollen som CERT (Computer Emergency Response Team) for UNI•C og Forskningsnettet. De er suppleret og/eller perspektiveret med data fra internettets åbne kilder, så afsnittet afspejler udviklingen på hele det danske internet i 2011. Et år, som internationalt var præget af store sager om tyveri og lækage af data fra myndigheder og internationale virksomheder.

Vi indleder afsnittet med en generel fortælling om de sikkerhedshændelser, der i 2011 blev indrapporteret, og de tendenser tallene afspejler.

Herefter dykker vi ned i tallene og kigger frem. Vi beskriver udviklingen af de trusler, som i årets løb ramte danskerne. Trusler, som hvad enten det drejer sig om spam, phishing eller andet, stort set alle er relateret til malware (skadelig software). Det vil sige den malware, som i 2011 så dagens lys, samt data vedrørende spam og phishing. En fælles tendens er, at malware også i 2011 blev mere målrettet og avanceret i både mål og midler. Perspektivet er ikke kun dansk, da udviklingen internationalt i høj grad præger det som vi oplever herhjemme.

Vi afslutter med fortællingen om de sårbarheder, som blev offentliggjort i 2011, samt de sårbarheder, vi fandt ved scanning af vores kunders systemer. Vi ser også til dels på de sårbarheder, som blev udnyttet i året der gik.

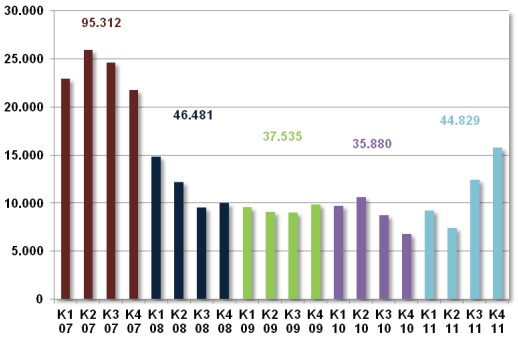
3.1. Årets sikkerhedshændelser

Medens antallet af sikkerhedshændelser rapporteret til DK•CERT har været faldende siden 2007, steg det i 2011. I alt medførte 48.501 henvendelser, angående 25.820 forskellige IP-adresser, registrering af 44.829 unikke sikkerhedshændelser (Figur 1). Det er en stigning på 25 procent i forhold til 2010. Stigningen skyldes primært mange sikkerhedshændelser i årets to sidste kvartaler.

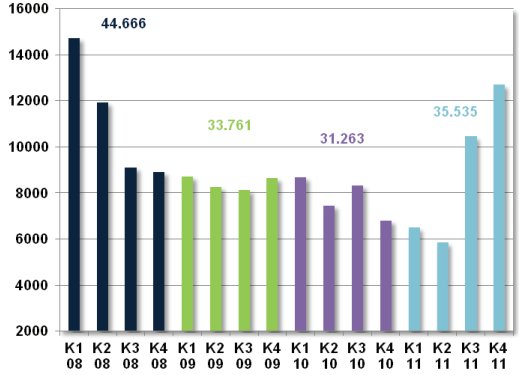
Graver vi os ned i tallene for 2011, udgør rapporteringer om scanninger det største problem. I alt registrerede vi 35.535 hændelser, der blev klassificeret som scanninger, mod 31.263 i 2010 (Figur 2). Årsagen til stigningen skal igen findes i årets to sidste kvartaler. Der er ikke nogen umiddelbar forklaring på dette, da størstedelen af hændelserne er automatiserede rapporteringer fra samme kilder, som har rapporteret denne type hændelser gennem de seneste år. De registrerede scanninger blev sidste år foretaget fra i alt 15.396 forskellige IP-adresser placeret i det meste af verden.

Ser vi bort fra de sidste kvartaler af 2011, har der siden registreringen af 94.647 scanninger i 2007 været et generelt fald i den type hændelser. En årsag kan være, at kompromittering af it-systemer nu foregår med midler, der er mere effektive og vanskeligere at opdage og afværge. Hvor målet for eksempel er at finde sårbare webapplikationer, som kan udnyttes til spredning af malware eller phishing, vil en målrettet søgning på Google ofte kunne løse opgaven, uden at man på netværket eller den afsøgte host vil kunne se det.

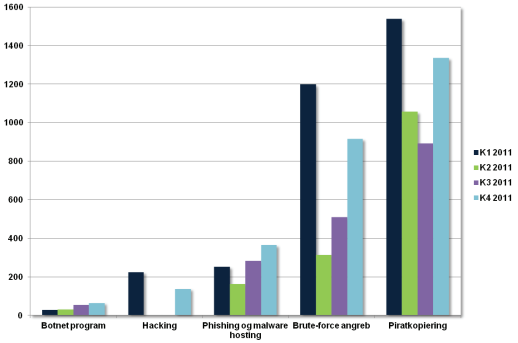
Også henvendelser angående krænkelse af ophavsretten til film, musik og software fyldte meget i statistikken (Figur 3). I 2011 registrerede vi således registrerede



Figur 1. Kvartalsvise antal registrerede sikkerhedshændelser.



Figur 2. Kvartalsvise antal registrerede scanninger.



Figur 3. Væsentligste registrerede hændelsestyper.

4.824 hændelser om piratkopiering, primært fra IP-adresser placeret på Forskningsnettet. I alle tilfælde var der tale om download af enkeltstående værker fra fildelingstjenester, som blev overvåget af repræsentanter for rettighedshaverne.

Piratsoftware udgør ikke blot et brud på kunsternes rettigheder,- men også et brud på organisationens informationssikkerhedspolitik. For eksempel er det en væsentlig kilde til spredning af malware. Det er således ikke kun et ophavsretsligt problem, men også en informationssikkerhedsmæssig problemstilling.

Herefter udgjorde hændelser, der blev kategoriseret som henholdsvis brute-force-angreb og websteder, der hostede phishing-sider eller malware, de største problemer. Også for de kategorier har vi i fjerde kvartal registreret en stigning.

I 2011 registrerede vi 1.068 hændelser om danske websites, der var blevet kompromitteret og herefter benyttet til hosting af både phishing-sider og malware. Størstedelen af var placeret på webhoteller hos hosting-selskaber, men også virksomhedernes egne webservere blev kompromitteret og udnyttet.

De 2.942 brute-force-angreb, der i 2011 blev rapporteret til DK•CERT, var primært rettet mod tjenester, der benyttede TCP-port 22 og 25. Det vil sige SSH-tjenester (Secure Shell) og mailsystemer. Formålet med de angreb er at skaffe sig adgang til enten et system, som kan benyttes til yderligere kompromittering, eller en valid mailkonto, der kan benyttes i forbindelse med afpresning, spam, phishing eller lignende.

En væsentlig tendens for 2011 er en stigning i antallet af rapporteringer om danske computere, som var inficeret med botnet-programmer. Selvom kampen mod botnet gennem de seneste år er intensiveret, oplevede vi en stigning fra 30 rapporteringer i første kvartal til 66 i fjerde kvartal. Det udgør en stigning på 120 procent.

3.2. Malware og andre trusler

Malware i alle afskygninger benyttes ved stort set alle former for internetkriminalitet og udgør det væsentligste problem for vores sikkerhed på internettet.

Kritikken af NemID-løsningen var sidst på året fremtrædende i medierne. Det var dog kun til dels løsningens udformning og kvalitet, der var årsag til, at otte Nordea-kunder i september fik tømt deres netbankkonti for i alt 62.400 kr. Her var der tale om et phishing-angreb, der ledte kunderne til en hjemmeside, hvor transaktionerne blev udført som et man-in-the-middle-angreb. Både e-mails og hjemmeside var udført på fejlfrit dansk og med brug af Nordeas grafik.

Historien afspejler, hvordan brugen af avanceret malware bliver mere professionel og målrettet. Det gjorde sig også gældende for det skadelige program Duqu, som af mange blev kaldt efterfølgeren til Stuxnet. Duqu havde mange lighedspunkter med Stuxnet, og man mente, at det var sandsynligt, at udviklerne havde haft adgang til den oprindelige Stuxnet-kode. I modsætning til Stuxnet var antallet af computere, som blev inficeret dog få.

Duqu benyttede sig af samme kryptering som Stuxnet, og dele af programmet blev signeret med stjålne certifikater. Programmet, som blandt andet intallerede en

bagdør til det inficerede system, blev kun observeret i forbindelse med målrettede angreb. Her blev programmet installeret via et Word-dokument, der udnyttede en hidtil ukendt sårbarhed i Windows.

Siden 2010 har flere malware-varianter benyttet sig af stjålne certifikater for at få øgede privilegier på det inficerede system. Blandt eksemplerne på det var Qbot og Duqu samt den trojanske hest ZXshell. Det har skabt et behov og marked for gyldige certifikater, som malwaren ofte også er designet til at stjæle.

Set over året mener vi, at stjålne certifikater udgør en ny tendens for malware. Forklaringen er enkel. Ved et benytte et certifikat, som systemet har tillid til, kan man på tværs af platforme skaffe sig øgede privilegier uden at benytte specifikke sårbarheder og exploits. Eller som antivirusproducenten AVG skriver som konklusion i deres rapport over malware-trusler i andet kvartal:

"Stealing the keys to the house becomes easier than breaking the windows."

Som tidligere var det også i 2011 trojanske heste, der udgjorde den største malware-trussel (Figur 4). I forhold til 2010 er den væsentligste forskydning, at det for F-Secure ikke var muligt at kategorisere 20,7 procent af den malware, som blev identificeret på danskernes computere. Det har betydet, at andelen af trojanske heste, som blev identificeret, var 10 procent mindre end i 2010.

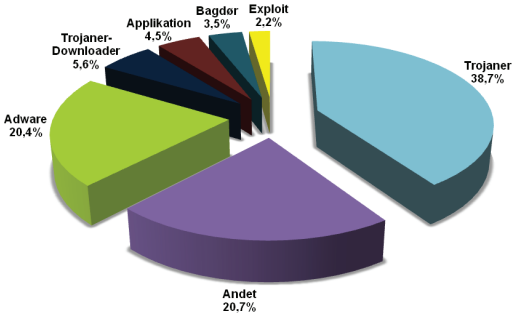
I første halvdel af året havde brugerne således selv foretaget handlinger, som medførte inficering af deres computer. Således var næsten 45 procent af de malware-varianter, der i starten af året blev identificeret af Microsofts værktøj til fjernelse af skadelig software (MSRT), af en type der krævede bruger-interaktion. De hyppigst benyttede exploits var rettet mod Java Runtime Environment (JRE) og Java Virtual Machine (JVM).

Antallet af nye malware-varianter til både traditionelle pc'er og mobile platforme steg i løbet af året. I tredje kvartal var Android-platformen ifølge antivirusproducenten McAfee malware-producenternes foretrukne mål. Det skyldes en udvikling i både udbredelse og brug af mobile platforme, samt at åbenheden i Android Market gør det muligt at distribuere malware gennem en kanal, som brugerne har tillid til.

Det har medført en genopstandelse af dialer-programmer, som ellers uddøde med telefonmodemmet. Denne gang sender de overtakserede SMS'er fra det inficerede system, som tilfældet var for de trojanske heste Wapaxy, LoveTrp og HippoSMS. Der har dog også været eksempler på Android-malware, der havde til formål at indsamle personlige data fra telefonen, som siden kunne benyttes til for eksempel identitetstyveri eller målretning af phishing-angreb.

Når antallet af nye malware-varianter stiger, afspejler det Ovids berømte citat,- den lever godt, der lever skjult (bene vixit, qui bene latuit). Udviklerne af malware har ikke en interesse i, at deres kode bliver opdaget. Det har afledt en forretning for cloudbaserede scannerfarme, hvor utallige mutationer af samme malware scannes med de gængse antimalware-produkter. Resultatet er en stigende mængde malware-varianter, som når de frigives i mange mindre, men til gengæld mere målrettede angreb, næsten er usynlige for scanneren. Når malwaren tillige benytter sig af sårbarheder, som endnu ikke er offentliggjort, er resultaterne skræmmende.

Også de sociale netværkssteder havde de internetkriminelles fokus. Ved et angreb i august forsøgte e-mails med falske venne-anmodninger til Facebook, at få



Figur 4. Danske malware-infektioner i de første tre kvartaler af 2011.

modtagerne til at installere en trojansk hest. Senere spredte en Facebook "synes-godt-om-kampagne" sig i september med titler som:

- *"The first 50.000 participants Get an iPhone 4 for free"*.
- *"The first 25,000 that signup get a free pair of Beats by Dre headphones"*.
- *"The first 1,000 participants Will Get An Facebook Phone for Free"*.
- *"The first 25,000 Participants Will Get A Free Facebook Hoodie"*.

Ifølge Symantecs rapporter for januar til november 2011 faldt andelen af spam-mails, som blev sendt til danskerne. Hvor spam i starten af 2011 udgjorde cirka 80 procent af alle mails, udgjorde de i november måned under 70 procent (Figur 5). Det skal ses i forhold til, at samme tal for 2010 var på mere end 90 procent. I tillæg hertil kommer dog spam, som spredes via for eksempel de sociale medier.

De seneste års lukning af flere spam-botnet er en mulig årsag til et fald i antallet af spam mails. Det har dog også medført et skift i spammernes taktik. I stigende grad benytter de kompromitterede e-mail-konti. Det gør det vanskeligere at blokere den specifikke IP-adresse, hvorfra e-mailen er afsendt, men byder til gengæld på nogle ulemper for afsenderen:

- Der kan oftest kun udsendes et begrænset antal mails fra den kompromitterede mail-konto.
- Den legitime mail-konto skal kompromitteres først.

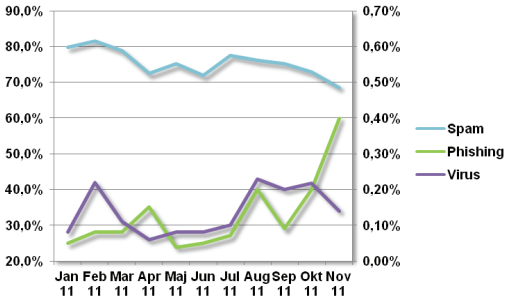
I modsætning til spam har der i 2011 været en stigning i phishing-mails og i bedste fald en stagnation i andelen af virus-mails (Figur 5). Hvor sidstnævnte i løbet af året har svinget mellem 0,06 og 0,22 procent af alle mails, udgjorde phishing-mails i november 0,40 procent.

I 2011 registrerede vi ialt 1.068 hændelser om danskhostede domæner, der lagde lagerplads til phishing-sider eller malware (Figur 6). Det er en væsentlig stigning i forhold til de kun 467 hændelser, vi registrerede i 2010. Som tidligere år var der tale om kompromitterede legale websteder, hvoriblandt der forekom gengangere.

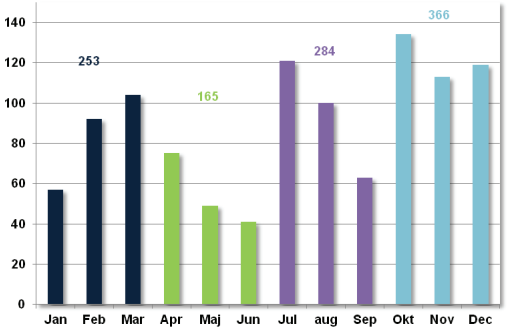
Antallet af henvendelser steg sidst på året. Således registrerede vi i fjerde kvartal 366 hændelser om phishing-sider eller malware placeret på danskhostede domæner mod kun 253 i første kvartal. Den udvikling skal ses i relation til samme periodes stigning i phishing-mails. Årsagen til at phishing-angrebene igen i år steg sidst på året, skal sandsynligvis findes i den øgede nethandel op til julen.

Også antivirusproducenten McAfee registrerede i løbet af året en stigning i websites, som var inficeret med malware. De registrerede ved udgangen af tredje kvartal cirka tre gange så mange aktive URL'er, der indeholdt skadelig kode som i starten af året. I gennemsnit registrerede de i tredje kvartal 3.500 nye malware-inficerede URL'er om dagen, mod 3.000 i kvartalet inden. Drive-by-download var stadig den en væsentlig kilde til malware-inficering.

En tilsvarende global stigning af phishing-angreb blev registreret af Anti Phishing Working Group (APWG). En rapport med data indsamlet i første halvår af 2011 viste 115.472 registrerede angreb fra i alt 79.753 forskellige domæner. Af dem var 14.650 oprettet af dem, som forsøgte at fiske vores data. De øvrige sider var placeret på domæner, som var blevet kompromitteret. 188 af phishing-siderne var placeret på i alt 141 forskellige danske domæner, hvoraf kun et var registreret til formålet.



Figur 5. Danske e-mail trusler i 2011.



Figur 6. Danske websites med phishing-sider og malware registreret i 2011.

På positivsiden faldt den tid, hvor phishing-siderne var aktive, til 54 timer og 37 minutter. Det er stadig lang tid, men man er øjensynlig blevet hurtigere til at reagere hos hostingselskaberne og internetudbyderne.

Generelt viser året en stigende professionalisering af internetkriminaliteten. Malware udnytter sårbarhederne hurtigere, ofte inden de er offentliggjort. Angreb med malware og phishing målrettes brugerne, for eksempel på sociale netværksmedier, hvor links kan skjules med URL-forkortere. Hertil kommer en øget troværdighed i afsendelse og udformning af uønskede mails, som sendes fra vennernes mailkonto. Som phishing-siderne er de skrevet på næsten fejlfrit dansk og med brug af grafik, som øger troværdigheden.

APWG, 2011; "*Global phishing survey: Trends and domain name use in H12011*".
AVG, 2011; "*AVG community powered threat report - Q2 2011*".
Commtouch, 2011; "*Internet threats trend report October 2011*".
Commtouch, 2011; "*The State of hacked accounts October 2011*".
F-secure.com, 2011; "*F-Secure Security Lab - virus world map*".
IBM, 2011; "*IBM X-Force 2011 trend & risk report*".
McAfee, 2011; "*McAfee threats report: Third quarter 2011*".
Microsoft, 2011; "*Microsoft security intelligence report (volume 11)*".
Symantec, 2011; "*Intelligence reports*".

3.3. Sårbarheder

Sårbare it-systemer udgør en væsentlig trussel mod borgernes og organisationernes sikkerhed. Et kompromitteret system benyttes ikke blot til at høste data og informationer fra systemet selv og eventuelt tilknyttede systemer, men også til spredning af malware, upload af phishing-sider, udsendelse af spam og lignende. Et sårbart system kan således være årsag til kompromittering af data på mange andre systemer. Defor er manglende applikations- og systemopdatering en af de væsentligste trusler mod sikkerheden på nettet.

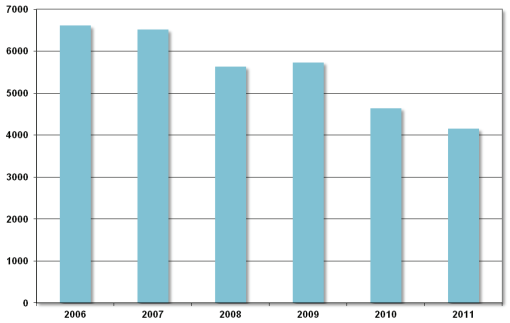
Hurtigere udnyttelse af nye sårbarheder i programmer som for eksempel Adobe Reader, Adobe Flash Player, eller Apples QuickTime er en fortsættelse af tendensen for de sidste år. Sammen med browserne udgør sårbarheder i de programmer i dag den største trussel.

Den amerikanske tjeneste National Vulnerability Database, der samler og katalogiserer CVE-nummererede (Common Vulnerabilities and Exposures) sårbarheder i standard it-systemer, offentliggjorde i 2011 i alt 4.152 nye sårbarheder (Figur 7). Året fortsatte tendensen med stadig færre offentliggørelser af nye sårbarheder i standard-systemer, som har været gældende siden 2006.

Det må ikke tages som udtryk for generelt mere sikre it-systemer. En stigende diversitet i platforme, stadig flere nye it-systemer og software-versioner giver anledning til at tro, at antallet af sårbarheder, der endnu ikke er opdaget og offentliggjort, er flere end nogensinde før. Det vidner flere udnyttelser af sårbarheder, der på angrebstidspunktet endnu ikke var kendte, om.

Problemet er i stigende grad de sårbarheder, som bliver udnyttet inden de bliver kendt. Det samme gælder for sårbarheder i organisationsspecifikke webapplikationer, som ikke offentliggøres med et CVE-nummer.

Det generelle fald kan måske forklares ved mere målrettede angreb. Når målet er



Figur 7. Antal nye CVE-nummererede sårbarheder per år.

en specifik organisation, vil det i stigende grad være sårbarheder i specifikke applikationer, der søges udnyttet. Det kan også forklare et generelt fald i nye websårbarheder, der offentliggøres med et CVE-nummer (Figur 8) på trods af, at legitime webapplikationer er den væsentligste spredningskilde for malware. De største problemer er her manglende inputvalidering og -sanitering, fraværet af udviklingsstandarder og manglende viden om sikkerhed hos programmørerne.

Antallet af sårbarheder af typen cross-site request forgery, path traversal, information leak, SQL injection og cross-site scripting i standard webapplikationer er gennem de seneste år faldet. Fra at udgøre 45 procent af alle sårbarheder, der blev publiceret med et CVE-nummer i 2008, udgjorde de i 2011 kun 29 procent. Eneste undtagelse er sårbarheder af typen information leak/disclosure. De steg i 2011 med 54 procent, til i alt 297. Om der er en sammenhæng til årets mange angreb, der havde tyveri og offentliggørelse af fortrolige data som formål vides ikke.

SQL-injektion var ifølge IBM den hyppigst udnyttede sårbarhedstype på webapplikationer i første halvdel af 2011, efterfulgt af brute-force-angreb på databaser og Windows-netværksdrev. For de sårbare webapplikationer gjaldt desuden, at 90 procent havde en eller flere sårbarheder, der var introduceret gennem tredjeparts JavaScripts som for eksempel marketing kampagner, inkludering af Flash-animationer og AJAX-biblioteker.

Der blev i 2011 offentliggjort flest nye CVE-nummererede sårbarheder i Google Chrome (Figur 9). Det kan dog ikke tages som udtryk for, at browseren er mere usikker end de øvrige, da der i statistikken ikke er medtaget versionsnummer. Google har i 2011 udgivet otte forskellige versioner af browseren, der opdaterer sig selv. Således var der på et givet tidspunkt kun tre forskellige versioner i brug. Kun få af de offentliggjorte sårbarheder har således været i de aktuelle versioner.

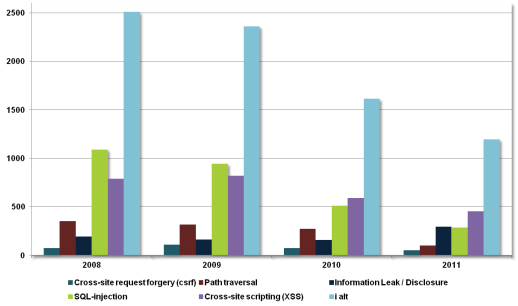
Derudover er det Microsofts forskellige versioner af Windows og Apples styresystem Mac OS X, der præger listen over de systemer, hvortil der i 2011 blev offentliggjort flest CVE-nummererede sårbarheder. Ny på listen er Apples iTunes. Lige efter Adobe Flash finder vi med henholdsvis 63 og 60 sårbarheder Adobe Reader og Adobe Acrobat.

Også til de mobile platforme blev der sidste år offentliggjort nye CVE-nummererede sårbarheder, om end antallet her var mere beskedent. Til Apples operativsystem iOS til iPhone og iPad blev der offentliggjort 35 sårbarheder, mens tallet for Googles Android-operativsystem var 14.

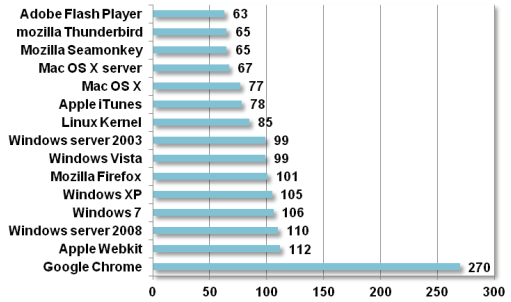
DK•CERT udførte i 2011 scanning mod næsten 50.000 forskellige IP-adresser på Forskningsnettet. Her var 3.211 eller små 7 procent af de scannede adresser på scanningstidspunktet tilgængelige på en eller flere porte. 735 af dem havde i gennemsnit ni CVE-nummererede sårbarheder. I forhold til sidste år konstaterede vi i år færre sårbare IP-adresser og under halvt så mange sårbarheder.

I alt konstaterede vi CVE-nummererede sårbarheder på 39 forskellige porte og/eller protokoller. I forhold til tidligere år optræder der nu flere sårbarheder på UDP-protokollen. Årsagen til dette skal primært findes i, at vi i 2011 supplerede vores scanningsværktøjer med en initierende afsøgning af åbne porte og/eller protokoller. Vi tog også et nyt scanningsværktøj i brug.

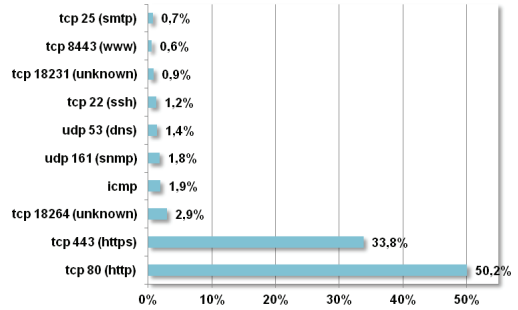
Flest sårbarheder blev der igen i år konstateret på webapplikationer, der lytter på henholdsvis TCP-port 80 og 443 (Figur 10). Webapplikationerne stod for 84 procent af alle konstaterede CVE-nummererede sårbarheder. Derudover fordelte



Figur 8. Antal nye CVE-nummererede websårbarheder per år.



Figur 9. Nye CVE-nummererede produktsårbarheder.



Figur 10. Hyppigste sårbare porte konstateret ved scanning.

sårbarhederne sig på et bredt spekter af porte og/eller protokoller. Mest bemærkelsesværdigt var TCP-port 18231 og 18264, som tilsammen udgjorde 3,8 procent af de fundne sårbarheder. De knytter sig til henholdsvis krypteringen af VPN-forbindelser og portnummeradressering på CheckPoint-firewalls.

Sårbarhederne på UDP-port 161 knytter sig til SNMP-protokollen, der som udgangspunkt bør være blokeret fra organisationens yderside.

I løbet af året blev der offentliggjort sårbarheder i en bred vifte af produkter rettet mod organisationer og forbrugere. De væsentligste knytter sig til browseren eller plugins til den. Flere sårbarheder blev set udnyttet i året der gik. De kan potentielt ramme på tværs af platforme. Særligt exploits (angrebskode), som udnyttede sårbarheder i Java, var hyppige i 2011. De stod ifølge Microsoft for et sted mellem en tredjedel og halvdelen af alle exploits, der blev observeret i starten af året.

Den 16. februar 2011 offentliggjordes sårbarheden CVE-2011-0654, der gør det muligt at udføre Denial of Service-angreb eller fjernovertage sårbare Windows-systemer. Sårbarheden findes i alle versioner af Windows og blev vurderet som kritisk. Kort efter offentliggørelsen af sårbarheden blev der publiceret skadelig kode, der udnytter den.

Den 14. marts 2011 udsendte Adobe en sikkerhedsbulletin angående en kritisk sårbarhed i Flash Player, Acrobat og Adobe Reader. Den blev set udnyttet gennem en skadelig Flash-fil (.swf) indlejret i et Microsoft Excel-dokument. Sårbarheden er tilgængelig på alle gængse operativsystemer og kan udnyttes til Denial of Service-angreb eller fjernkontrol af det sårbare system. Sårbarheden blev dagen efter registreret med CVE-nummer (CVE-2011-0609). Adobe udgav siden opdaterede versioner af deres programmer.

Blandt andet kvartals udnyttede sårbarheder var desuden en sårbarheder i Flash Player, Acrobat og Adobe Reader. Sårbarheden (CVE-2011-0611) blev offentliggjort i april og blev kategoriseret som kritisk. Der blev inden offentliggørelsen fundet exploits til sårbarheden, der potentielt kan udnyttes på flere platforme.

Den 14. juni udgav Adobe en opdatering til Adobe Reader og Acrobat. Den rettede 13 CVE-nummererede kritiske sårbarheder, som var blevet offentliggjort tidligere i 2011. Sårbarhederne kunne udnyttes på både Windows- og Macintosh-computere.

Også Microsoft måtte i juni måned frigive en opdatering, som rettede kritiske CVE-nummererede sårbarheder. Den 15. juni kom der en rettelse til Internet Explorer for versionerne til og med 9. Den rettede otte sårbarheder, der kunne medføre kodeeksekvering, og tre sårbarheder som kunne resultere i informationslækage.

Apple udsendte den 23. juni en sikkerhedsopdatering, som rettede 39 unikke CVE-nummererede sårbarheder i forskellige dele af Mac OS X. Flere af sårbarhederne blev kategoriseret som kritiske, og man anbefalede brugerne at installere opdateringerne hurtigst muligt.

Den 9. august udgav Microsoft en opdatering til Internet Explorer (MS11-057), som rettede syv CVE-nummererede sårbarheder i version 6 til 9 på forskellige Windows-platforme. Blandt sårbarhederne blev to kategoriseret som kritiske. Sårbarhederne CVE-2011-1963 og CVE-2011-1964 kan medføre eksekvering af kode ved besøg på hjemmesider, der udnytter fejl i browserens håndtering af hukommelse.

Adobe udsendte den 9. august en opdatering (APSB11-21), som rettede i alt 14 CVE-nummererede sårbarheder rettet mod Windows, Macintosh, Linux, Solaris og

Android. Sårbarhederne er tilgængelige i Flash-Player versionerne tidligere end 10.3.183.5 og kan potentielt medføre, at en angriber får fuld kontrol over det angrebne system.

Mozilla udgav den 16. august Firefox 6. Samtidig med udgivelsen publicerede man en advisory (MFSA 2011-29), der redegjorde for 10 CVE-nummererede sårbarheder, som var rettet i den nye version af browseren. De otte blev kategoriseret som kritiske. Sårbarhederne var tilgængelige i de fleste tidligere versioner af Firefox og var alle blevet offentliggjort den 9. juli. Sårbarhederne kan medføre Denial of Service samt eksekvering af kode via fejl i forskellige dele af programmet.

Den 13. september udsendte Adobe en kvartalsopdatering (APSB11-24) til Adobe Reader og Acrobat. Den retter 13 kritiske CVE-nummererede sårbarheder i ældre versioner af Adobe Reader til Windows, Macintosh, Unix og Linux. Sårbarhederne kan medføre Denial of Service samt eksekvering af kode ved hjælp af hjemmesider, som udnytter sårbarhederne.

Igen den 21. september udsendte Adobe en opdatering til Flash Player (APSB11-26), som rettede flere kritiske sårbarheder. I alt rettede opdateringen seks CVE-nummererede sårbarheder, hvoraf en cross-site scripting-sårbarhed på daværende tidspunkt var set udnyttet (CVE-2011-2444) til at narre brugere til sider inficeret med ondsindet kode. Sårbarhederne er tilgængelige på flere versioner af Flash Player til Windows, Mac OS X, Linux, Solaris og Android og muliggør blandt andet eksekvering af kode.

En kritisk 0-dags sårbarhed (CVE-2011-2462) i Acrobat og Adobe Reader fik den 6. december Adobe til at udsende en sikkerheds advarsel (ASPA11-04). Sårbarheden var blevet set udnyttet til spear phishing (phishing målrettet enkeltpersoner) gennem et særligt udformet PDF-dokument sendt til medarbejdere i internationale virksomheder. Sårbarheden, der var tilgængelig på både Windows, Macintosh og UNIX, kunne medføre denial of service og kontrol med det sårbare system.

Den 13. december frigav Microsoft 13 sikkerhedsbulletiner (MS11-087 – MS11-099) vedrørende opdatering af kritiske sårbarheder i flere af deres produkter og komponenter. Flere af sårbarhederne gjorde det muligt at køre kode på det sårbare system.

Selvom en sårbarhed (CVE-2005-1898) i PHP Thumbs blev rapporteret for mere end fem år siden, blev den stadig udnyttet i 2011.

Adobe, 2011; "*Security advisory for Adobe Flash Player, Adobe Reader and Acrobat*".
Adobe, juni 2011; "*Security updates available for Adobe Reader and Acrobat*".
Adobe, august 2011; "*Security update available for Adobe Flash Player*".
Adobe, september 2011; "*Security update available for Adobe Flash Player*".
Adobe, september 2011; "*Security updates available for Adobe Reader and Acrobat*".
Adobe, december 2011; "*Security Advisory for Adobe Reader and Acrobat*".
Apple, 2011; "*About the security content of Mac OS X v10.6.8 and security update 2011-04*".
Apple, 2011; "*How to avoid or remove Mac Defender malware*".
Commtouch, 2011; "*Internet threats trend report October 2011*".
F-Secure, 2011; "*Internet Explorer cumulative security update*".
IBM, 2011; "*IBM X-Force 2011 trend & risk report*".
Microsoft, 2011; "*Microsoft safety scanner detects exploits du jour*".
Microsoft, 2011; "*Microsoft security bulletin MS11-057 – Critical*".
Microsoft, 2011; "*Microsoft security intelligence report (volume 11)*".
Microsoft, 2011; "*Oversigt over sikkerhedsopdateringer fra Microsoft for december 2011*".
Mozilla, 2011; "*Mozilla foundation security advisory 2011-29*".
nvd.nist.gov; "*National Vulnerability Database version 2.2*".

nvd.nist.gov; "*CVE and CCE statistics query page*".
Vupen, 2011; "*Microsoft Windows SMB "mrxsmb.sys" remote heap overflow vulnerability*".

4. Opsamling på fjerde kvartal

Vi samler her op på de emner og historier som vi fandt væsentlige i fjerde kvartal 2011. Du kan blandt andet læse om, hvordan svindelnumre rettet mod danskerne er blevet mere troværdige og målrettede, og hvordan et nyt botnet pludselig dukkede op i røgen efter Stuxnet for herefter øjensynligt at forsvinde igen.

Gennem året har udbredelsen af ny teknologi og fortrængningen af gammel teknologi budt på både trusler og muligheder for de teknologiinteresserede og os i sikkerhedsbranchen. 2011 blev året, hvor internetopkoblet hjemmeelektronik vandt indpas i de danske hjem. Smart-tv'et bød på nye muligheder for tv seeren, men introducerer samtidig nye risici. Det samme kan siges om HTML5, der langsomt synes at overtage Flash's rolle som den væsentligste platform til visning af video og interaktivt indhold på nettet.

Læs også, hvordan de politiske aktivisters dagsorden har ændret sig, således at hacktivisme nu er blevet et begreb, der inkluderes i trusselsbilledet fra Politiets Efterretningstjeneste, PET, og om de danske hosting selskaber, der i samarbejdets ånd har skabt fælles front for at højne sikkerheden på deres produkter.

Har du behov for det fulde overblik over året der gik, kan du læse eller genlæse vores øvrige artikler fra de tre første kvartaler i afsnit 9, 10 og 11.

4.1. Svindel med dyre kinesiske domænenavne

Nogen forsøger at registrere dit varemærke som kinesisk domæne. Den besked kan få de fleste virksomheder til at reagere. Det er jo trods alt deres varemærke, og hvad vil en kineser med det? Svaret er, at de vil sælge dig dyre, men ubrugelige kinesiske domænenavne.

Hvorfor vil nogen registrere domænet Forskningsnettet.cn? Det var den første tanke, der slog os, da vi midt i oktober modtog en mail fra John, som angiveligt var direktør i den kinesiske virksomhed Ygnetwork Ltd (Figur 11).

I mailen skrev John, at han repræsenterede det kinesiske center for registrering af internetdomæner. Her havde den kinesiske virksomhed Tianhua Ltd ansøgt om registrering af domænerne forskningsnettet.cn, forskningsnettet.com.cn med flere. Som de retmæssige ejere af varemærket Forskningsnettet havde vi dog krav på i en begrænset tidsperiode at registrere domænerne først. Hvis vi ønskede det, skulle den ansvarlige ledelse kontakte Ygnetwork Ltd så hurtigt så muligt. Et besøg på Ygnetworks Ltd hjemmeside (Figur 12) bekræftede umiddelbart Johns historie.

"*Yi Guan Information Technology Co.,Ltd, headquartered in Shanghai, is a leading provider of domain name registration and web hosting services.*"

Problemet er blot, at Ygnetwork Ltd ikke er det kinesiske center for registrering af internetdomæner. De er ikke engang registreret på listen over kinesiske registrarer hos det rigtige kinesiske center for registrering af internetdomæner, China Internet Network Information Center (CNNIC). Ygnetwork Ltd kan således ikke selv registrere domæner under topleveldomænet CN. De skal registreres gennem en tredjepart.

Men hvis Ygnetwork Ltd ikke var, hvad John fortalte os, hvem var de så, og hvad

Fra John <john.pan@yg-networksltd.com>
Emne **Asia/Cn domain name & Internet Keyword** 09:01
Til fsk@cert.dk Flere funktioner

Dear Manager,

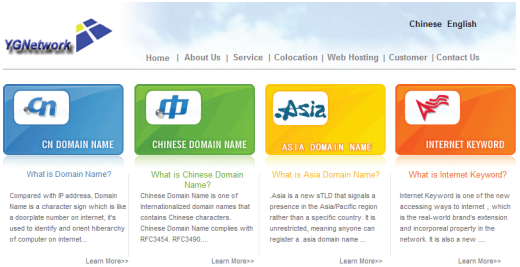
(If you are not the person who is in charge of this, please forward this to your CEO,Thanks)

This email is from China domain name registration center, which mainly deal with the domain name registration and dispute internationally in China and Asia.
On October 10th 2011, We received Tianhua Ltd's application that they are registering the name " forskningsnettet " as their Internet Keyword and " forskningsnettet .cn "、" forskningsnettet .com.cn " 、 " forskningsnettet .asia "domain names etc.., they are China and ASIA domain names. But after auditing we found the brand name been used by your company. As the domain name registrar in China, it is our duty to notice you, so we are sending you this email to check. According to the principle in China, your company is the owner of the trademark, In our auditing time we can keep the domain names safe for you firstly, but our audit period is limited, if you object the third party application these domain names and need to protect the brand in china and Asia by yourself, please let the responsible officer contact us as soon as possible. Thank you!

Best Regards,

John
General Manager
Shanghai Office (Head Office)
3002, Nanhai Building, No. 854 Nandan Road,
Xuhui District, Shanghai 200070, China
Tel: +86 216191 8696
Mobile: +86 136615 29704
Fax: +86 216191 8697
Web: www.ygnetworkltd.com

Figur 11. Mail fra John, direktør i Ygnetwork Ltd.



Figur 12. Domænenavne er det centrale på Ygnetwork Ltds hjemmeside.

var de ude på? En Googlesøgning på ordene ygnetworkltd og fraud gav svaret. Det hele var et svindelnummer, som havde til formål at overbevise modtageren af mailen om, at han skulle registrere domænerne gennem Ygnetwork Ltd. Selvfølgelig til horrible overpriser.

Den direkte henvendelse med brug af informationer om modtagerens forhold er et godt eksempel på social engineering. Når der hertil lægges en troværdigt udseende hjemmeside og et vist tidspres, er det ikke svært at forestille sig, at nogle lader sig narre. Særlig mindre virksomheder, som har eller overvejer at få relationer på det kinesiske marked, er her i farezonen.

Vores bedste råd er, at man blot sletter mailen. Er man i tvivl, kan man eventuelt henvende sig hos DK Hostmaster, som varetager registreringen af danske domæner, eller søge juridisk bistand.

708media.com, 2010; "*SCAM: Asian/China domain name scam*".
Cnnic.net.cn, 2011; "*CNNIC accredited CDN domestic registrars*".
Ygnetworkltd.com; "*About us*".

4.2. Duqu træder i Stuxnets fodspor

Årets mest omtalte skadelige program har kun inficeret ganske få computere. Men to ting gør Duqu spændende: Den ser ud til at være i familie med Stuxnet, og den udnytter en hidtil ukendt sårbarhed.

Duqu er et skadeligt program, der giver angribere en bagdør ind i den computer, det kører på. Formålet er at få fat i fortrolige oplysninger på offerets computer. Duqu er kun observeret i målrettede angreb, hvor bagmændene sendte Word-dokumenter i mail til ofrene. Når Word-dokumentet blev åbnet, udnyttede det en hidtil ukendt sårbarhed i Windows til at installere Duqu-programmet.

Microsoft lukkede sårbarheden den 13. december med en rettelse, som er beskrevet i sikkerhedsbulletin MS11-087. Hullet ligger i Windows› behandling af fonte.

Duqu har flere lighedspunkter med Stuxnet, der angiveligt havde til formål at sabotere det iranske atomprogram. Begge trusler udnytter sårbarheder, der ikke var alment kendte på anvendelsestidspunktet. De bruger også de samme krypteringsnøgler. Elementer i dem begge er signeret digitalt med stjålne certifikater.

Duqu-programmerne kommunikerede med flere forskellige fjernstyringsservere, der alle er lukket ned nu. Duqu blev opdaget i oktober måned. Den 20. oktober gennemførte bagmændene øjensynlig en oprydningsaktion, hvor data blev slettet fra serverne så langt tilbage som til 2009.

Sikkerhedsfirmaet Kaspersky mener, at det er sandsynligt, at udviklerne af Duqu har haft adgang til de samme ressourcer som udviklerne af Stuxnet. Hvis bagmændene er de samme, som stod bag Stuxnet, samler mistanken sig om USA og Israel. Begge lande menes at have været involveret i udvikling og spredning af Stuxnet.

Iran har oplyst, at landet er blevet ramt af Duqu. Det skete i november. Men allerede i april talte Iran om angreb. Programmet herfra blev ikke sendt til

"Duqu har flere lighedspunkter med Stuxnet, der angiveligt havde til formål at sabotere det iranske atomprogram. Begge trusler udnytter sårbarheder, der ikke var alment kendte på anvendelsestidspunktet."

antivirusfirmaer, men Kaspersky finder det sandsynligt, at det var en variant af Duqu. Det første kendte Duqu-angreb stammer også fra april. Stars-navnet kan henvise til, at der indgår et billede af stjernehimlen i et af Duqu-programmerne.

Duqu er et eksempel på de våben, der bruges til målrettede angreb. Dem har der været flere af 2011. Målrettede angreb er rettet mod et nøje udvalgt mål. Det målrettede består for eksempel i, at mailen er sendt til navngivne personer og indeholder firmanavne og andre oplysninger, der får den til at se troværdig ud. Det vides ikke, hvilke firmaer eller myndigheder, Duqu blev brugt til angreb mod.

Kaspersky, 2011; "*Duqu FAQ*".
Kaspersky, 2011; "*The Duqu saga continues: Enter Mr. B. Jason and TV's Dexter*".
Kaspersky, 2011; "*The mystery of Duqu: Part six (The command and control servers)*".
Microsoft, 2011; "*More information on MS11-0872*".

4.3. Telefonsvindlere ringede fra dansk Skype-nummer

Sidst i oktober forsøgte udenlandske svindlere igen telefonisk at lokke danskere til at give dem adgang til pc'en. De hævdede, at den var ramt af virus og tilbød hjælp med at rense den. Denne gang benyttede de et dansk Skype-nummer til at øge troværdigheden af opkaldene.

Fra et dansk Skype-nummer kontaktede engelsktalende svindlere danske borgere telefonisk under påskud af, at deres computer var inficeret med skadelig kode. De påstod at ringe fra en global virksomhed, der repræsenterer Microsoft og overvåger alle Windows-operativsystemer for kritiske inficeringer.

Dette trick var i sig selv ikke nyt. Vi har skrevet om det i vores Trendrapport for tredje kvartal 2011, se også afsnit 11.2, og Microsoft har udsendt deres egen advarsel på et tidligere tidspunkt.

Den seneste drejning var, at de prøvede at legitimere deres svindelforsøg ved at oprette et dansk Skype-telefonnummer, som de gerne udleverer på forlangende. I en aktuel sag var det benyttede telefonnummer 36 96 93 28.

På grund af det danske nummer virkede svindelnummeret meget overbevisende. Men Microsoft vil aldrig ringe til en bruger direkte. Derfor anbefalede DK•CERT på det kraftigste, at man slet og ret afbrød samtalen.

Microsoft, 2011; "*Undvik bedrägeri som använder Microsofts namn*".

4.4. Politisk aktivisme bliver digital

I 2011 gik hacktivisme fra at være forbeholdt de få til at være en udbredt aktionsform på begge politiske yderfløje i både Danmark og udlandet. Internettets anonymitet og tilgængeligheden af værktøjer har betydet, at politiets efterretningstjeneste (PET) har accepteret truslen og sat fokus på elektroniske angreb fra ekstremistiske miljøer.

Hvor internettet i en årrække har været benyttet som rekrutteringsplatform for mennesker, der søgte sandheden på de politiske yderfløje, er det i stigende grad

også blevet midlet til aktion. Den globale bølge af politisk motiverede angreb i 2011, som du kan læse mere om i afsnit 11.4, kan inspirere aktivisterne herhjemme til også at kaste med digitale brosten.

På både den yderste højre- og venstrefløj står den modsatte fløj, statsapparatet og de eksisterende politiske strukturer som de primære mål for deres aktiviteter. Særligt på den politiske venstrefløj, hvor demokratiet i nogle kredse ses som en hindring for anarki, benytter man sig ifølge PET af hacking som metode til indsamling af oplysninger om modstanderen. Her opfatter man statsapparatet som en undertrykkende institution, hvilket understreges af nedenstående citat om Occupy-bevægelsen på Anonymous CPHs hjemmeside:

"Selvom det ER en fredelig bevægelse så kan frygten og ønsket om at styre folket medføre at både politi og militær skal bruges til at tryne medborgerne i Danmark."

Særligt i de venstreekstremistiske miljøer råder man ifølge PET over de fornødne it-kompetencer. Her indgår videndeling og samarbejde omkring omgåelse af blokeringer, anonym færden på nettet med mere i den aktivistiske uddannelse.

Med udbredelsen og tilgængeligheden af værktøjer er der en risiko for, at internettets bekvemmelighed og anonymitet kan gøre hacktivisme attraktivt i et bredere segment, som måske ikke helt forstår hverken midlet, målet eller konsekvensen for og af deres handlinger. Hvis der for eksempel herhjemme kan mobiliseres samme angrebsstyrke som ved DDoS-angrebene mod Mastercard i 2011, kan det udgøre en risiko for virksomhedernes indtjening og/eller vores offentlige digitale infrastrukturer.

I lyset af dette er det PETs opfattelse, at den fremtidige indsats mod politisk ekstremisme, blandt andet skal have fokus på:

"Risikoen for hacking og elektroniske angreb på IT-systemer som led i ekstremistiske aktiviteter."

Anonymous CPH, 2011; *"Hvem ejer Occupy bevægelsen teori og løgn om de få eller mange 99%"*.
Ingeniøren, 2011; *"Eksperter: Dagens aktivister kaster cyberbrosten"*.
Politiets Efterretningstjeneste, 2011; *"PET's indsats i forhold til politisk ekstremisme"*.

4.5. Smart skal det være…

Integrationen af netværksadgang og apps i vores forbrugerelektronik er den forventede evolution. På brugersiden giver det større funktionalitet, men på sikkerhedssiden giver det øget kompleksitet.

Hvis der ikke allerede står et i stuen, så bliver dit næste tv med stor sikkerhed et smart-tv. Computeren og tv'et er for alvor smeltet sammen til det ultimative stuealter - med et overflødighedshorn af muligheder indbygget.

Når nettet skal tilgås, så vil de fleste benytte fjernbetjeningens møjsommelige måde at trykke sig frem til de rette bogstaver for brugernavn, password og adresser. Det er så retro, at man næsten bliver nostalgisk.

Det er lidt bøvlet at logge ind de første gange - men så findes der i mange tilfælde en "husk mig" checkboks - som efterfølgende gør det legende let. Derefter kan

"Med udbredelsen og tilgængeligheden af værktøjer er der en risiko for, at internettets bekvemmelighed og anonymitet kan gøre hacktivisme attraktivt i et bredere segment, som måske ikke helt forstår hverken midlet, målet eller konsekvensen for og af deres handlinger."

man slappe af i sofaen og læse mails, tilgå sociale medier eller spille et spil, medens den lejede online-video hentes.

Der går ikke længe, før alle de tilgængelige apps, der modsvarer de samme services som på ens pc, er afprøvet og sandsynligvis også demonstreret for familie og venner. For det ER smart, at et traditionelt stykke underholdningselektronik tilbyder en ny dimension. Lean Back i sin yderste konsekvens.

Men i kraft af, at vi i det små benytter vores tv på samme måde som computeren, så kommer sikkerhedsaspektet også ind i billedet. Både i forhold til sårbarheder i operativsystemet og i særdeleshed ved håndtering og beskyttelse af personlige oplysninger.

Personlige oplysninger findes nu på ens computer, smartphone, medieafspiller, tablet og smart-tv. Spredningen af sådanne kritiske oplysninger ud over en håndfuld af forskellige teknologier, øger kompleksiteten ganske markant.

Specielt smart-tv'et betragtes endnu som et stykke underholdningselektronik, hvor man ikke skænker det en tanke, at ens information sendes via apps af ukendt oprindelse gennem ukendte netværk blot for at nå ukendte servere. Alt sammen fra en "blackbox" i stuen, der er frit tilgængelig.

Skulle man blive udsat for indbrud, hvor ens smart-tv er en del af rovet, så har tyven adgang til information rettet mod online videoleje, mail, Facebook og Twitter med flere. Hvis ikke tyven selv, så har hæleren, specielt når "husk mig" muligheden benyttes.

Som smart-tv-ejer bør man derfor sætte sig ind i de muligheder, der gives på sikkerhedssiden. Det er hurtigt overstået, for mange producenter har tilsyneladende ikke haft brugeren med i tankerne, da de implementerede menuer rettet mod informationssikkerhed.

Hos de smart-tv producenter, som har givet brugeren en lille smule at arbejde med, skal man søge grundigt, før det findes. Forventer man herefter et interface, der blot tilnærmelsesvis minder om noget, man kender, så skuffes man fælt. Oftest er der kun ét enkelt menupunkt til et så essentielt emne. Aktiveres det, så fjerner man gerne alt relateret til forældrekontrol, adgangskoder, cookies, favoritter og historik.

Hvis producenterne regner med, at man som bruger vil benytte sig af så ugennemtænkte muligheder, så må de tro om igen. Dette er nemlig et lysende eksempel på, hvornår brugeren tager den letteste udvej og benytter usikre muligheder såsom "husk mig". Producenterne må tage deres ansvar alvorligt og stramme op.

Men ud over minimale og ugennemtænkte menupunkter så halter online-opdatering af smart-tv'ets interne software også. I et konkret eksempel bebudede daglige opdateringstjek, at alt var i skønneste orden. Der fandtes ikke ny software. Et manuelt tjek på producentens hjemmeside afslørede dog, at der faktisk fandtes en 73 megabyte opdatering.

Til trods for at både tv'et og brugeren var registreret hos producenten, så kom der ingen notifikation om, at denne opdatering var tilgængelig. Hverken notifikation eller automatisk online-opdatering virkede efter hensigten. Hvis Microsoft eller Apple havde lige så svigtende services i dag, ville det aflede et ramaskrig.

Om smart-tv

Smart-tv er den benævnelse der bruges til at beskrive integrationen af internettet og Web 2.0 funktioner i moderne tv-apparater og settop-bokse. Det beskriver således også den teknologiske konvergens mellem computer og tv. Denne type tv har oftest et lige så stort fokus på online-aktivitet som på den traditionelle tv-funktion.

Et smart-tv har indbygget eget operativsystem, oftest baseret på en Linux-kerne, som fra tid til anden skal opdateres for at rette fejl og sårbarheder eller tilføje ny funktionalitet.

Ved hjælp af apps, kendt fra smartphones, kan brugeren tilføje ny funktionalitet og muligheder. Det kan eksempel være adgang til sociale medier eller video-on-demand løsninger. Disse løsninger kræver oftest, at man benytter personlige oplysninger i forbindelse med login.

"Personlige oplysninger findes nu på ens computer, smartphone, medieafspiller, tablet og smart-tv. Spredningen af sådanne kritiske oplysninger ud over en håndfuld af forskellige teknologier, øger kompleksiteten ganske markant."

For at føje spot til skade faldt dette sammen med, at der kort forinden var frigivet information om to fundne cookie-sårbarheder i Opera-browseren. Det er en skrabet version af denne browser, som flere producenter benytter. Endnu et tjek på producentens hjemmeside afslørede ikke, om den indbyggede browser var berørt af sårbarhederne.

Selvom man ikke kan skære alle producenter over en kam, så er det næsten en deja-vu-oplevelse. Vi skal ikke mange år tilbage, før der var sammenlignelige problemer på en anden platform. Der skal åbenbart "lig på bordet" først, før der gøres noget aktivt.

En yderligere faktor der komplicerer tingene er, at de forskellige producenter tilsyneladende har hver deres platform med egne apps, brugergrænseflade og ikke mindst system til sikkerhedsopdateringer. Da det ikke er ualmindeligt at have mere end ét tv i hjemmet, skal man som forbruger holde tungen lige i munden.

Nu ønsker vi ikke at afskrække nogen fra at købe et smart-tv. Vi vil blot sætte fokus på, at producenterne har et ansvar, når deres elektronik kan tilsluttes internettet, opbevare og sende personlige informationer samt kan tilgå andre enheder på hjemmenetværket.

4.6. HTML5 - den grimme ælling

Web-grænseflader bliver til stadighed mere centrale i dagligdagen. Den nuværende HTML version 4.01 har sine begrænsninger, hvilket har afledt brugen af løsninger såsom Flash. HTML5 er svaret på en tidssvarende standard – men der er udfordringer på sikkerhedssiden.

Der er sket meget, siden World Wide Web Consortium (W3C) frigav HTML version 4.01 i 1999. En stigende del af de services vi benytter i dag, er web-applikationer. Hvad enten de er Cloud-baserede eller lokale, så foregår mere og mere af vores arbejde i et browser-interface.

Begrænsningerne i HTML version 4.01 blev imødekommet med eksterne løsninger såsom Flash, Silverlight og ActiveX. Hvor disse tiltag forbedrede brugeroplevelsen, så introducerede de en sikkerhedsmæssig kompleksitet, der har medført mange kompromitterede maskiner. Specielt Flash har sine ofre.

HTML5 imødekommer denne fragmentering og introducerer en del teknologiske ændringer til HTML-standarden. I den gode sags tjeneste kan disse muligheder give særdeles stærke web-applikationer med stor brugerfunktionalitet.

Eksempelvis kan "Web Storage" lagre omkring fem megabyte data på klienten, som efterfølgende kan tilgås ved hjælp af JavaScript i en senere web-session. Tilsvarende giver det nye "Web Sockets API" muligheden for at etablere en full-duplex-forbindelse mellem klient og server. Det nye "Geolocation API" gør det muligt at bestemme en brugers position og dermed lokalisere indholdet.

Disse udvalgte muligheder introducerer på nuværende tidspunkt ingen sårbarheder i sig selv – men vil kunne udnyttes indirekte til at udføre ganske avancerede angreb.

HTML5 giver også udvikleren mulighed for at definere egen indholdshåndtering. Det betyder, at web-applikationer kan registreres, så de eksempelvis åbner e-mail

eller SMS-applikationer, når en bruger klikker på et link. I sin yderste konsekvens kan det medføre videregivelse af kritiske data, brugersporing og spam.

Web Sockets API'et alene har givet mange forskere grå hår. Ud over at give muligheden for cache poisoning og port-scanning af det interne netværk så er remote shells en mulighed. Dermed er der åbnet op for et web-baseret botnet, hvor der åbnes forbindelser til flere klienter ad gangen fra en central server.

Hvor HTML5 har potentialet til at blive en smuk svane med tiden, så mangler der stadig nogle sikkerhedsmæssige eftersyn. Eftersom Apple, Mozilla og Opera på den ene side vedligeholder deres version - og W3C på den anden vedligeholder deres - så vil der være forskelle på nogle punkter. Det er derfor spændende at se, hvad kandidatudgaven byder på, når den frigives i 2012.

Compass Security AG, 2011; "*HTML5 web security December 6th, 2011*".

4.7. Samarbejde øger hostingsikkerhed

Efter flere års kritik gik den danske hosting-branche sammen for at få styr på sikkerheden. Det bliver til fordel for både udbydere og kunder.

Svindlere opretter falske udgaver af websteder. Det sker hele tiden, også på danske netadresser. Formålet er at lokke fortrolige oplysninger fra internetbrugere ved at bilde dem ind, at et websted tilhører deres bank eller lignende. Det kaldes phishing.

Når DK•CERT modtager en henvendelse om sådan et phishing-websted, kontakter vi den udbyder eller det webhotel, hvor det falske websted er placeret. Og så venter vi på svar. Ofte må vi vente længe. Der kan gå fra otte dage til flere uger, før udbyderen tager affære og fjerner den farlige side.

Det kritiserede vi i et indlæg på Computerworld Online i april. Tidligere har DK•CERT også taget fat på problemerne med sikkerheden på webhoteller. Når et webhotel lægger serverplads til falske websteder, kan det nemlig skyldes problemer med sikkerheden. Hvis webhotellet for eksempel ikke har opdateret serversoftwaren, kan forbrydere udnytte sårbarheder til at trænge ind og placere deres svindelsider på serveren.

Tilbage i 2009 foreslog vi i en klumme, at branchen indførte en form for smiley-ordning i stil med den, vi kender fra fødevarebranchen. På den måde kan et webhotel dokumentere, at det tager hånd om sikkerheden.

Nu sker der noget. Webhotel-virksomhederne i Danmark oprettede i slutningen af 2011 Brancheforeningen for it-hostingvirksomheder i Danmark. Mere end tyve af de vigtigste spillere på området er medlemmer af den nye forening.

Foreningens formål er at højne kvalitets- og sikkerhedsniveauet på området. Det skal blandt andet ske gennem et fælles kvalitetsmærke og tilhørende certificering for kvalitet og sikkerhed.

Det er en særdeles god nyhed både for branchen og dens kunder. Branchen får fælles retningslinjer og mål for sikkerheden. Og kunderne får mulighed for at sammenligne og vurdere sikkerheden hos de forskellige udbydere. Dermed

"Hvor HTML5 har potentialet til at blive en smuk svane med tiden, så mangler der stadig nogle sikkerhedsmæssige eftersyn."

"Efter flere års kritik gik den danske hosting-branche sammen for at få styr på sikkerheden. Det bliver til fordel for både udbydere og kunder."

behøver prisen ikke længere være det eneste parameter, man sammenligner udbyderne på.

I DK•CERT ser vi frem til at samarbejde med Brancheforeningen for it-hostingvirksomheder i Danmark.

DK•CERT, 2011; "*Dit webhotel tager ikke din it-sikkerhed alvorligt*".
DK•CERT, 2009; "*Smiley'er skal begrænse defacements*".

5. Status på 2011

Vi vil her samle trådene for året 2011, således at du får et billede af de udfordringer, vi stod over for. Med udgangspunkt i årets data og historier kigger vi på de overordnede temaer og sammenhænge, som prægede året der gik og vil have betydning for, hvordan vi tænker og handler informationssikkerhed i fremtiden.

I lyset af internetkriminalitetens transnationale natur er det ikke overraskende, at niveauet herhjemme ifølge en undersøgelse foretaget af revisionsvirksomheden PwC svarer til niveauet i både Norden, Vesteuropa og globalt. Omfanget af truslen vurderes af 22 procent af respondenterne i undersøgelsen at være stigende, mens kun to procent mente, at risikoen for internetkriminalitet var faldet gennem de seneste 12 måneder. Det understreges i nedenstående citat om internetkriminalitet fra virksomhedens globale undersøgelse:

"Ten years ago, our survey showed that hardly anyone knew what it was. But this year's report ranks it as one of the top four economic crimes – just behind asset misappropriation, accounting fraud, and bribery and corruption."

Set i lyset af årets megen medieomtale af kompromittering og offentliggørelse af følsomme data er det ikke overraskende, at 59 procent af respondenterne i en årlig undersøgelse fra Ernst & Young svarede, at de i løbet af det kommende år havde en forventning om at øge udgifterne til informationssikkerhed.

De internetkriminelle har udviklet deres mål og midler gennem året, så truslen mod borgerne, organisationerne og samfundet fremstår større end nogensinde. De internetkriminelle videndeler og samarbejder på tværs af landegrænser. Der er en global undergrundsøkonomi, hvor for eksempel kreditkortinformationer, malware og DDoS-angreb handles.

Internetkriminalitetens udvikling afføder en række udfordringer for varetagelsen af informationssikkerheden. Det er dog ikke de eneste forandringer. Også ændringer i samfunds- og organisationsstrukturer medfører en række udfordringer, som vi er nød til at inddrage i vores måde at tænke informationssikkerhed på.

Tænk blot på de udfordringer det giver, at medarbejdere flere steder medbringer og bruger deres egne elektroniske enheder. Det kræver ikke blot nye politikker, regler og procedurer, men også overvejelser om, hvor meget indgreb organisationen kan og må udføre på udstyr, der ikke er deres. Kan man for eksempel forlange, at medarbejderne skal installere centralt overvåget krypterings-, backup- og sikkerhedssoftware, som også giver potentiel adgang til medarbejderens private data, på deres egne bærbare computere?

Tilsvarende giver stigende brug af tjenester i skyen grå hår for hovedet it-chefen. Cloud computing giver fordele med hensyn til skalerbarhed og fleksibilitet, men hvordan er det med sikkerheden? Kan man samarbejde med Google? Og hvad siger Datatilsynet?

Ernst & Young, 2011; "*Into the cloud, out of the fog*".
PwC, 2011; "*Cybercrime: protecting against the growing threat*".
PwC, 2011; "*Virksomhedskriminalitet i Danmark 2011*".

"De internetkriminelle har udviklet deres mål og midler gennem året, så truslen mod borgerne, organisationerne og samfundet fremstår større end nogensinde. De internetkriminelle videndeler og samarbejder på tværs af landegrænser."

5.1. Internetkriminalitetens udvikling

Kigger vi hen over årets historier, er den overordnede fortælling, at målene for internetkriminalitet er opdelt i hacktivisme, industrispionage og berigelseskriminalitet. Midlerne er for alle tre typer langt hen ad vejen de samme: Avanceret, målrettet malware og et godt forarbejde, hvor kendskab til ofrets egne data og systemer benyttes i angrebet.

Hacktivister i mere eller mindre diffuse grupperinger og med til tider uklare mål stod for mange af sidste årets angreb. Mest tydelige var Lulzsec og den løsere Anonymous-bevægelse. Andre og mere lokale grupper var også aktive. Særligt i Mellemøsten modarbejdede lokale og internationale grupper de siddende regeringers forsøg på at bevare kontrollen.

Nogen, der giver sig ud for at repræsentere Anonymous-bevægelsen, har i januar 2012 fremsat trusler mod myndigheder, universiteter og skoler i blandt andet Danmark. Formålet med operation "#opeurope" er at afslører, at der er korruption i Europa. Uanset ens holdning til målet for operationen må man tage truslen alvorligt. Særligt med øjne på Danmarks indtrædelse i formandsstolen for EU fra januar 2012 er den overhængende.

Lulzsec og Anonymous-bevægelsen kan også have inspireret andre grupperinger, som i fremtiden vil lufte deres holdninger og synspunkter gennem aktioner på internettet. Vi tror, at også 2012 vil stå i hacktivismens tegn. Således tror vi, at der kommer angreb på alt fra politiske modstandere til myndigheder og organisationer, der ikke handler i overensstemmelse med aktivisternes holdninger og/eller etiske og moralske standpunkter. Som i 2011 vil man forsøge at udstille målet ved offentliggørelse af fortrolige eller følsomme data, men også DDoS-angreb kan meget vel være i aktivisternes værktøjskasse.

Piratkopiering handler ikke kun om musik, film og software. I dag bliver alt fra medicin over modetøj og tasker til reservedele og industrianlæg kopieret. Når der for eksempel kan købes serienummererede reservedele til endnu ikke producerede bilmodeller og industrivirksomheder oplever reklamationer på industrianlæg, som man ud fra serienummeret kan konstatere er i produktion andre steder på kloden, kan man undre sig over, hvordan man har fået adgang til de data der har muliggjort kopieringen.

Hændelsen fra andet kvartal 2011 hvor flyproducenten Lockheed Martin viste sig at være målet for et angreb på RSA SecurID-tokens, anskueliggjorde, at internettet kan være en mulig kilde til indhentning af de nødvendige fortrolige produkt- og virksomhedsdata.

I august kom det tillige frem, at en dansk virksomhed optrådte på en liste over 72 virksomheder, der havde været inficeret med et fjernstyringsprogram, som gav uvedkommende adgang til virksomhedens lokale ressourcer. Listen blev offentliggjort af sikkerhedsvirksomheden McAfee, der fortalte, at angrebet dækkede over industrispionage. Det stod på i perioden 2006 til 2009.

Selv om hændelser om kompromittering af virksomhedskritiske forretnings- eller produktdata kun sjældent når vores eller mediernes søgelys, vurderer vi, at truslen om internetfaciliteret industrispionage i de kommende år vil være stigende. Vi har dog ingen forventning om, at sådanne hændelser i fremtiden vil figurere i vores rapporter.

"Selv om hændelser om kompromittering af virksomhedskritiske forretnings- eller produktdata kun sjældent når vores eller mediernes søgelys, vurderer vi, at truslen om internetfaciliteret industrispionage i de kommende år vil være stigende."

Mens hacktivisme og industrispionage er rettet med myndigheder og virksomheder, har berigelseskriminaliteten primært fokus på borgerne og adgangen til deres kreditkort. I løbet af 2011 oplevede vi større tyverier af kreditkortdata fra virksomheder, svindelnumre, phishing-angreb, falske telefonopkald fra Microsoft og spam, der havde til formål at sælge os falske eller værdiløse produkter.

Her stikker en hændelse ud. Hændelsen hvor en kinesisk formidler af internet domæner til overpris forsøgte at sælge kinesiske domæner, der modsvarede det i Danmark registrerede. Her var det virksomhederne, som var i søgelyset. Hændelsestypen er dog ikke ny, da den på mange måder minder om fortidens salg af værdiløse eller falske annoncer. Det nye er, at det blev udført fra udlandet.

Fælles for alle typer af hændelser er, at de er blevet mere målrettede. Den første kontakt foregår i færre tilfælde som tilfældige massehenvendelser, men udføres i stigende grad med brug af information om ofret, der har til formål at øge henvendelsens troværdighed. Oplysninger som man selv har lagt på sociale medier og lignende indgår i den kontekst, hvor data er tilvejebragt. Det gælder, hvad enten målet er at inficere brugerens computer med malware, franarre kreditkortoplysninger, lokke ham til at købe falske eller værdiløse produkter, finde sårbare systemer eller lignende.

Det er en medvirkende årsag til en stigning i mængden af spam, som blev sendt fra kompromitterede e-mailkonti. Her er der adgang til både personlige informationer og en mailkonto med høj troværdighed, når den udnyttes til at sende til de øvrige i den tilhørende adressebog.

En undersøgelse foretaget af Commtouch i september og oktober 2011 viste, at 15 procent af deltagerne, som alle havde fået kompromitteret deres mailkonto, var blevet kompromitteret ved et Facebook-link. Andre 15 procent svarede, at de umiddelbart inden havde benyttet et offentligt trådløst internet. 62 procent vidste ikke, hvordan det var sket, og formodningen er, at de benyttede svage passwords og kontoen havde været udsat for et brute-force-angreb. I 12 procent af tilfældene blev der sendt mails til adresser i adressebogen, der angav, at man var "stuck overseas" og bad modtageren om at overføre penge.

Set i lyset af årets mange offentliggørelser af persondata, heriblandt adgangskoder og passwords til e-mailkonti, kan det problem vise sig at være stigende. Særligt med baggrund i Anonymous-bevægelsens seneste trusler mod offentlige myndigheder, universiteter og skoler i Danmark. Det kan medføre en stigning i offentliggørelser af danske borgeres data, som senere misbruges.

Tilsvarende er den benyttede malware blevet mere avanceret, og anstrengelserne for at holde dens funktioner skjult er øget. Avancerede metoder til kryptering og kodeforplumring er ikke længere et særsyn, ligesom der ofte viderestilles til flere forskellige domæner. Det er alt sammen med til at gøre det vanskeligere at afklare, hvad koden gør og hvad formålet med den er.

Brugen af stjålne certifikater øger troværdigheden af koden. En stigende brug af ikke offentliggjorte sårbarheder benyttes til at lokke den ind på ofrets maskine. Det hvad enten der er tale om en Macintosh-, Windows- eller Linux-computer. De sårbarheder der benyttes, rammer bredt på alle styresystemer. I 2011 var det exploits til Java, der var de kriminelles foretrukne værktøj, men også sårbarheder i Flash, PDF og lignende blev udnyttet.

Også de internetkriminelle har gjort en forretning ud af skyen. Nye malware-

"Fælles for alle typer af hændelser er, at de er blevet mere målrettede. Den første kontakt foregår i færre tilfælde som tilfældige massehenvendelser, men udføres i stigende grad med brug af information om ofret, der har til formål at øge henvendelsens troværdighed."

varianter scannes mod betaling i cloud-baserede scannerfarme med de almindeligste antimalware-produkter. Formålet er at udsende malware, som ikke opdages. Når malwaren udsendes i et utal af mutationer, der hver i sær benyttes i målrettede lokale angreb, forlænges tiden, inden den når antimalware-producenterne.

Samtidig sammensættes alt hvad der behøves til et angreb i brugervenlige og prisbillige crimeware kits, der kun kræver moderat it-kendskab. I sådanne pakker indgår alt fra kompromittering af sårbare hjemmesider, malware der ikke kan detekteres, phishing-sider og udsendelse af mails til indsamling og videresalg af data.

Det har betydet, at traditionelle organiserede kriminelle nu også har fået øjnene op for internettets muligheder. Ofte er risikoen her mindre end ved for eksempel narkotikahandel og menneskesmugling. I modsætning til dem er de rene internetkriminelle grupperinger ifølge Europol langt mindre strukturerede og hierarkiske. Der er sjældent en egentlig leder, og medlemmerne, der ofte kun kender hinanden på internettet, udfører opgaver, der svarer til deres tekniske færdigheder. Det gør internetkriminaliteten vanskelig at efterforske og optrævle.

De forskellige transnationale organiserede grupperinger, der står bag de angreb, vi ser på danskernes informationssikkerhed, arbejder sammen og deler værktøjer og data. For eksempel sælges eller udlejes dele af større botnet og værktøjer fra forskellige grupper samlet i crimeware kits med henblik på udlejning eller videresalg. Hele den internetkriminelle forsyningskæde er blevet mere specialiseret og professionel for hermed at øge succesraten. Det har medført en digital undergrundsøkonomi, hvor alle typer af data og information er til salg.

Den globale finanskrise har en del af skylden for dette. Ifølge Europol har de internetkriminelles demografiske profil ændret sig således, at en større del er dygtige og højtuddannede yngre mænd, der ofte rekrutteres direkte fra universiteterne. Mænd, der hvis muligheden havde budt sig, sandsynligvis havde taget et arbejde på den rigtige side af loven.

Derfor er forretningsverdenens sprog også blevet de internetkriminelles sprog. Strategier for markedspenetrering og -andele går hånd i hånd med målinger af for eksempel et malware-angrebs succes. Her handler det om at skabe maksimal profit, og forståelse af den menneskelige psyke er et væsentligt aspekt i det at ramme målgruppen.

Internetkriminaliteten flytter sig over på de teknologier og services, som de potentielle ofre benytter. Det har medført, at sociale netværksmedier og mobiltelefoner i stigende grad er i søgelyset. Tilsvarende forventer vi, at "nye teknologier" som for eksempel HTML5 og IPv6 vil forsøges udnyttet, så snart udbredelsen er tilstrækkelig stor. Også smart elektronik i borgernes hjem kan vise sig at være et attraktivt mål.

Indførelsen af NemID har øjensynligt gjort det vanskeligere at misbruge de danske netbanker. Et avanceret phishing-angreb medførte dog, at otte Nordea-kunder i september fik tømt deres konti for i alt 62.400 kr. Både e-mails og hjemmeside var professionelt udført på fejlfrit dansk og med brug af Nordeas grafik. Overførslerne blev udført som man-in-the-middle-angreb på den webside, som brugerne blev ledt hen til i mailen.

At tro, at vi med NemID er beskyttede, vil derfor være en fejl. Der er andre veje til vores penge. Her spiller kreditkortet en væsentlig rolle. Også i 2011 modtog vi

"Internetkriminaliteten flytter sig over på de teknologier og services, som de potentielle ofre benytter. Det har medført, at sociale netværksmedier og mobiltelefoner i stigende grad er i søgelyset."

phishing-mails, der angiveligt var fra for eksempel Visa eller Mastercard. Angrebet på Sony Playstation Network i starten af 2011 viste også, at der er andre adgange til vores kreditkort informationer. Selv om kreditkortdata her viste sig at være krypteret, illustrerede det, hvordan vores data kan blive kompromitteret, uden vi selv har andel i det. Det handler blot om at have brugt sit kreditkort det forkerte sted. Vi tror, at der kommer flere angreb, som er målrettet usikre e-handels- og betalingsplatforme, hvor man på samme tid kan skaffe sig adgang til mange kreditkort- og kundeinformationer.

Fortsætter den økonomiske udvikling som vi har set det i 2011, er det vanskeligt at bevare troen på at glasset er halvt fuldt. Den finansielle krise har medført større international social ulighed. Til enhver tid har det betydet en stigende kriminalisering. Samtidig har internetkriminaliteten vist sig at være en god forretning, der mange steder på kloden kan udføres stort set uden risiko for senere retsforfølgelse.

Vi tror dog, at der er en vej ud af dette. Vi mener, at tiden kalder på mere samarbejde og information om, hvordan vi sikrer danskerne og deres data. Spørgsmålet er, om vi har råd til at lade være. Uden en fælles retning for udviklingen af vores informationssamfund kan det til tider virke som at famle i blinde.

Commtouch, 2011; "*The State of hacked accounts october 2011*".
Europol, 2011; "*iOCTA: Threat assessment on internet facilitated organised crime*".
Microsoft, 2011; "*Microsoft security intelligence report (volume 11)*".
Pastebin, 2011; "*Nicks in #AntiSec on irc.AnonOps.net*".
Version2, 2011; "*Dansk satellitfirma ramt af industrispion-bagdør*".

5.2. informationssikkerhedens fremtidige udfordringer

De kommende år byder på en række udfordringer, som bør søges løst gennem strategiske initiativer for samarbejde og kommunikation, da de er for vitale og vidtrækkende til at blive løst gennem sporadiske ad hoc-initiativer. Det drejer sig blandt andet om at skabe konsensus om NemID løsningen, at dæmme op for en stigende mængde malware og at sikre compliance til ISO 27001 i både ord og handling. Strategien bør i alle disse tilfælde være det styrende element.

Informationssikkerhed betragtes dog kun i mindre grad som en integreret del af det at gøre forretning. I Ernst & Youngs årlige undersøgelse havde 52 procent af respondenternes organisationer en dokumenteret fremadrettet informationssikkerhedsstrategi. Med danske øjne forventer vi, at dette tal er lavere af den simple årsag, at de organisationer som deltog i undersøgelsen, var større og mere globalt orienteret end den gennemsnitlige danske organisation.

I revisionsvirksomheden PwC's globale undersøgelse svarede 40 procent af respondenterne, at man ikke havde kompetencer til opdage og imødegå internetkriminalitet. Det er selvfølgelig udtryk for en stigende fokusering af kerneforretningen med heraf følgende brug af outsourcing og eksterne konsulentydelse, men også manglende ledelsesfokus på truslerne og deres potentielle konsekvenser.

Vi mener, at informationssikkerhed bør betragtes som et strategisk aktiv, snarere end en nødvendig udgift. Hvis ikke informationssikkerhed medtages i strategien på lige fod med den øvrige strategiske it-udvikling og -implementering, får det aldrig

"Vi mener, at tiden kalder på mere samarbejde og information om, hvordan vi sikrer danskerne og deres data. Spørgsmålet er, om vi har råd til at lade være. Uden en fælles retning for udviklingen af vores informationssamfund kan det til tider virke som at famle i blinde."

"De kommende år byder på en række udfordringer, som bør søges løst gennem strategiske initiativer for samarbejde og kommunikation, da de er for vitale og vidtrækkende til at blive løst gennem sporadiske ad hoc-initiativer."

den fornødne fokus hos beslutningstagerne.

Formår man ikke at flytte informationssikkerheden til det strategiske niveau, er det vanskeligt at forstille sig, at man kan opbygge en sikkerhedskultur, hvor man i tilstrækkelig grad kan informere og involvere medarbejderne. Derfor bør man prioritere uddannelse og inddrage medarbejderne i processen med at sikre organisationens it-aktiver. Det er trods alt medarbejderne, som ved, hvordan aktiverne benyttes.

Godt nok er informationssikkerhed ledelsens ansvar, men hvis det skal fungere, kræver det en kultur, hvor medarbejderne må, kan og vil tage ansvar. I modsat fald kan vi ikke imødegå truslerne fra stadig mere avanceret og målrettet malware, truslen om spear phishing-angreb med brug af medarbejderpublicerede private informationer, og de netop fremsatte trusler om offentliggørelse af data fra myndigheder, universiteter og skoler i blandt andet Danmark. Erfaringen fra 2011 har vist, at det kan få fatale konsekvenser.

Også den stigende brug af netværksopkoblet smart elektronik i hjemmene kan vise sig at blive en udfordring. Sammensmeltningen af arbejdsliv og privatliv betyder i mange tilfælde, at arbejdscomputeren derhjemme kobles på samme netværk som smart-tv'et, spilkonsollen, internet radioen, køleskabet og de intelligente enheder til styring af lys og varme. Fælles for dem er, at de introduceres som en "blackbox", hvor vi ikke har kendskab til eller kan påvirke og overvåge sikkerheden. Eneste mulighed er at stole på, at de indbyggede opdateringsmekanismer er tilstrækkelige.

Flere af disse enheder transmitterer og lagre data som i nogle tilfælde kan være følsomme. Et er for eksempel kreditkortinformationer og kontooplysninger til Twitter, Gmail og lignende. Under alle omstændigheder vil en kompromitteret enhed betyde lettere adgang til de øvrige enheder bag samme firewall. Heriblandt medarbejderens pc, som næste dag medbringes på arbejdspladsen.

Manglende versionsopdatering af styresystemerne udgør stadig en væsentlig trussel mod borgernes og organisationernes sikkerhed. Således viste data fra Microsofts værktøj til fjernelse af skadelig kode (MSRT), at malware-inficering af systemer der kørte Windows XP eller Windows Vista, i første halvdel af 2011 var mere end tre gange hyppigere, end på maskiner der kørte Windows 7. Det på trods af, at Windows 7 i juli måned herhjemme blev benyttet af flere brugere end de ældre styresystemer.

Her mener vi, at software producenterne har et medansvar for, at borgere og organisationer får opdateret til seneste version. En del af løsningen hedder oplysning og kommunikation om de nye systemers bedre sikkerhed og øvrige fortræffeligheder. En anden hedder løsninger, der gør den økonomiske byrde ved skift til nye versioner mindre for brugerne. Det skal være både nemt og billigt at opdatere sit styresystem til seneste version.

Samme problematik gør sig til dels gældende, når næsten en tredjedel af respondenterne i en global undersøgelse foretaget af Ernst & Young svarede, at deres organisation havde investeret i sikkerhedsløsninger, der enten fejlede eller ikke levede op til de krav, organisationen havde. Her kan argumenteres for, at organisationerne havde investeret i standardløsninger til at løse specifikke behov, ikke vidste, hvad de ville have, eller ikke havde undersøgt markedet godt nok. Under alle omstændigheder illustrerer det et behov for bedre kommunikation og samarbejde. Både internt i de organisationer, der køber produkterne, og i særdeleshed også i forhold til producenterne.

"Sammensmeltningen af arbejdsliv og privatliv betyder i mange tilfælde, at arbejdscomputeren derhjemme kobles på samme netværk som smart-tv'et, spilkonsollen, internet radioen, køleskabet og de intelligente enheder til styring af lys og varme. Fælles for dem er, at de introduceres som en "blackbox", hvor vi ikke har kendskab til eller kan påvirke og overvåge sikkerheden."

Organisationerne og deres medarbejdere har i dag taget skyen til sig, og mange benytter sig af cloud services. Vi kommer dog ikke til at opbygge samarbejdsrelationer til hverken Google, Yahoo, Amazon eller til de andre store cloud-udbydere. Derfor vil der altid være usikkerhed om, hvor og hvordan vores data opbevares, hvilket vil være en udfordring i forhold til for eksempel persondatalovens regler om opbevaring og behandling af personhenførbare data. Man bør derfor sikre sig, at man forstår de sikkerhedsvilkår, der gælder for den enkelte service, benytte sig af kryptering og konsultere Datatilsynet, inden man vælger at lægge hele sin forretning ud i skyen.

En ting er de store virksomhedssystemer, som vi kan vælge at drive selv eller placere hos en leverandør, hvor vi har sikkerhed for, at gældende regler overholdes. Noget andet er medarbejdernes brug af tjenester, som er placeret i skyen. Tjenester som alle er med til at få det daglige arbejde til at gå lidt lettere, og som man måske ikke er bevidst om er placeret i skyen. Når medarbejderen for eksempel lægger arbejdsrelaterede dokumenter i Dropbox eller sender det til deres egen Gmail-konto, for at arbejde på det derhjemme, er de reelt en tur over skyen uden for organisationens kontrol.

Problematikken om medarbejdernes kopiering af data og information til steder og medier, hvor de ikke var tiltænkt, har altid eksisteret. Men den er blevet forstærket af mangfoldigheden af muligheder, hvor opbevaringen af data er uklar og vanskelig at gennemskue. Det lægger et pres på organisationerne om at have klare regler for kopiering af virksomhedsdata, samt procedurer, der sikrer overholdelse af disse. Klassifikation af hvilke data, der er kritiske for forretningen og dens kunder er en hjørnesten i dette arbejde. Udfordringen stiger i takt med, at organisationerne behandler og lagrer stadig flere data.

Mens det er naturligt at begrænse, kontrollere og overvåge medarbejderne på deres virksomhedsejede arbejdsstationer, kan det være vanskeligt, når det er medarbejderen selv, der ejer den medbragte bærbare pc, tavle-pc eller mobiltelefon. Det er ikke desto mindre en virkelighed, som stadig flere organisationer må forholde sig til.

Når medarbejderne medbringer deres eget udstyr, er det for eksempel vanskeligt at forestille sig, at man kan stille krav om, at de ikke selv må eller kan installere applikationer på det. Under alle omstændigheder er det en udfordring at implementere procedurer, der sikre dette.

Tilsvarende gælder centralt udstyr til overvågning, kryptering og lignende, der også kan give potentiel adgang til medarbejderens private data. En ting er, at et tredjeparts-firma som vi selv har valgt som leverandør, har en sådan adgang, men det kan godt være, at man i nogle forhold ønsker en større fortrolighed i forhold til sin arbejdsplads. I sådanne tilfælde kræves nye politikker, regler og procedurer som er mere gensidige i forhold til også at sikre medarbejderen og dennes privatliv.

Selvfølgelig kan der laves politikker, der foreskriver, at adgangen til data skal være adskilt for arbejde og privatliv på bærbare pc'er, som er ejet af medarbejderne. Under alle omstændigheder gælder det om at risikovurdere de konfigurationer og enheder, der benyttes, og sørge for, at der udfærdiges politikker på området. Derudover bør man overveje, om følsomme data overhovedet skal kunne overføres til mobile enheder, som står uden for organisationens ejerskab og kontrol.
I det hele taget mangler mange organisationer ifølge Ernst & Young at omstille sig til en mere mobil verden. Således svarede kun 57 procent af respondenterne i virksomhedens årlige globale undersøgelse om informationssikkerhed, at de havde

"Selvfølgelig kan der laves politikker, der foreskriver, at adgangen til data skal være adskilt for arbejde og privatliv på bærbare pc'er, som er ejet af medarbejderne."

tilpasset deres politikker til også at imødegå risici på mobile enheder. Kun 47 procent havde således implementeret kryptering på bærbare computere og mobile enheder.

Heldigvis ser det ud til at gå i den rigtige retning. I Ernst & Youngs årlige globale undersøgelse om informationssikkerhed svarede 66 procent af respondenterne, at man havde implementeret data loss prevention (DLP). Hele 74 procent havde defineret politikker for klassifikation og håndtering af følsomme data. Den gruppe af organisationer, der ikke havde specifikke politikker for brug af mobile enheder, kan således på anden vis have imødegået problematikkerne ved at begrænse adgangen til følsomme data.

Den økonomiske krise må ikke give anledning til, at der opstår tvivl om kvaliteten af vores arbejde. I debatten om nedskæringer på Det Kongelige Teater har tidligere medlemmer af ledelsen og bestyrelsen udtrykt bekymring for, om man kan bevare den høje kvalitet i teatrets kommende forestillinger. En sådan debat vil uundgåeligt medføre, at teatrets dygtigste medarbejdere vil søge hen, hvor pengene, kvaliteten og prestigen er større.

Det samme vil ske, når det drejer sig om informationssikkerhed. Særligt set i lyset af, at Anonymous-bevægelsen i januar 2012 muligvis har fremsat trusler mod skoler, universiteter og myndighederne i blandt andet Danmark, vil det være bekymrende, hvis vi herhjemme på samme måde lader økonomien være argumentet for nedskæringer på sikkerheden. Lad os i stedet samarbejde om løsninger, som i første omgang højner sikkerheden og på sigt muliggør, at vi kan gøre det mere effektivt.

Udviklingen på it-fronten og i samfundet som helhed udfordrer nemlig de måder, hvorpå vi hidtil har tænkt informationssikkerhed. Vi mener, at man skal tænke fornyelse i helheder. Tiden kalder på mere samarbejde. Ikke kun om hvordan vi beskytter mod de aktuelle trusler, men også hvordan vi som samfund, organisation og borger kan bidrage til at gøre det i fremtiden.

Hver gang en borger eller organisation herhjemme udsættes for internetkriminalitet, hvad enten det drejer sig om netbankindbrud, phishing, industrispionage eller andet, betyder det penge, der forsvinder ud af landet. Penge som ikke fremgår af betalingsbalancen, men optræder som et nationaløkonomisk mørketal, der i stedet kunne være brugt til at sikre danske arbejdspladser.

Tingene hænger sammen. På samme vis som organisationerne har et medansvar for at uddanne deres medarbejdere, så de også i privatlivet kan agere sikkert, har vi som samfund en forpligtelse til at opretholde fødekæden af uddannet arbejdskraft. Vi mener dog, at vi med hensyn til informationsteknologi mangler de overordnede retningslinjer for den retning, vi ønsker at styre samfundet i.

Når vi som danskere bryster os af at være blandt verdens førende it-nationer, hvad angår digitalisering af den offentlige sektor og borgernes adgang til og brug af internettet, kan man derfor undre sig over, at vi ikke har en national it-strategi, der for eksempel også inkluderer borgernes og organisationernes sikkerhed. I øjeblikket har vi strategier for digitalisering af stat, regioner og kommuner samt strategier på sektorniveau som for eksempel sundheds- og uddannelsessektoren. I ingen af dem indgår sikkerheden som en integreret del.

Vi mangler en strategi, som samler det fremadrettede perspektiv. Som for eksempel inkluderer udvikling og samspil med den private sektor, uddannelse, forskning samt sikkerhed. I vores perspektiv hænger disse ting sammen. Fraværet

"Når vi som danskere bryster os af at være blandt verdens førende it-nationer, hvad angår digitalisering af den offentlige sektor og borgernes adgang til og brug af internettet, kan man derfor undre sig over, at vi ikke har en national it-strategi, der for eksempel også inkluderer borgernes og organisationernes sikkerhed."

af en national it-strategi betyder samtidig fraværet af visioner på den nationale it-front. Også når det gælder informationssikkerhed. Når der ikke er en national it-strategi, der sætter pejlemærker for den fremtidige udvikling, er det i vores perspektiv vanskeligt at forestille sig, at vi kan opbygge den nødvendige indsigt og kompetence, som nationalt kan gøre en forskel, også udover effektiviteten af den offentlige sektor.

At informationssikkerhed ikke fra starten medtænkes som et element i udviklingen og brugen af informationsteknologi på nationalt plan, har blandt andet medført, at vi i dag diskuterer, hvorvidt logningsdirektivet er for omfattende eller ikke vidtrækkende nok. Vi mangler at sætter det i forhold til, hvorfor vi overhovedet ønsker at logge.

Anonymous, 2012; "*Anonymous - #opeurope - Expect us!*".
Ernst & Young, 2011; "*Into the cloud, out of the fog*".
Microsoft, 2011; "*Microsoft security intelligence report (volume 11)*".
Politiken, 2012; "*Det Kgl. Teater bliver reduceret til provinsteater*".
PwC, 2011; "*Cybercrime: protecting against the growing threat*".

6. Det eksterne perspektiv

Ifølge en undersøgelse, foretaget af revisionsselskabet PwC, vil næsten 20 procent af de danske virksomheder blive ofre for internetkriminalitet i løbet af et år. Deres historie er også væsentlig.

Derfor har vi i nærværende afsnit valgt at give ordet til nogle af de parter, som vi har en samarbejdsrelation til, og som har en interesse i informationssikkerhed. For at belyse emnet fra flere vinkler, har vi ladet forskellige aktører med forskellige roller i det danske informationssikkerhedssamarbejde komme til orde. Målet er, at gøre vores perspektiv på informationssikkerhed mere åbent og brugbart.

Vi lægger ud med at høre om internetkundens betragtninger på informationssikkerhed nu og i fremtiden. Vi har valgt at give ordet til informationssikkerhedschef Henrik Larsen fra Københavns Universitet, som her fortæller om de udfordringer KU havde i 2011 samt forventer fremadrettet. Endelig giver han sit perspektiv på samarbejde omkring informationssikkerhed.

Herefter lader vi divisionsdirektør Martin Bech fra UNI•Cs, som driver Forskningsnettet, komme til orde. Han giver et indblik i internetudbyderens perspektiv og betragter de udfordringer man her står over for, når det handler om informationssikkerhed.

NemID har i løbet af året været gennem en storm af kritik. Øjeblikket er dog forpasset, hvor vi frit kan vælge og vrage mellem udbydere og løsninger til offentlig digital autentificering. Kigger vi ud i verden, kan det være vanskeligt at se reelle alternativer.

Grundlæggende mener vi, at implementeringen af NemID har løst nogle af de problemer, vi tidligere havde. Dette afspejles blandt andet i Finansrådets statistikker over netbank-indbrud. Hvis der så er nogle børnesygdomme, må vi kunne luge dem ud hen ad vejen. Til at kommentere dette har vi inviteret centerleder Palle H. Sørensen fra Digitaliseringsstyrelsen til at skrive i årets rapport.

Finansrådet, 2011; "*Netbankindbrud - statistik*".
PwC, 2011; "*Virksomhedskriminalitet i Danmark 2011*".

6.1. Informationssikkerhedschefens syn på temaet "Har vi råd til ikke at samarbejde?"

Af Henrik Larsen, informationssikkerhedschef, Københavns Universitet

Københavns Universitet har siden 2004/05 opbygget sin informationssikkerheds-organisation. Universitetsdirektøren er formand for nformationssikkerhedsudvalget (ISU), der en gang om året leverer en rapport til universitetets ledelsesteam (LT), der består af rektoratet, universitetsdirektøren og dekanerne for de 8 fakulteter.

Informationssikkerhedschefen har som sekretær for ISU ansvaret for den daglige drift af informationssikkerhedsorganisationen, som består af syv lokale informationssikkerhedsudvalg (LISU), der tilsammen dækker de otte fakulteter og fællesadministrationen. En organisation på omkring 90 medlemmer, hvor næsten

alle har informationssikkerhed som en mindre del af deres jobbeskrivelse. Kun et enkelt fakultet har en professionel informationssikkerhedsspecialist, der - ligesom informationssikkerhedschefen - beskæftiger sig fuldtids med området.

Denne artikels forfatter overtog med udgangen af september 2011 funktionen som informationssikkerhedschef efter at have "stået i lære" et års tid hos forgængeren Kurt Bjernemose. Hvad er så udfordringerne for en ny mand med ansvar for driften af et stort universitets informationssikkerhedsorganisation?

Først og fremmest har jeg forgængerens solide arbejde at bygge på. En velfungerende organisation med ledelsesbevågenhed. Sikkerhedsstrategi, informationssikkerhedspolitik og øvrige retningslinjer samlet i en webbaseret håndbog samt risikovurderinger og beredskabsplaner på alle institutter. Efter flere awareness-kampagner en udbredt bevidsthed om trusler og sikker adfærd – og desuden gode kontakter både til DK•CERT og til de øvrige universiteter. Men der er stadig nok at tage fat på.

Risikovurderinger og beredskabsplaner skal opdateres og informationssikkerheds-håndbogen skal revideres, dels i forbindelse med at universitetet har vedtaget at overgå til den internationale sikkerhedsstandard ISO 27000-serien, og dels efter at bestyrelsen har vedtaget en ny strategi for universitetet frem til 2016. Sikkerhedspolitikker skal rettes og i et vist omfang nyskrives, i takt med at nye teknologier tages i brug og trusselsbilledet ændrer sig. Vejledninger og anvisninger på nettet skal vedligeholdes og i et vist omfang flyttes over på intranettet. Nye awareness-kampagner skal udtænkes og iværksættes for at fastholde og udbygge sikkerhedsbevidstheden blandt ansatte og studerende.

Eksempler på nye områder, der skal udarbejdes politikker for, er den øgede anvendelse af mobile enheder som bærbare computere, tavlecomputere og smartphones. Ikke kun vores næsten 50.000 studerende, men også en stigende del af de ansatte medbringer deres egne enheder, hvortil de forventer at kunne synkronisere universitetsejede data. Det kræver stor bevidsthed om overholdelse af regler for at undgå datatab eller fortrolighedsbrud.

Også den øgede anvendelse af tjenester, der bygger på cloud computing, er en udfordring. Her er både tilgængelighed, integritet og fortrolighed truet, hvis tjenesterne tages i brug uden at følge de vedtagne retningslinjer.

Sommerens skybrud over København gik ikke ud over driften af universitetets centrale systemer, selvom man oplevede lokale afbrydelser. Det har dog sat fokus på trusler fra vand, strøm, brand med videre mod ikke-elektroniske informationsaktiver i form af genstande i universitetets museer, arkiver og andre samlinger. Det drejer sig om alt fra sten og mineraler over plantefrø og levende planter, udstoppede dyr og skeletter af ofre for middelalderens spedalskhed til islandske håndskrifter, boreprøver af den grønlandske indlandsis og kunst, samlet over flere århundreder. Et område, der hidtil har været upåagtet i forbindelse med risikovurderinger og beredskabsplaner, men som nu har givet anledning til overvejelser og ekstra arbejde. Ikke mindst for lokale informationssikkerhedsan-svarlige.

Hvordan kan vi opretholde et tilstrækkeligt niveau i informationssikkerheds-organisationens arbejde, i en situation hvor den i lighed med den øvrige administration forventes at yde mere for færre midler? Hvordan kan vi i en virkelighed med stadig nye og voksende trusler opretholde tilstrækkelig beskyttelse af forskningsdata og personoplysninger med mere? Det kan kun ske gennem samarbejde indadtil, såvel som udadtil.

"Hvordan kan vi i en virkelighed med stadig nye og voksende trusler opretholde tilstrækkelig beskyttelse af forskningsdata og personoplysninger med mere? Det kan kun ske gennem samarbejde indadtil, såvel som udadtil."

Et vigtigt samarbejdsforum er "UNI-ITs Sikkerhedsgruppe", under Danske Universiteter. Gruppen består af informationssikkerhedschefer og informationssikkerhedskoordinatorer ved universiteterne, der dels mødes 3-4 gange om året og dels bruger hinanden til sparring omkring nye politikker, aktuelle trusler og udfordringer med mere.

Andet samarbejde sker i formelle og uformelle netværk, hvor man bliver opdateret om tendenser, sårbarheder, trusler og modforholdsregler. Jeg kan også kun opfordre til, at man opfatter den eksterne revision som mere end blot en kontrollant. Den er også en samarbejdspartner, der giver gode råd til at øge sikkerheden omkring institutionens data.

Det er afgørende for de fleste ikke at skulle opfinde alting fra grunden og tænke alle tanker selv. Når man kan udveksle viden i et tæt og godt samarbejde med ligestillede, kommer alle længere med de forhåndenværende ressourcer i kerneopgaven: Beskyttelsen af institutionens informationsaktiver.

6.2. Forskningsnettet – en internetudbyder med fokus på sikkerhed

Af Martin Bech, divisionsdirektør, UNI•C

Forskningsnettet er internetudbyder for alle universiteter og forskningsinstitutioner i Danmark, og drives som en brugerbetalt og brugerstyret infrastruktur, hvor UNI•C varetager den daglige drift og udvikling.

Når Forskningsnettet drives som et selvstændigt net helt ned til de fysiske bokse og fibre, er det fordi dets formål blandt andet er at levere ydelser, som er hurtigere og mere avancerede, end man kan købe på det almindelige marked. Det avancerede ligger både i de høje båndbredder og i de tjenester, der kører på nettet. Og det giver spændende udfordringer, når det gælder sikkerheden.

Forskningsnettet har for eksempel længe (faktisk siden 1993) brugt den næste version af internettets protokolstak, IPv6. Men med hensyn til sikkerheden er vi først nu ved at se nogle af de sikkerhedsproblemer, som vi kender så godt fra forgængeren, IPv4. Her ved vi alt om, hvordan vi håndterer udfordringer som hackerangreb, ude-af-drift-angreb, virus, orme og spam.

Med overgangen til IPv6 skal vores brugere i nogle tilfælde lære nye metoder til at beskytte deres systemer med. For eksempel er det i IPv4 normalt at anvende firewalls med NAT (Network Address Translation), hvor man kun viser en enkelt IP-adresse ud mod internettet. I IPv6 er det ikke nødvendigt for at spare på adresserne – dem er der nemlig masser af. Men hvilke konsekvenser får det for sikkerheden, at de enkelte computere inde på et institut nu kan nås direkte ude fra nettet? Den slags tekniske spørgsmål er vi i gang med at løse. Vi har også allerede set det første eksempel på IPv6-baseret spam.

I november viste årets Forskningsnet-konference, at it-sikkerhed står højt på dagsordenen hos Forskningsnettets brugere. Der var således stor interesse for indlæggene fra WAYF og Forskningsnet CERT (DK•CERT). WAYF tilbyder en sikker metode til login på tværs af institutioner og tjenester. Forskningsnet CERT står for den daglige behandling af sikkerhedshændelser på Forskningsnettet. Begge organisationer mødte stor interesse og fik mange opfølgende spørgsmål fra konferencedeltagerne.

Forskningsnettet

Forskningsnettet er et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner Forskningsnettet 100.000 ansatte og studerende på universiteter og forskningsinstitutioner med en række tjenester til forskning, samarbejde og kommunikation.

Det overordnede ansvar for den daglige drift af Forskningsnettet ligger hos driftskoordinatoren UNI•C, der også er ansvarlig for en række projekter og kommunikationsopgaver for Forskningsnettet.

"Forskningsnettet har for eksempel længe (faktisk siden 1993) brugt den næste version af internettets protokolstak, IPv6. Men med hensyn til sikkerheden er vi først nu ved at se nogle af de sikkerhedsproblemer, som vi kender så godt fra forgængeren, IPv4."

Et af Forskningsnettets udviklingsprojekter handler om brugerstyret bestilling og opsætning af dedikerede optiske kredsløb – i daglig tale kaldet bandwidth on demand. Her er formålet at enkelte (store) brugere i begge ender af forbindelsen trækker de dedikerede forbindelser helt ind til det udstyr, som har brug for at transmittere data ved store båndbredder og/eller have en meget konstant kvalitet uden pakkekollisioner. Men den slags forbindelser, der i øvrigt som regel er internationale, kører netop uden om de firewalls og andre sikkerhedstiltag som ellers beskytter institutionerne. Det skaber selvsagt nye udfordringer for alle parter.

Forskningsnettet og dets brugere opfatter sikkerhed som en meget væsentlig parameter – også fordi mange videnskabelige anvendelser kræver et vist mål af åbenhed for at dele ressourcer og data. Så det er måske nok usædvanligt, at Forskningsnettet som internetudbyder bruger næsten 10 procent af de samlede udgifter på sikkerhed, men det er egentlig ikke overraskende. Hvis ikke Forskningsnettet lavede hele denne indsats via sin CERT-funktion, ville brugerne selv skulle bruge tilsvarende ressourcer.

Nu skal Forskningsnettet i løbet af 2012 til at indgå i en samlet organisation under navnet Dansk e-Infrastruktur Center (DEIC), hvor det skal samtænkes med infrastruktur til videnskabelige beregninger (scientific computing), og hvor den samlede organisation skal løse nye opgaver inden for fælles infrastruktur. Det vil utvivlsomt give nye udfordringer for sikkerhedskonfigurationen, når den rette balance mellem beskyttelse og åbenhed skal findes.

Sikkerhed og en langt højere grad af samarbejde er altså en af de måder, hvorpå Forskningsnettet adskiller sig fra en sædvanlig internetudbyder. Og medens det er svært at forestille sig, hvilke sikkerhedstiltag der er nødvendige fremover, vil samarbejdet mellem alle parterne på Forskningsnettet helt sikkert være en af de vigtigste faktorer i bekæmpelsen af fremtidens sikkerhedsproblemer. Når vores modstandere arbejder sammen, skal vi også gøre det.

6.3. NemID – samarbejde om sikkerhed

Af Palle H. Sørensen, centerleder, Digitaliseringsstyrelsen

Tæt på 3,6 millioner danskere havde ved udgangen af 2011 brugt NemID 550 millioner gange til myndighedernes hjemmesider, netbanker eller andre private virksomheders hjemmesider. Med dette resultat har NemID-løsningen opfyldt ét af de væsentlige mål, nemlig at løsningen skulle udbredes hurtigt til mange danskere og anvendes hyppigt.

Målet blev nået på grund af et internationalt set enestående samarbejde mellem den finansielle og den offentlige sektor.

Formålet med udviklingen af NemID var at øge sikkerheden i forhold til den tidligere digitale signatur og de tidligere netbankløsninger. Løsningen er designet, så brugerens private nøgle opbevares sikkert på en central signaturserver.

Generering og anvendelse af den private nøgle kan kun foregå i specielle sikrede kryptografiske hardware-moduler under brugerens fulde kontrol. Brugerens anvendelse af den private nøgle er baseret på en ægte to-faktor-autentifikation. Brugeren skal både have noget i hovedet – adgangskoden – og noget i hånden – nøglekortet. NemID har derved hævet sikkerhedsbarren ved blandt andet at

"... fremover, vil samarbejdet mellem alle parterne på Forskningsnettet helt sikkert være en af de vigtigste faktorer i bekæmpelsen af fremtidens sikkerhedsproblemer. Når vores modstandere arbejder sammen, skal vi også gøre det."

Figur 13. NemID nøgle kort.

beskytte brugeren mod hackerangreb på pc'en i form af trojanske heste og lignende.

Både Finansrådet og Nordsjællands Politi har offentligt oplyst, at der i 2011 har været et fald i antallet af netbank-indbrud, og at noget tyder på at indførelsen af NemID har bidraget hertil.

Med det nye design er trusselsbilledet flyttet fra trojanske heste og lignende angreb til man-in-the-middle-angreb eller "live" phishing-angreb af den type, som otte netbankkunder blev udsat for i september 2011.

Sikkerhed er ikke en absolut størrelse. Trusselsbilledet ændrer sig konstant, og det er ikke praktisk muligt at etablere sikkerhedssystemer, der over tid er 100 procent sikre. Vi er derfor nødt til at acceptere, at der ligesom i den analoge verden er en risiko ved at anvende digitale løsninger. Risikoen for misbrug og svindel i den papirbaserede verden er trods alt stadig langt større.

Identitetstyveri eller økonomiske tab er, uanset om det sker i den digitale eller den analoge verden, alvorlige forbrydelser og falder under dansk rets almindelige regler, herunder straffeloven og betalingstjenesteloven.

Sikkerheden i løsningen har fra starten haft højeste prioritet. Som et led heri har Nets DanID blandt andet etableret et beredskab, der gør det muligt hurtigt at sætte supplerende sikkerhedsforanstaltninger i værk, hvis det vurderes at blive aktuelt.

Bankerne, Nets DanID og Digitaliseringsstyrelsen foretager løbende en risikovurdering af de aktuelle trusler og afvejer behovet for supplerende sikkerhedsforanstaltninger i forhold til brugervenlighed og økonomi.

De tekniske sikkerhedsforanstaltninger i NemID kan dog ikke stå alene. Bankerne, Nets DanID og Digitaliseringsstyrelsen oplyser løbende brugerne, så de bedre kan gennemskue for eksempel phishing. Det er alfa og omega, at brugerne bliver bedre til at færdes sikkert på nettet og være kritiske over for de it-kriminelles lokkemidler.

Blandt andet kan nævnes det årlige offentlige-private samarbejde om "Netsikker nu!"-kampagnen samt den løbende oplysningsindsats på den offentlige hjemmeside nemid.nu og bankernes og Finansrådets hjemmesider.

Tilliden til, at NemID løbende opretholder et højt sikkerhedsniveau, er altafgørende, fordi løsningen er et centralt element i den fællesoffentlige digitaliseringsstrategi. Digitaliseringen af kommunikationen mellem offentlige myndigheder, borgere og virksomheder skal bidrage til at realisere store besparelsespotentialer. Dermed sikres en holdbar samfundsøkonomi, som er forudsætningen for at bevare velfærdssamfundet i de kommende år.

Heldigvis er der stor opbakning blandt brugerne af NemID. 73 procent siger i en måling fra september 2011, at de har tillid til løsningen.

Samarbejdet mellem den finansielle og den offentlige sektor har været afgørende for udbredelsen af NemID. Sikkerheden nyder dog også godt af de fælles kræfter. Både Nets DanID, finanssektoren og Digitaliseringsstyrelsen bidrager til den samlede overvågning af trusselsbilledet, og det øger chancen for, at et eventuelt angreb opdages og stoppes i tide.

NemID til borgerne blev lanceret den 1. juli 2010.

NemID til erhverv forventes lanceret i juni 2012.

Kontrakten med Nets DanID løber til 2015 med mulighed for forlængelse i to år.

3.586.922 borgere har taget NemID i brug.

Der har siden lanceringen været 550 million transaktioner med NemID.

239 private virksomheder tilbyder log-in med NemID.

"Sikkerhed er ikke en absolut størrelse. Trusselsbilledet ændrer sig konstant, og det er ikke praktisk muligt at etablere sikkerhedssystemer, der over tid er 100 procent sikre. Vi er derfor nødt til at acceptere, at der ligesom i den analoge verden er en risiko ved at anvende digitale løsninger."

De økonomiske gevinster ved samarbejdet er også værd at nævne. Det er selvsagt en meget stor opgave at udvikle og vedligeholde et stort sikkerhedssystem, og det er oplagt, at der er økonomiske gevinster for både den finansielle og den offentlige sektor i ikke at skulle udvikle og vedligeholde flere adskilte systemer, men i stedet bidrage til et rigtig godt fælles system.

I en undersøgelse fra september 2011 svarer 97 procent af de adspurgte, at de har brugt NemID til log-in til netbank. 84 procent har brugt NemID til log-in på offentlige myndigheders hjemmesider.

I samme undersøgelse svarer 90 procent, at de er tilfredse med NemID.

7. Opsamling

"Hardware er stadig hardware og software er stadig sårbar."

I et tilbageblik på året der er gået kan vi konstatere, at flere af sidste års forudsigelser af fremtidige tendenser for internetkriminalitet i 2011 er realiseret. Tidligere afsnit har haft fokus på data og enkeltstående begivenheder. Her forsøger vi at sætte ord på de tendenser, vi så som de mest fremherskende i 2011. Herunder de trends vi tror, vil præge fremtidens trusselslandskab.

Flere af punkterne er ikke nye, men har blot fået nye ord eller ny næring ved teknologiens ibrugtagning og udbredelse. Det gælder for eksempel truslen om angreb på hjemmeelektronik, som er blevet langt mere nærværende efter udbredelsen af smart-tv. Problemet er, at vi accepterer at ny teknologi udvikles og udbredes som en "blackbox" med fokus på den oplevede funktionalitet. I modsætning til på computeren, giver tv'et i dag kun ringe mulighed for at tilpasse og overvåge sikkerheden. Det sker, selvom tv'et er placeret på samme trådløse netværk som computeren, spilkonsollen og mobiltelefonen, der blandt andet bruges til lagring af kreditkortdata og anden følsom information.

Fra en overordnet betragtning kan man mene, at der ikke er meget nyt under solen. At det blot er dimserne og måden vi forbinder dem på som er nye. Hardware er stadig hardware og software er stadig sårbar. De internetkriminelles motiver og metoder er også stort set de samme som sidste år. Som teknologien er de blot blevet forfinet og mere sofistikerede og målrettede. Herved er virkeligheden blevet mere kompleks og vanskelig at overskue. Vi tror, at vi i fællesskab kan være med til at stille krav og skabe fremtiden, således at vi kan imødegå truslerne.

Om trusselsbilledet er korrekt, må være op til individuel vurdering og tiden at vise. Vi håber dog, at du kan bruge det som inspiration og baggrund for samarbejde, så vi fremadrettet kan sikre danskernes it-aktiver.

7.1. Tendenser fra året der gik

Betragter vi det forgangne år, gives der bund for teknologiforskrækkelse og paranoia. Året var præget af flere tendenser, der hver for sig eller tilsammen var muliggjort af udvikling og udbredelse af teknologi, stigende globalisering, samfundsmæssig fragmentering og større professionalisme og samarbejde hos dem, som forsøger at misbruge vores systemer og data.

Vi har tidligere nævnt netopkoblet forbrugerelektronik som en potentiel trussel. Selv om 2011 blev året hvor Smart elektronik for alvor indtog vores hjem, var offentliggørelsen af brugerdata fra Sony Playstation Network det nærmeste vi kommer et misbrug. Angrebet var dog ikke rettet mod hjemmets elektronik, men mod Sony. Denne og lignende hændelser var med til at definerere 2011 som hacktivismens år.

Sidst på året udsendte medierne historier om overvågningssoftware på mobiltelefoner og PET's brug af trojanske heste. Tidligere rullede skandalen om den engelske presses aflytning af telefonsvarere på mobiltelefoner og historierne om, hvordan de politiske yderfløje herhjemme overvågede og registrerede hinanden. I betragtning af, at overvågning er mest effektiv, hvis man ikke ved, at man bliver overvåget, er dette nok kun toppen af isbjerget. Vi regner med, at problemet er større i egne af verden, hvor holdningen til privatlivets fred er mere lemfældig.

Udnyttelse af sårbarheder i programmer der benyttes på flere platforme, førte til malware, der ramte bredt. Særligt Java var i de it-kriminelles søgelys. For eksempel var exploits til Java de hyppigste i 2011. Både Windows-, Macintosh- og UNIX-computere blev mål for samme malware, der for at undgå opdagelse blev udsendt i millioner af mutationer, som forinden var scannet med de mest almindelige antivirus-produkter. Cloud-baserede scannerfarme udgjorde her et nyt skridt i evolutionen af de internetkriminelles forretningsmodel.

Med angrebene på Comodo og DigiNotar blev der åbnet for de internetkriminelles brug af digitale certifikater. Flere malware-varianter var designet til at stjæle digitale certifikater, som siden kunne benyttes til signering af malware. For eksempel var både ormen Qbot og den trojanske hest ZXshell signeret med stjålne certifikater. Tillige søgte de efter digitale certifikater på de inficerede systemer for herefter at uploade dem til centrale servere. Også Stuxnet og Duqu benyttede sig af stjålne certifikater.

Der er sket en kraftig stigning i mængden af information som vi selv, vores arbejdsplads eller øvrige relationer publicerer om os på for eksempel sociale netværkssteder. Det udgør en stigende risiko for misbrug. Det måtte to medarbejdere i RSA sande, da de i marts blev udsat for et spear phishing-angreb. Det medførte i sidste ende kompromittering af SecurID-sikkerheden. De sociale netværk udgør dog også en stigende risiko for, at brugerne udsættes for spam, svindel og malware. Tilliden og den udbredte brug af URL-forkortere er blandt de væsentligste årsager til, at det lykkes.

Som på de sociale medier udnytter de internetkriminelle den tillid, der ligger i at modtage mails fra folk, man kender. Spam- og phishing-mails blev i stigende grad udsendt fra kompromitterede webmailkonti hos Google, Yahoo og tilsvarende. Denne tendens må nok betegnes som værende mere af nød end af lyst, da flere af de store botnet de seneste år er blevet lukket. En anden forklaring kan være, at kompromitterede mailkonti blev publiceret på nettet af blandt andet Anonymous-bevægelsen. Derfor har vi set et generelt fald i mængden af uønskede mails, da det nu ikke er muligt at udsende spam i samme mængder som tidligere.

Udbredelse og brug af smartphones, som i dag reelt er små computere, har gjort dem til et mål for internetkriminalitet. Særligt Android-telefoner har været i skudlinjen for malware og var i tredje kvartal malware-skribenternes foretrukne platform. Åbenheden i Android Market har her vist sig som en del af problemet. Ud over de mange brugbare applikationer som kan hentes, fungerer Android Market også som platform for spredning af malware og hvidvaskning af penge. Hertil kommer selvfølgelig de applikationer, som sælges uden reelt af have noget indhold eller værdi.

Nedenfor angiver vi de tendenser for internetkriminalitet som vi med et dansk ståsted og globalt udsyn fandt mest fremtrædende i året der gik. Listen er ikke prioriteret og angiver ikke, hvilke trusler der var størst eller mest udbredt.

1. **Hacktivisme**. Internet-aktivisme nåede med Anonymous-bevægelsen og operation Antisec globalt set nye højder i året der gik. Herhjemme var der for eksempel politikere og politiske partier, der fik deres hjemmesider overskrevet. Hacktivisme fik for alvor vind i sejlene i 2011.
2. **Overvågning nåede nye højder**. Overvågningssamfundet nåede globalt set nye højder i 2011. Myndighederne overvågede borgerne, de politiske fløje overvågede hinanden og medierne overvågede alle.
3. **Java exploits**. Java var ifølge Microsoft målet for mellem en tredjedel og

"Der er sket en kraftig stigning i mængden af information som vi selv, vores arbejdsplads eller øvrige relationer publicerer om os på for eksempel sociale netværkssteder. Det udgør en stigende risiko for misbrug."

halvdelen af alle exploits observeret i starten af året. Herved fortsættes en tendens, der gør det muligt at ramme på tværs af operativsystemer og platforme.

4. **Samme malware til flere platforme**. 2011 bød på det endelige gennembrud for malware målrettet flere platforme. Flere nye sårbarheder i for eksempel Java, Flash Player, Adobe Reader og Acrobat muliggjorde udviklingen af malware, der ramte flere platforme.
5. **Usynlige malware-mutationer**. Billige cloud-baserede scannerfarme benyttede de fleste gængse antimalware produkter og gjorde det muligt at udsende millioner mutationer i relativt små mængder, som ikke kunne opdages.
6. **Signeret malware**. Malware signeret med stjålne certifikater udgjorde en stigende trussel i 2011. Ved at signere malware var det muligt at øge kodens troværdighed, og få øgede privilegier på det inficerede system.
7. **Stigende brug af social engineering**. Igen i år blev brugerinformation benyttet til målretning af angreb på borgere og organisationer. Særligt ved en række spear phishing angreb mod internationale organisationer var brugen af social engineering udtalt. Angrebet mod RSA i starten af året var det mest omtalte.
8. **Udnyttelse af sociale netværk**. Sociale netværk var en stigende kilde til spredning af spam, svindel, malware via nyhedsfeeds og beskeder fra personer, der udgav sig for at være venner. En del af problematikken skyldes, at op mod 65 procent af alle links benytter URL-forkortere, så der ingen reel mulighed er for at se destinationen.
9. **Spam udsendes fra kompromitterede mail-konti**. Lukningen af flere botnet har medført, at kompromitterede mail-konti i stigende grad benyttes til udsendelse af spam og phishing-mails.
10. **Android Market**. Android Markets åbenhed viste sig at være en platform for misbrug i form af malwareinficerede applikationer, hvidvaskning af penge og betalingsapplikationer uden reelt indhold.

AVG, 2011; "*AVG community powered threat report - Q2 2011*".
Microsoft, 2011; "*Microsoft security intelligence report (volume 11)*".
Toptenreviews, 2011; "*Malware trends according to Symantec*".

7.2. Fremtidige trends

Mange af de tendenser vi har set i løbet af 2011, forventer vi vil fortsætte de kommende år. Når vi så alligevel ikke har medtaget dem på listen over kommende trends, skyldes det den manglende nyhedsværdi, samt at de i medieomtale og opmærksomhed vil blive overskygget af andre og nyere trends.

Informationsteknologien undergår i disse år en hastig forandring. Flere systemer forbindes på måder, som gør det mere komplekst at overskue, hvilke problematikker der kan være forbundet hermed. Som eksempel på dette er udbredelsen af smart elektronik til hjemmet. Et fjernsyn kan i dag koble sig på internettet, installere applikationer, streame indhold fra computeren, betjenes via telefonen og meget mere. I modsætning til computeren har vi kun ringe mulighed for at konfigurere og overvåge sikkerheden på fjernsynet, da hardware og software leveres og betjenes som en "blackbox". Både producenter og forbrugere har her et medansvar da begge parter hovedsageligt har øje for funktionaliteten.

Indtil videre har vi ikke konstateret angreb på den stigende mængde netforbundet smart elektronik, der sniger sig ind i vores hjem. Vi tror, at det er stilhed før stormen. Tidligere tider har vist, at det primært er et spørgsmål om, hvornår en given teknologi og/eller platform opnår en kritisk masse, før det kan betale sig at udnytte den. Med en lukket teknologi, der behandler og lagrer stadig flere data, kan vi frygte, at forbrugerelektronikken ender som det bløde mål for de internetkriminelle. Deres mål er nemlig som tidligere at skaffe sig adgang til vores pengepung.

"Indtil videre har vi ikke konstateret angreb på den stigende mængde netforbundet smart elektronik, der sniger sig ind i vores hjem. Vi tror, at det er stilhed før stormen."

Anonymous-bevægelsen og Lulzsec satte i 2011 fokus på, hvor effektivt internettet kan være som middel til global aktion. En stigende utilfredshed med finanssektorens rolle i den vestlige verdens økonomiske krise, de siddende regeringer, dyrevelfærd, miljø og tilsvarende enkeltsager, får os til at spå, at hacktivisme er en aktionsform, der vil vokse. Vi tror således, at vi i de kommende år vil se flere politisk motiverede defacements, DDoS-angreb og datatyverier rettet mod virksomheder, politiske partier og myndigheder, der ikke deler holdninger, politisk standpunkt eller etisk holdning med dem, der angriber.

Som reaktion på dette og en terrortrussel, der med angrebet i Oslo er blevet mere nærværende, tror vi, at overvågning og registrering af borgernes gøren og laden vil tage til. Mange steder i den vestlige verden vil man tilpasse lovgivningen og udnytte den til det yderste, for at komme et eventuelt angreb i forkøbet. Herhjemme er overvågning af borgere, der mistænkes for socialt bedrageri, skattesnyd, forsikringssvindel og lignende taget til i styrke. Også den form for overvågning og registrering venter vi vil blive mere udbredt i årene, der kommer.

Også de internetkriminelle vil i stigende grad overvåge os og benytte informationen til at målrette angreb, som skal nedbryde vores mentale forsvarsværker. Vi har tidligere set falske anmodninger om pengeoverførsler til venner eller familiemedlemmer, som angiveligt var blevet bestjålet på rejser. På samme måde kan de informationer og relationer vi selv offentliggør på for eksempel sociale medier, blive benyttet til at inficere vores enheder med malware og lignende. Social engineering er stadig det nye sort.

Organisationernes nøglemedarbejdere kan blive mål for angreb, som har fokus på at stjæle fortrolige virksomhedsoplysninger, forsinke produktionen og andet. Et element i de målrettede virksomhedsangreb vil være malware, der har fokus på den enkelte organisations specifikke systemer. Vi tror, at der kommer flere angreb, der som Stuxnet er tilpasset specifikke virksomhedssystemer.

Det kan blandt andet være målrettede angreb på e-handelssider og betalingsplatforme. Mens bankerne gennem de seneste år har oprustet deres sikkerhedsmekanismer, kan netbutikkerne blive mål for tyveri af kreditkortinformationer. Sony Playstation Network viste, at det var muligt, og de kommende år vil mindre og mere lokale online butikker og -tjenester også komme under pres fra internetkriminelle.

Heller ikke de mobile platforme kommer i de kommende år til at gå fri. Stigende udbredelse og brug af mobile enheder vil medføre en stigende interesse fra de internetkriminelles side. Åbenheden i Android Market gør det til et oplagt medie for spredning af alle typer af malware. Også QR-koder, SMS'er og MMS'er kan som kompromitterede websider målrettet mobile enheder være midlet til spredning af spam, phishing og malware. For eksempel forventer vi at se malware, som låser brugerens enhed, som herefter kun kan benyttes efter pengeoverførelse via for eksempel Paypal, Bitcoin eller lignende.

Sommerens europamesterskaber i fodbold vil som de fleste store begivenheder have de internetkriminelles fokus. Vi tror, at vi op til og under begivenheden vil se en intensivering af angreb. Det vil primært være i form af phishing- og spammails, der skal lokke os til sider med malware eller køb af alt fra spillertrøjer til billetter, som muligvis er kopierede, falske eller ikke eksisterer.

Indførelsen af ny teknologi byder både på nye muligheder og nye udfordringer. HTML5 er ved at vinde indpas som det foretrukne medie til præsentation af video og interaktivt webbaseret indhold. I de kommende år forventes IPv6 at blive rullet ud. Begge teknologier vil blive forsøgt udnyttet.

Nedenfor kan du læse mere om vores forudsigelser for de kommende år:

1. **Sårbarheder og angreb på smart hjemmeelektronik**. De kommende år vil der blive frigivet sårbarheder i smart elektronik. Lagring af kreditkortinformationer, kontoinformationer til sociale netværk og lignende vil medføre 0-dags-angreb målrettet de enheder. Det vil her primært være spilkonsollen, smart-tv'et og smart-tv-bokse, der vil være målet.
2. **Hacktivisme**. Internettet har gjort det nemt og næsten risikofrit anonymt at lufte sine holdninger og sympatier gennem hacking af offentlige institutioner, globale virksomheder og politiske partier eller grupperinger. 2011 har for nogle vist vejen, så det at hacke for en sag vil blive en mere udbredt aktionsform både globalt og herhjemme.
3. **Mere overvågning**. Et stigende pres på myndighederne om at imødegå truslen om terrorangreb, internetaktivisme, hacking og organiseret kriminalitet vil medføre stigende overvågning.
4. **Den menneskelige faktor**. Social engineering er midlet, der lokker os til at sænke paraderne. Den stigende brug af sociale medier vil medføre et stigende misbrug af de informationer, man selv publicerer. Særligt organisationernes ledere og mellemledere er blevet synlige og kan blive mål for spear phishing-angreb, som vi så det i tilfældet med RSA.
5. **Malware målrettet virksomheder**. Stuxnet, angrebet på RSA og tilsvarende var kun en begyndelsen. Vi kommer til at se flere malware-angreb, som er målrettet specifikke virksomheder, deres systemer og data.
6. **Angreb på online betalingstjenester og -butikker**. Selv om angrebet på Sony Playstation Network nok ikke bliver overgået, viste det vejen for tyveri af kreditkortinformationer. Internetbutikker, online spillesider og lignende tjenester, der selv står for transaktionen og lagring af kreditkortdata bliver i stigende grad mål for angreb.
7. **Nye angreb på mobile platforme**. Angreb på mobile enheder vil nå nye højder i de kommende år. Smartphones og tavle-pc'er benyttes i dag som små computere. De er kun sjældent krypteret eller beskyttet af firewall, antivirussoftware og lignende. Vi vil se trojanske heste, ransomware og orme, der spredes via links i SMS'er, MMS'er og QR-koder, som er målrettet de mobile platforme.
8. **Europamesterskaberne i fodbold**. Sommerens europamesterskaber i fodbold er en begivenhed, der vil blive forsøgt misbrugt. Facebook-links til resultater, de bedste mål og lignende vil ligesom mails, der reklamerer for billige billetter til kampene, føre brugerne til malware-inficerede sider, falske webbutikker og tilsvarende.
9. **Målrettede angreb på HTML5**. Udbredelsen af HTML5 gør standarden til et attraktivt mål for internetkriminelle. For eksempel vil det fælles scripting-API blive udnyttet til at ramme på tværs af platforme og browsere.

"Sommerens europamesterskaber i fodbold vil som de fleste store begivenheder have de internetkriminelles fokus."

10. **Angreb der udnytter IPv6**. Udrulningen af IPv6 tager til i løbet af de kommende år. Ud over de ressourcer det vil kræve, kan manglende erfaring og sikkerhedsværktøjer, som endnu ikke understøtter standarden, medføre nye typer angreb. For eksempel har man på bloggen iniqua.com påvist muligheden for spoofing gennem IPv6-tunneller.

Iniqua.com, 2011; "*Hacking IPv6 III – IP6 spoofing in 6in4 tunnels*".

8. Anbefalinger

På baggrund af rapportens konklusioner giver vi i dette afsnit en række anbefalinger til, hvordan du kan være med til at skabe mere sikkerhed. Det hvad enten du er borger, it-ansvarlig eller beslutningstager. Vi håber, at du finder dem brugbare og vil lade dem danne grundlag for refleksioner over, hvordan vi kan samarbejde på tværs af organisationer, brancher og sektorer. På den måde kan vi på bedste vis sikre de danske it-aktiver.

8.1. Anbefalinger til borgerne

Som sidste år har vi valgt at videregive de fem råd som du kan finde på "Opdater din pc", hvor de er yderligere uddybet. Grundlæggende er der enighed om, hvordan vi beskytter vores computere. Selvom teknologien forandrer sig, er metoderne stadig de samme. Vi har suppleret dem med fem anbefalinger til beskyttelse af mobiltelefon og tavle-pc'er, brug af passwords, mail og sociale netværkstjenester samt beskyttelse af privatlivets fred.

Beskyt din pc:

1. **Beskyt din pc mod ondsindede programmer**. Brug firewall og opdateret antivirus program.
2. **Hold dine programmer opdateret**. Brug automatisk opdatering, hvor det er muligt. Opdater også tredjepartsprogrammer og tilføjelsesprogrammer til browseren, eventuelt ved brug af programmerne PSI fra Secunia eller Heimdal fra CSIS.
3. **Slå krypteringen til på dit trådløse netværk**. Brug som minimum WPA2-kryptering, og brug et sikkert password (se også anbefaling nummer 7).
4. **Indstil sikkerhedsniveauet i din browser**. Herved kan du sikre dig, at du som minimum bliver spurgt inden overførsel af informationer, filer og programmer.
5. **Installer kun programmer du har brug for**. Sårbarheder i ubrugte programmer udgør også en risiko, særligt hvis de ikke holdes opdateret.

Smartphones og tavle-pc'er reelt små computere, der bruges som sådanne til at surfe på nettet og bruge mail, Facebook, netbank med mere. Sikkerheden på de bærbare enheder adskiller sig ikke væsentligt fra den almindelige pc. Når det alligevel er nødvendigt at give yderligere anbefalinger, skyldes det, at de er mere mobile og derfor oftere glemmes eller stjæles med risiko for at andre kan læse de data, som er gemt på dem.

Beskyt din smartphone og tavle-pc:

6. **Brug passwordbeskyttelse på mobile enheder, og benyt om muligt kryptering af data**. Husk at opdatere din bærbare enhed, samt at smartphones og lignende ofte også giver adgang til mail-kontoen, Facebook og lignende.

Opdatering af sårbare systemer giver kun ringe beskyttelse, hvis ikke der er en nemmere måde at tilgå data på. Brug af standard-passwords og/eller passwords der er nemme at gætte, udgør en ligeså stor risiko som ikke opdaterede systemer.

Særligt på tjenester, der er placeret på nettet, hvor du ikke selv kan beskytte dem på anden vis.

Beskyt dine data med password:

7. **Brug individuelle sikre passwords på alle tjenester**. Et sikkert password består af minimum otte tegn indeholdende både store og små bogstaver, tal og specialtegn. Undgå standard brugernavne og –passwords og husk, at brugernavne og passwords er personlige.

Størstedelen af de mails vi modtager, har vi ikke bedt om eller forventet at modtage. I de fleste tilfælde er der tale om spam-, virus-, eller phishingmails. Heldigvis sørger mailfilteret hos vores internetudbyder, arbejdsplads, Google og lignende for, at det meste bliver sorteret fra inden det havner i indbakken. Alligevel slipper noget igennem og kan udgøre en risiko, hvis vi ikke er bevidste om det.

Brug mail med omtanke:

8. **Lad være med at besvare eller klikke på links og vedlagte filer i mistænkelige mails**. Vær opmærksom på ,at din bank, kreditkort- eller mailudbyder aldrig beder dig bekræfte dine kontooplysninger over mail. Links kan føre dig til websider med skadelig kode, og vedlagte filer kan indeholde virus og lignende. Slet mailen, hvis du er i tvivl.

Personlige data som du selv eller andre lægger på nettet, kan misbruges eller benyttes i sammenhænge, som kan være vanskelige at overskue. Det gælder også de data, der afgives ved kursustilmeldinger og jobansøgninger eller som skal indtastes ved tilmelding til online tjenester og lignende. Mange data er du ikke selv herre over, om ender på nettet. Desuden gælder, at læserbreve, debatindlæg, deltagerlister fra diverse aktiviteter samt billeder fra julefrokosten eller din seneste ferie ofte vil være tilgængelige på internettet, selv om du sletter dem. De kan på et tidspunkt blive set af nogen, som du ikke ønsker skal se dem.

Beskyt privatlivets fred på nettet:

9. **Læg kun oplysninger om dig selv på nettet, som alle til enhver tid må se**. Vær også opmærksom på, hvilke oplysninger du afgiver til andre. Sørg for at læse aftalevilkår igennem, så du ved, hvordan dine data bruges og hvad andre publicerer om dig. Tilsvarende skal du spørge, inden du lægger billeder og oplysninger ud om andre end dig selv.

Sociale medier misbruges i stigende grad til spredning af malware og social engineering. Ud over risikoen for misbrug af din egen konto bør du være opmærksom på de oplysninger, du giver andre adgang til, venneanmodninger fra folk du ikke kender, samt links til applikationer og hjemmesider, som er inficeret med malware. Nedenstående anbefaling kan suppleres med DK•CERT og KOMFOs vejledning til sikker brug af Facebook.

Brug af sociale netværkstjenester:

10. **Beskyt dine private oplysninger og vær kritisk over for andres informationer og motiver.** Vær opmærksom på hvem du giver adgang til. Brug privatlivsindstillinger til at beskytte dine personlige oplysninger.

Brug tredjepartsapplikationer med omtanke, og vær opmærksom på informationer, du modtager fra andre. Sender dine venner ikke normalt links til videoklip med spektakulære titler, anbefalinger af applikationer og lignende, kan det som med venneanmodninger fra fremmede være en god idé at ignorere det.

Selv om du følger ovenstående anbefalinger, byder brugen af informationsteknologi på risici, som kan være vanskelige at overskue og vejlede om. Derfor gælder det om at forholde sig kritisk til mediet og de informationer du modtager og afsender. Tænk dig om og brug din sunde fornuft.

CSIS; "*Heimdal*".
DK•CERT & KOMFO, 2010; "*Styr dit privatliv på Facebook*".
Opdaterdinpc, 2011; "*Gode råd*".
Secunia; "*Download - Secunia Personal Software Inspector (PSI)*".

8.2. Anbefalinger til it-ansvarlige

Mens det hjemme i privaten er den enkelte bruger, der er ansvarlig for sikkerheden, varetages den rolle i organisationerne centralt af ledelsen og de it-ansvarlige. De it-ansvarlige varetager den praktiske del af informationssikkerheden på de systemer, hvor udvikling og drift endnu ikke er blevet outsourcet. De har således et ansvar for, at organisationens systemer og data er tilgængelige, samtidig med at integritet og fortrolighed opretholdes. Retningslinjerne for dette arbejde bør være beskrevet i organisationens informationssikkerhedspolitik.

En væsentlig udfordring er klassificeringen af en stadig stigende mængde data og information. Hvis vi ikke kan klassificere, hvad der er følsomt, er det vanskeligt at lave konsekvens- og risikovurdering, som i sidste ende skal føre til politikker, regler og procedurer. Også i dette arbejde bør de it-ansvarlige i samarbejde med organisationernes ledelse spille en rolle, da det i sidste ende er dem, der skal implementere og håndhæve de vedtagne procedurer.

At holde de ansattes arbejdsstationer sikre og opdaterede udgør et grundlæggende element i organisationens samlede sikkerhed. Det er de it-ansvarliges ansvar. Som en naturlig del af informationssikkerhedspolitikken bør der implementeres procedurer, der sikrer, at medarbejdernes udstyr er sikret mod angreb. Særligt hvor medarbejderne har mulighed for at medbringe og bruge deres egne enheder, bør det have skærpet fokus.

De ansatte, deres pc'er og mobile enheder:

1. **Hold brugernes enheder opdaterede**. Implementer procedurer til at sikre, at der benyttes automatisk opdatering på alle enheder samt at brugerne benytter centralt styret firewall og opdateret antivirusprogram med mere.
2. **Hold løbende organisationens ansatte opdateret**. Hold organisationens ansatte opdateret med informationssikkerhedsproblematikker, der er relevante for netop dem.

En væsentlig del af informationssikkerheden handler i dag om at holde sig opdateret med de aktuelle trusler. Her spiller de it-ansvarlige en central rolle i forhold til at komme med input til den løbende opdatering og revision af

organisationens informationssikkerhedspolitik. Det er trods alt dem, der oplever angrebene i de systemer, som de er ansvarlige for.

Informationssikkerhedspolitik:

3. **Løbende opdatering af organisationens informationssikkerhedspolitik.** Sørg for at aktuelle trusler inkluderes i organisationens informationssikkerhedspolitik. Sørg også for, at brugerne kender indholdet i politikken. Awareness handler ikke kun om, at brugerne er opdateret med potentielle trusler, men i lige så høj grad om de retningslinjer, som de skal følge og hvorfor. Sørg derfor for at holde brugerne bekendt med ændringer i informationssikkerhedspolitikken.
4. **Retningslinjer for brug af mobile enheder.** Udarbejd regler og procedurer for brug af egne computere med videre og gør det klart, hvordan et stigende krav om brug af og tilgængelighed fra multiple platforme skal håndteres. Er det for eksempel muligt at anskaffe samme krypterings-software og antivirus til alle platforme?

Det er ikke kun brugerne og deres enheder, som udgør en risiko for organisationens sikkerhed. Også organisationens forretningssystemer kan være sårbare og bør holdes opdaterede for at sikre mod angreb.

Organisationens forretningssystemer:

5. **Hold systemerne opdaterede**. Benyt automatisk softwareinspektion, scanninger og penetrationstests og abonner eksempelvis på varsling af sårbarheder. Services, der ikke bruges, kan også være sårbare og misbruges. Luk derfor for services, som ikke benyttes, og minimer adgangen fra segmenter og brugerkonti, der ikke skal benytte den pågældende service.
6. **Giv kun mulighed for brug af stærke passwords**. Implementer procedurer til at sikre, at brugerne kun har mulighed for at definere stærke passwords lokalt såvel som på organisationens forretningssystemer.
7. **Valider brugersendte data**. Sørg for at alle data, der sendes til serveren valideres inden eksekvering og/eller lagring på organisationens webapplikationer.

Fortrolighed af data vedrører ikke kun organisationen selv. Hvis for eksempel kunder, leverandører og samarbejdspartnere skal bevare tilliden til organisationen, skal fortrolige data vedblive at være fortrolige. Tænk derfor dataadgang og kryptering ind i alle scenarier.

Det er ofte menneskelige fejl, som er årsag til tab af fortrolige forretningsdata. Gør organisationens data tilgængelige på en sikker måde. Giv for eksempel medarbejderne mulighed for at transportere data i krypteret form. I modsat fald risikeres det, at data sendes over Gmail-kontoen, overføres til Dropbox eller noget helt tredje, når de skal benyttes uden for arbejdspladsen. Her har man ikke har kontrol over sikkerheden.

Fortrolighed af data:

8. **Overvej, hvem der skal have adgang til data**. Begræns adgangen til det nødvendige og brug eventuelt systemer til Data Leak Prevention for at sikre, at organisationens informationssikkerhedspolitik overholdes.

9. **Krypter forretningskritiske data**. Det gælder både i skyen, på serveren, i transaktionen og ved anden transport på fx. bærbare computere, smartphones og andre mobile enheder.

Organisationens leverandører og kunder udgør en potentiel risiko, hvis ikke man er bevidste om hvilke data de har adgang til og hvordan de behandler dem. Tænk sikkerhed ind i hele forsyningskæden. Undersøg markedet og stil krav til leverandørerne, således at krav til drift og sikkerhed indføres i kontrakten. Betragt herefter jeres kunder og leverandører som samarbejdspartnere snarere end som netop kunder og leverandører.

Samarbejdsrelationer og leverandører:

10. **Tænk kunder og leverandører som samarbejdspartnere**. Benyt aktivt organisationens risikovurderinger ved udfærdigelse af kravspecifikationer og kontrakter. Tænk herefter internetudbydere, hostingselskaber, outsourcing-leverandører og kunder som samarbejdspartnere. Det er trods alt dem, der kender sikkerhedsproblematikker i deres systemer. Sørg samtidig for at modtage tilstrækkelig information og uddannelse.

8.3. Anbefalinger til beslutningstagere

På et overordnet plan er det beslutningstagerne, der skaber rammerne for, hvordan vi kan beskytte danskernes it-aktiver mod en stigende trussel fra internationale organiserede kriminelle. Hvad enten man sidder som beslutningstager i erhvervslivet, det offentlige system eller på det politiske plan, har man medansvar for og -indflydelse på denne proces.

Det er vores håb, at nedenstående anbefalinger vil blive taget imod i en ånd af samhørighed og samarbejde. Sådan kan vi på bedst mulig vis sikre både samfundet, borgerne og erhvervslivet uden at skulle gå på kompromis med privat livets fred og vores grundlovssikrede rettigheder.

I debatten om it-teknologien som motor for udbredelse af informationssamfundet herhjemme mener vi, at man med mulighederne som fokus og guleroden som incitament i samarbejde skal skabe rammerne for sikring af danskernes it-aktiver og økonomi. Det er i den ånd, vi håber, du vil tage nedenstående anbefalinger til dig. Eller som Dells teknologidirektør Don Smith udtalte i forbindelse med et besøg i Danmark:

"I stedet for at stå for enden af vejen med et rødt flag og sige 'det må du ikke', så skal sikkerhedsfolkene være en del af de strategiske og taktiske ændringer hele tiden."

Det oplagte punkt er her at starte med at inkluderer informationssikkerheden i strategien for, hvordan vi benytter informationsteknologien som vækstskaber.

It-strategi:

1. **Tænk informationssikkerhed ind i strategien**. Inkluder informationssikkerhed i de langsigtede strategier for brug af teknologien. I modsat fald kan kompromittering af systemer og data medføre store økonomiske konsekvenser i form af manglende indtjening, tabt arbejdstid, bod og

"I stedet for at stå for enden af vejen med et rødt flag og sige 'det må du ikke', så skal sikkerhedsfolkene være en del af de strategiske og taktiske ændringer hele tiden."

- Don Smith, teknologidirektør, Dell

mistet omdømme.

2. **Prioriter og synliggør risikostyring**. Lad risikostyringsaktiviteter være en naturlig og synlig del af den fremadrettede brug af informationsteknologi ved at lade dem indgå som obligatorisk del af strategien.
3. **Skab samarbejdsrelationer omkring informationssikkerhed**. Som alt andet udvikles informationssikkerhed ikke i lukkede fora. Skab samarbejder for hvordan informationssikkerhed inkluderes i strategien. Inkluder leverandørers, kunders og øvrige interessenters perspektiver og skab fælles løsninger der gavner helheden.

I sikkerhedssammenhæng er informationssikkerhedspolitikken strategiens forlængede arm. Det er her, risikostyringen konkretiseres og gøres operationel. Vi mener, at der bør være transparens omkring denne proces, således at brugerne bidrager, kender og forstår beslutninger omkring brug af organisationens it-aktiver.

"I sikkerhedssammenhæng er informationssikkerhedspolitikken strategiens forlængede arm. Det er her, risikostyringen konkretiseres og gøres operationel."

Informationssikkerhedspolitik i et perspektiv af god selskabsledelse:

4. **Kommuniker og gå i dialog med brugerne**. Sørg for at kommunikere muligheder og begrænsninger såvel som rettigheder og pligter til brugerne af informationsteknologi. Indgå i dialog og samarbejde omkring løsningen af konkrete problemstillinger.
5. **Tag stilling til brug af konkrete teknologier**. Beskriv hvorledes det fremadrettet ønskes, at teknologien bruges, hvilke krav der stilles til brugerne og ikke mindst hvorfor.
   Synliggør politikker, der specificerer regler for brug af organisationens installationer og indfør procedurer, der implementerer reglerne.

2011 bød på flere eksempler på lækage af personfølsomme oplysninger. Herhjemme har vi endnu ingen lovmæssig hjemmel til at sikre, at kunder hvis data lækkes, bliver informeret herom. Vi mener, at kunden har ret til at få besked, således at denne i tide kan tage sine forholdsregler.

Informationspligt ved datatyveri:

6. **Lad informationspligt være lovpligtig ved datalækage**. Dansk lovgivning bør omfatte pligt til at informere myndighederne og organisationernes kunder ved kompromittering af systemer eller data, der vedrører kunden. I forlængelse heraf bør der oprettes standarder for, hvornår informationspligten træder i kraft, og hvad den omfatter.

Viden om hvordan informationsteknologien kan bruges, er et fundamentet for, at vi kan benytte den til at skabe økonomisk vækst. På samme vis er viden om risici ved brug af teknologien afgørende for, at vi kan beskytte os mod misbrug. Vi mener derfor, at man bør prioritere uddannelse i, hvordan vi på sikker vis kan udvikle og bruge informationsteknologien.

Prioriter uddannelse:

7. **Afsæt ressourcer til uddannelse**. Viden og erfaring er et grundlæggende fundament for at kunne varetage informationssikkerhedsarbejdet. Prioriter derfor uddannelse og styrk aktiviteter til videndeling, samarbejde og oplysningskampagner.

At skabe 100 procent sikkerhed er en utopi i en stadig mere forbundet verden, da informationssikkerhed er en afvejning af risiko, konsekvens og økonomi. Det er derfor nødvendigt at vide, hvordan skaden begrænses, når det går galt. En klar beredskabsplan er en væsentlig del af organisationens risikostyring, der i sidste ende kan spare mange penge.

Vær beredt:

8. **Hav beredskabsplanen på plads**. Sørg for, at der udfærdiges fyldestgørende beredskabsplaner for kritiske forretningsaktiver, der klart specificerer, hvem der skal foretage sig hvad, hvornår og hvorfor. Det sikrer samtidig et detaljeret billede af hele infrastrukturen, hvilket naturligvis skal holdes opdateret.

Gennem de sidste års økonomiske krise har mange organisationer måttet svinge sparekniven. Selv om de systemer og data man søger at beskytte, ikke er blevet hverken færre eller mindre komplekse, har det flere steder medført færre midler til informationssikkerhed. En sådan beslutning kan dog koste dyrt. Det måtte den hollandske certifikatudsteder DigiNotar sande i 2011. Efter at være blevet kompromitteret erklærede de sig den 19. september konkurs.

Informationssikkerhed koster:

9. **Brug de fornødne ressourcer**. At spare på informationssikkerheden kan i det lange løb være en dyr fornøjelse. Økonomisk knaphed bør ikke give anledning til at gå på kompromis med god selskabsledelse og grundlæggende principper for informationssikkerhed. I sidste ende kan det koste langt mere end det som er sparet. Overvej om der er råd til at spare på informationssikkerhed.

Vi har ikke råd til manglende samarbejde. På it-området mangler der dog i øjeblikket nogle visioner for, hvordan vi kan trække samarbejdet i en retning, hvor det tilgodeser ikke blot enkelte sektorer, men hele det danske samfund. En strategi for hvordan vi i fremtiden ønsker teknologien brugt, så den på sikker vis kan understøtte en gunstig samfundsudvikling også for organisationerne og den enkelte borger.

National it-strategi:

10. **Lav en national it-strategi, der inkluderer det offentliges, organisationernes og borgernes informationssikkerhed**. En national it-strategi, der sætter retning for udvikling, udbredelse og brug af teknologier og services. Uddannelse og forskning der understøtter den. Samarbejde på tværs af det private og offentlige samt informationssikkerhed, efterforskning og beredskab.

Version2, 2011; "*Dells teknologichef: Sikkerhedsfolk skulle have et los bagi*".

"Lav en national it-strategi, der inkluderer det offentliges, organisationernes og borgernes informationssikkerhed ."

9. Artikler fra første kvartal

Flere overskrifter og begivenheder har i løbet af første kvartal været med til at præge vores syn på udviklingen med hensyn til internetkriminalitet og -sikkerhed. Udvælgelsen af begivenheder var selvfølgelig præget af vores perspektiv på informationssikkerhed som CERT for Forskningsnettet. Enkelte historier udsprang derfor fra vores verden, snarere end det billede, som blev tegnet af medierne. Fælles er, at de var med til at tegne et billede af informationssikkerheden i hele det danske samfund.

9.1. Stigende it-investeringer giver øget sikkerhed

På trods af at de danske it-chefer ifølge en undersøgelse foretaget af Dansk IT havde afdæmpede forventninger til it-investeringerne i 2010, viste året sig at slå alle rekorder. Grundlæggende betyder den fornyede optimisme i erhvervslivet, at man ud over større effektivitet også opnår bedre sikkerhed.

Under den finansielle krise havde man udsat investeringer til blandt andet fornyelse af hardware. Med ny tiltro til fremtiden blev 2010 året, hvor man igen investerede i it, og året endte med et rekordsalg på 65 milliarder kroner. Salget var primært båret af pc'er, servere og software, mens investeringer i strategiske it-projekter og -løsninger var under niveauet for 2008. Også for både 2011 og 2012 har analysehuset IDC en forventning om vækst.

Investeringer i nye computere betyder i vid udstrækning også, at softwareplatformen fornys. Således kan det forventes, at mange organisationer planlægger eller allerede er gået over til Windows 7, der vurderes at være mere sikker end Windows XP. Dette skifte kan vi aflæse på webstatistikken for www.cert.dk, hvor andelen af besøgende der benytter Windows XP, fra januar 2010 til januar 2011 er faldet fra 54 procent til 42 procent. Tilsvarende er besøgende med Windows 7 i samme periode steget fra 12 procent til 25 procent.

Med overgangen til Windows 7 følger også en ny og mere sikker version af browseren Internet Explorer. Således var der i januar 2011 kun 28 procent, der benyttede Internet Explorer i ældre versioner end 8 mod 37 procent året tidligere. En stor andel er også overgået til at bruge alternative browsere som for eksempel Mozilla Firefox eller Google Chrome. De stod i januar 2011 for mere end 25 procent af de besøgende. De alternative browsere hentes og bruges primært i nyeste version.

Business.dk, 2011; "IT-salget satte rekord i 2010".
Dansk IT, 2010; "*CIOViewpoint - Krisens spor*".
Dansk IT; "*Dansk IT*".

9.2. Industrispionage og angreb mod itinfrastruktur

En undersøgelse foretaget af Dansk IT blandt 119 danske it-chefer i både den offentlige og private sektor viste, at 26 procent af organisationerne havde været udsat for hacker- eller virusangreb, der havde til formål at lamme it-infrastruktur eller produktionssysemer.

Dansk IT

Dansk IT er en forening for itprofessionelle med mere end 5.600 medlemmer. Foreningen er en non-profit organisation, der arbejder uafhængigt af politiske tilhørsforhold, fagforenings- eller brancheforeningsinteresser med det formål at udbrede anvendelsen af it til gavn for professionen, samfundet og den enkelte.

Freningen repræsenterer medlemmernes interesser på den politiske scene og gennem blandt andet netværk, konferencer, gratis på-vejhjem-møder og lignende.

Truslen fra Stuxnet og tilsvarende har medført, at 55 procent har indført skærpede informationssikkerhedsforanstaltninger.

Omvendt har kun 10 procent af virksomhederne indført særlige informationssikkerhedsforanstaltninger i forhold til nøglemedarbejderes tjenesterejser. Det sker på trods af, at undersøgelsen indikerer, at det bedste værn mod industrispionage er at vanskeliggøre medarbejdernes mulighed for at medbringe data uden for organisationen. Resultatet skal ses i relation til, at kun 5 procent tilkendegav, at deres organisation havde været udsat for industrispionage, mens 29 procent ikke var vidende om det. Kun i ét tilfælde var industrispionage udført som et computerbaseret angreb.

28 procent af undersøgelsens respondenter mente, at det var en national myndighedsopgave at minimere truslen fra angreb som for eksempel Stuxnet mod organisationernes it-infrastruktur og produktionssystemer. Lignende holdninger har i forbindelse med bekæmpelse at botnet været fremført af Dansk Industri. 13 procent mente, at bekæmpelsen burde ske i samarbejde med en aktiv offentlig myndighed og/eller internetudbyderne.

Dansk IT, 2011; "*CIOViewpoint - Industrivirus og industrispionage*".

9.3. Dansk samarbejde om bekæmpelse af botnet

Den 16. februar blev det offentliggjort, at Videnskabsministeriet i samarbejde med ISP Sikkerhedsforum går ind i bekæmpelsen af botnet på den danske del af internettet. Samarbejdet leverer svar på et forslag, der tidligere blev stillet af Dansk Industri om statslig bekæmpelse af botnet.

Samarbejdsaftalen mellem IT- og Telestyrelsen (GovCERT), DK•CERT og ISP Sikkerhedsforum udstikker rammerne for samarbejdet. Det giver mulighed for at beskytte mod botnet, som for eksempel forsøger at stjæle adgangsoplysninger til borgernes netbank eller andre af deres personlige data. Om aftalen udtalte vicedirektør i IT- og Telestyrelsen, Marie Munk:

"*Såkaldte botnet - dvs. computere, der organiseres i netværk gennem ondsindet software og bruges til at udsende spam og foretage koordinerede hackerangreb – er en trussel for danskernes brug af internettet. Det er derfor vigtigt med et solidt samarbejde om at bekæmpe botnet mellem de relevante myndigheder og de udbydere, som leverer internet til virksomheder, myndigheder og borgere. Den netop indgåede aftale styrker dette samarbejde.*"

Danmarks Radio, 2010; "*DI: Staten bør bekæmpe it-kriminelle*".
Govcert.dk, 2011; "*Styrket samarbejde i bekæmpelsen af botnet*".

9.4. Danske netbutikker under angreb

"I takt med at netbankerne implementerer sikkerhedsmæssige modforholdsregler, tror vi, at fokus kan flytte sig til større lokale webshops, der ikke i samme grad som bankerne har implementeret informationssikkerhed som del af deres forretningsmodel."

ISP Sikkerhedsforum

ISP Sikkerhedsforum blev dannet 6. maj 2004 af en række danske internetudbydere for at styrke udbydernes bidrag til indsatsen mod virus-, orme-, hackerangreb og spam.

ISP Sikkerhedsforum består af repræsentanter fra de fleste danske internetudbydere og repræsenterer størstedelen af internetbrugerne i Danmark.

Ovenstående citat fra vores egen "Trendrapport 2009" synes nu at være blevet virkelighed. Med kun seks vellykkede netbankindbrud i 201018 er danske netbanker nu blevet så sikre, at de it-kriminelle har fundet andre markeder. Det nye mål er netbutikkerne, som ifølge direktør Poul Thyregod fra Proshop oplever en voldsom stigning i antallet af sager, hvor stjålne kreditkortoplysninger bliver brugt til svindel.

Svindlen foregår ved, at kriminelle med stjålne kreditkortoplysninger køber elektronik fra netbutikkerne. Varen sendes til intetanende muldyr i Danmark, som pakker den om, og sender den videre til modtagere i udlandet, typisk Østeuropa. De danske muldyr, som risikerer en politianmeldelse, er ofte rekrutteret via jobannoncer fra tilsyneladende etablerede shipping- og kurerfirmaer i udlandet.

At rekrutteringen lykkes, skyldes troværdigt udformede jobannoncer, udstrakt brug af søgemaskineoptimering, personlig telefonisk kontakt samt brugen af "formelle" ansættelseskontrakter. Som taberne står netbutikken og muldyret.

Problemstillingen bliver ikke mindre ved, at mange danske netbutikker har alvorlige sikkerhedsfejl og således potentielt kan indgå i fødekæden for stjålne kreditkortoplysninger. En undersøgelse foretaget af firmaet Hackavoid viste, at 49 procent af de undersøgte danske netbutikker havde kritiske sårbarheder19. Otte procent af de undersøgte butikker havde SQL-injection-sårbarheder, som blandt andet kan misbruges til at læse informationer i databasen eller placere skadelig kode på den besøgenes computer.

DK•CERT, 2010; "*Trendrapport 2009*".
Finansrådet, 2011; "*Historisk få netbankindbrud*".
Version2, 2011; "*Hver anden danske webshop har alvorlige sikkerhedsfejl*".

9.5. Brute-force angreb fra skyen

Sidst i februar modtog DK•CERT en anmeldelse fra en institution på det danske Forskningsnet. En brugerkonto med svagt password var kompromitteret, og kontoen blev benyttet til at logge på en SSH-tjeneste, hvorfra man scannede efter andre SSH-servere på internettet.

På den kompromitterede SSH-server blev der fundet brugernavne og password til andre SSH-servere på internettet.

Som sådan var hændelsen ikke unormal. DK•CERT modtager dagligt rapporter om forsøg på brute-force-angreb. Alligevel giver den stof til eftertanke. I takt med at også de it-kriminelle tager regnekraften fra cloud-services til sig, øges risikoen for at passwords, som tidligere blev betragtet som relativt sikre, kan knækkes. Da en kompromitteret brugerkonto ofte giver potentiel adgang til flere af organisationens interne tjenester, stiller det nye krav til organisationens politikker omkring passwords. Blandt andet bør man på alle tjenester sikre sig, at brugerkonti låses efter eksempelvis tre ugyldige login-forsøg.

9.6. Smartphones, det nye mål

Efter tip fra bloggeren Lompolo valgte Google i starten af marts at fjerne 21 malware-inficerede apps fra Android Market.

De inficerede apps var alle legale gratis programmer, der var blevet ompakket og igen distribueret til Android Market, nu indeholdende skadelig kode. I løbet af de fem dage de var tilgængelige, estimeredes det, at mindst 50.000 brugere nåede at installere dem på deres Android-telefoner og tavle-pc'er.

Efterfølgende udtalte stifteren af antivirusproducenten Kapersky Lab, Eugene Kaspersky, i et interview med Version2, at han mente, at Android ville blive det næste mål for malware-udviklerne. Mobiltelefoner er i dag små computere, der benyttes til alt fra e-mail til nethandel og netbank. Incitamentet for at ramme mobiltelefonerne er til stede, og Googles fokus på udviklerne og operativsystemets åbenhed gør det til et naturligt mål for malware. Således mener han, at Androidplatformen vil overtage Windows' position som malware-skribenternes foretrukne mål.

I modsætning til Apples App Store er der på Android Market ingen kontrol af de apps, der lægges op. På mobiltelefoner hvor kun de færreste har installeret sikkerhedssoftware, kan det være et problem, når brugerne henter deres apps fra Android Market, som de må formode er en troværdig kilde.

Trendmicro, 2011; "*Google Android rooted, backdoored, infected*".
Version2, 2011; "*Eugene Kaspersky: Android bliver hackernes nye Windows*".

9.7. Nye cookie-regler beskytter privatlivet

Den 25. maj 2011 træder et nyt EU-direktiv i kraft, som har til formål at sikre privatlivets fred ved færdsel på nettet.

Artikel 5 stk. 3 i databeskyttelsesdirektivet betyder, at det kan blive betragtet som ulovlig indtrængen, hvis der uden brugerens accept gemmes noget lokalt på dennes harddisk, som ikke er en del af et program eller hjemmesides grundlæggende funktionalitet. Formålet er at sikre forbrugerne kontrol over, hvad for eksempel hjemmesider gemmer og henter af oplysninger på brugernes pc.

Hvordan den nye lov skal implementeres og håndhæves, står endnu hen i det uvisse. For eksempel giver spøgsmålet om brugeraccept nogle dilemmaer i forhold til, hvad brugerne skal acceptere og hvordan, samt hvor længe en accept er gældende. Problemet er også, om brugerne af en hjemmeside reelt forstår, hvad de accepterer og hvad det betyder for dem. Dertil kommer håndhævelse af loven for hjemmesider, som er placeret uden for EU.

Version2, 2011; "*Fovirret? Få styr på de nye cookie-regler*".

9.8. Hurtig udnyttelse af jordskælv i Japan

Fredag den 11. marts blev Japan ramt af et jordskælv, som medførte en altødelæggende tsunami. Kun ganske få timer efter jordskælvet kunne antivirusproducenten Trend Micro på deres blog fortælle, at søgninger efter nyheder og video fra katastrofen ledte til sider med falske antivirusprogrammer.

Udbredt brug af søgemaskineoptimering medførte, at søgninger efter nyt om katastrofen ledte til falske nyhedssider. Her blev de besøgende eksponeret for det

falske antivirusprogram MalFakeAV-25.

Katastrofen er det seneste eksempel på, hvordan interessen for aktuelle begivenheder stadig hurtigere udnyttes til spredning af malware.

Trendmicro, 2011; "*"Most Recent Earthquake in Japan" Searches Lead to FAKEAV*".

9.9. Microsoft knækker det berygtede Rustock botnet

Under kodenavnet "Operation b107" har Microsoft i samarbejde med flere sikkerhedspartnere samt U.S. Marshals Service knækket det berygtede Rustock botnet. Den koordinerede indsats startede ni måneder før, aktionen blev sat i gang den 16. marts 2011.

Der kom skred i tingene, da det lykkedes virksomheden FireEye at udarbejde en signatur på kommunikationen mellem botnetklienterne og -serverne. En unik indikator var, at kompromitterede computere forsøgte at hente de første 200 KB af Windows XP SP2. Formålet har været at teste for aktiv internetforbindelse og måling af hastigheden. Det kunne Microsoft bruge til at identificere inficerede computere – og dermed opnå yderligere indsigt i kommunikationsprocessen.

Microsoft udnyttede de juridiske muligheder i forbindelse med misbrug af deres varemærker til at opnå en dommerkendelse. Det gav U.S. Marshals Service lovhjemmel til at beslaglægge 26 command & control-servere fordelt over fem hostingselskaber i syv amerikanske byer. Med hjælp fra backboneleverandører afskar man samtidig de IP-adresser, der blev benyttet til at kontrollere botnettet. Rustock var nu knækket.

Man skønner, at omkring 1.000.000 maskiner stadig er inficeret, men inaktive i øjeblikket. Bagmændene er endnu ikke pågrebet.

Channelregister, 2011; "*Rustock Takedown: How the world's worst botnet was KO'd*".
Microsoft, 2011; "*Operation b107 - Rustock botnet takedown*".

Om Rustock

I sin storhedstid var Rustock ansvarlig for størstedelen af den udsendte spam på verdensplan. Selv efter lukningen af verdens største spam-affiliate-program var Rustock ansvarlig for mere end 30 procent af den samlede mængde spam.

Rustock var et avanceret botnet i forhold til Waledac, Mega-D og Szerbi. Kommunikation mellem de forskellige noder var kamufleret på en sådan måde, at det lignede almindelig dagligdagstrafik.

Kompromitterede maskiner blev inficeret med malware pakket ved hjælp af en egenudviklet krypteringsteknik, der fik den ondsindede kode til at fremstå som et pakket RA--arkiv. Spredningen foregik ved hjælp af hackede websites, hvor forskellige sårbarheder i internetbrowsere og plugins blev udnyttet.

Botnettets opbygning medførte, at Rustock var aktivt i mere end fire år. At det har været en lukrativ forretning understreges af, at udgiften alene på hosting af botnettets command & control-servere er opgjort til 10.000 dollar om måneden.

10. Artikler fra andet kvartal

Internetkriminaliteten medførte ifølge Europol et skift i de kriminelles demografiske profil. De individer som er engageret i internetkriminalitet, er personer med gode it-kvalifikationer, som ofte rekrutteres direkte fra universiteterne. Ud over behovet for it-kvalifikationer kan andre årsager findes i generel økonomisk afmatning, arbejdsløshed og ideologi.

Denne tendens afspejles til dels i de overskrifter, som vi i løbet af andet kvartal så som væsentlige. Enkelte af de udvalgte begivenheder er nemlig resultatet af økonomiske analyser, kreativitet og gode it-kvalifikationer kombineret med psykologisk indsigt og organisatorisk talent. Derudover bærer overskrifterne præg af vores perspektiv på informationssikkerhed som CERT for Forskningsnettet.

Europol, 2011; "*EU Organised Crime Threat Assessment - OCTA 2011*".

10.1. Sony blev hackernes yndlingsoffer

Den 20. april 2011 var en sur dag for ejere af en Sony PlayStation. Den dag lukkede Sony for Sony PlayStation Network (PSN). Årsagen til lukningen forblev en hemmelighed frem til den 22. april. Her fortalte Sony, at firmaet havde opdaget et hackerangreb på PSN og en anden online-tjeneste, Qriocity.

Allerede i begyndelsen af april satte hackergruppen Anonymous ind med et Denial of Service (DoS) angreb mod PSN og Sonys websteder. Det skete som reaktion på, at Sony havde anlagt sag mod udvikleren George Hotz, som fandt en metode til at bryde begrænsninger for den software man kan afvikle på en PlayStation 3. Den 10. april offentliggjorde Sony og George Hotz, at de havde indgået et forlig, men Anonymous fortsatte sine angreb.

Den 26. april oplyste Sony for første gang detaljer om hackerangrebet, der fandt sted mellem den 17. og 19. april. Her blev det klart, at brugernes personlige data var kommet i hackernes hænder. I de kommende dage viste det sig, at dataene, herunder passwords, ikke var krypteret.

Kreditkortoplysninger var dog angiveligt krypteret. Sony har ikke offentliggjort, hvor mange brugere det gik ud over – men kilder anslår, at data fra godt 70 millioner brugere kom i hackernes hænder.

På en af de hackede servere fandt Sony en fil, hvis indhold kunne tyde på, at Anonymous var involveret. Det nægtede Anonymous, der ikke tidligere har været forbundet med tyveri af kreditkortdata. Gruppen har i stedet været involveret i hacking med politiske eller ideologiske overtoner.

Undersøgelsen af PSN-angrebet førte til, at man opdagede et andet angreb. Det foregik den 16.-17. april og gik ud over Sony Online Entertainment, der driver en række online spil såsom EverQuest II og Clone Wars Adventures.

Ifølge en pressemeddelelse fra Sony blev der stjålet personlige data fra godt 24,6 millioner brugerkonti på Sony Online Entertainment. Hertil kommer knap 23.000 kreditkortnumre fra en database fra 2007. Den 14. maj begyndte PSN at gå i drift igen. Det samme gjaldt Sony Online Entertainment.

Siden de to store angreb er der fulgt en lang række mindre angreb på Sony-websteder. Nogle af dem er defacements, hvor hackere ikke fik adgang til fortrolige data, mens andre førte til tab af data. Det gælder blandt andet So-Net Entertainment, hvor hackere slap væk med virtuelle points til en værdi af 1.200 dollar.

Et angreb på Sony BMG i Grækenland førte til, at 8.500 brugernavne med tilhørende mail-adresser og passwords i krypteret form blev stjålet. Hackeren Idahc fik adgang til data om godt 2.000 kunder i Sony Ericsson eShop via et SQL-injection angreb. Knap 1.000 af dataposterne blev offentliggjort.

Den 2. juni angreb hackergruppen LulzSec websteder tilhørende Sony Pictures, hvor de fik adgang til 4,5 millioner dataposter. Mindst en million af dem indeholdt brugerinformationer.
LulzSec hackede sig også ind på Sony BMG i Belgien og i Holland, hvor de fik adgang til intern information samt brugernavne og ukrypterede passwords. Dagen efter offentliggjorde hackeren Idahc 120 navne, telefonnumre og mail-adresser fra en database fra Sony Europe.

I de følgende dage offentliggjorde LulzSec og Idahc samt andre hackere data fra Sony Pictures i Rusland, Sony Computer Entertainment Developer Network, Sony BMG, Sony Music i Portugal og Sony Pictures i Frankrig.

At Sony i andet kvartal blev hackernes yndlingsmålt skyldes primært, at firmaet havde gjort sig upopulært ved at sagsøge George Hotz. Mange kritiserede, at Sony ventede flere dage med at fortælle, at deres brugeres data var blevet hacket. Dertil kommer, at de succesfulde angreb mellem den 16. og 19. april utvivlsomt har lokket andre til at teste, om flere Sony-websteder var sårbare. Det blev med andre ord en form for sport for forskellige individer og grupper at deltage.

Virksomheder og organisationer kan lære af de fejl, Sony har begået. Det vides ikke, hvordan angrebene på PSN og Sony Online Entertainment blev gennemført. De øvrige angreb har udnyttet simpel SQL-injection til at få adgang til fortrolige data. Sådanne sårbarheder bør ikke findes på et professionelt drevet websted – og kan forholdsvis enkelt imødekommes med jævnlige webapplikationsscanninger.

Endvidere var data, heriblandt passwords, om de godt 70 millioner PSN-brugere gemt ukrypteret. Det er et brud på alle anbefalinger. Som minimum bør passwords være krypteret, og ideelt set bør man kryptere alle personfølsomme data.

Borgere og brugere af netværkstjenester kan lære af Sony-sagerne, at de ikke skal tage for givet, at deres data er i sikre hænder. Det er derfor en god ide at begrænse mængden at data, man overlader til websteder, til et absolut minimum.

Hvis tjenesten tilbyder at lagre ens kreditkortnummer, så man slipper for at indtaste det næste gang, skal man sige nej tak. Endelig er det afgørende, at man ikke genbruger passwords. Hvis man bruger det samme password til flere tjenester, skal blot en af dem hackes, for at hackerne har adgang til de øvrige tjenester.

Attrition, 2011; "*Absolute sownage - A concise history of recent Sony hacks*".
Computerworld.com, 2011; "*Sony says hacker stole 2,000 records from Canadian site*".
Dailytech, 2011; "*Anonymous engages in Sony DDoS attacks over GeoHot PS3 lawsuit*".
Networkworld, 2011; "*PlayStation Network hack timeline*".
Playstation.com, 2011; "*Update on PlayStation Network and Qriocity*".
Soe.com, 2011; "*Sony Online Entertainment announces theft of data from its systems*".

Hacking af Sony medfører markant kursfald

Sony er nu en af de virksomheder der har erfaret, at investering i it-sikkerhed kan betale sig i længden. Fra årsskiftet og frem til slut juni 2011, altså over en periode på seks måneder, er Sonys aktier faldet med 33 procent. Det er et drop på lige over fem procentpoint i gennemsnit pr. måned.
Økonomiske analytikere anslår i samme forbindelse, at de 171 millioner dollar, som Sony allerede har haft i omkostninger på grund af de målrettede angreb, vil ende i nærheden af 24 milliarder dollar når alt summeres op.

Disse tal skal måles op mod udgiften til at sikre Sonys onlinesystemer mod SQL-injectionsårbarheder. Her ligger udgiften på et scan på rundt regnet 10.000 dollar. Set i bagklogskabens klare lys ville en udgift på 1 million dollar også have været godt givet ud. Selvom der nok er mere international prestige for hackerne i at gå efter store multinationale selskaber, så bør danske virksomheder tage ved lære af dette forløb.

Sophos, 2011; "*Sony BMG Greece the latest hacked Sony site*".
Sophos, 2011; "*Sony Pictures attacked again, 4.5 million records exposed*".

10.2. RSA udsat for indbrud

Efter RSA var udsat for et hackerangreb, hvor informationer om SecurID Tokenteknologien blev stjålet, oplevede militære leverandører efterfølgende målrettede angreb. Det anslås, at 40 millioner brugere benytter SecurID.

Den 17. marts 2011 meddelte RSA, sikkerhedsdivisionen under EMC, at de var blevet kompromitteret i et APT-angreb (Advanced Persistent Threat), hvor der over længere tid blev benyttet avancerede teknikker til at udføre angrebet.

RSA oplyste, at data om firmaets udbredte to-faktor-godkendelses-system, SecurID, var kommet i hackernes hænder, men at man ikke mente, det muliggjorde et direkte angreb på SecurID-kunder.

Det viste sig efterfølgende ikke at være hele sandheden. Flere leverandører af militærteknologi, herunder Lockheed Martin, L-3 Communications og Northrop Grumman, kunne i april måned rapportere om angreb, der indikerede, at der var benyttet informationer fra RSA-angrebet. RSA har bekræftet, at angrebet på Lockheed Martin udnyttede data, som stammede fra angrebet på RSA. Ifølge Lockheed Martin mislykkedes angrebsforsøgene.

I kølvandet på RSA-kompromitteringen svirrede der mange rygter om angrebets udførelse. Alt fra fysisk indtrængen, SQL-injection til et RAT-program (Remote Administration/Access Tool) baseret på værktøjet Poison Ivy. RSA har valgt ikke at frigive detaljer om måden eller omfanget. Den 7. juni meddeler RSA, at man i nogle tilfælde vil tilbyde kunder at udskifte deres SecurID-tokens.

Da konsekvenserne af kompromitteringen er individuelle, anbefales det, at virksomheder laver en risikovurdering med henblik på at kontakte RSA. Har man ved implementeringen af SecurID fulgt "*RSA SecurID Software Token Security Best Practices Guide*", vil den umiddelbare ikkerhedsrisiko være lille.

Risikovurderingen bør inkludere hvilken type data som SecurID giver adgang til – samt virksomhedens branchetype og virkefelt. Følgende punkter bør tages med i vurderingen:

- Har virksomheden en politik der følger Best Practice-guiden fra RSA?
- Har virksomheden en politik for, hvordan informationer omkring disse tokens og brugeradgange generelt tilbydes og vedligeholdes?
- Ved brugerne, hvem de skal kontakte, såfremt de modtager et opkald om adgangen?

Krebsonsecurity, 2011; "*Domains used in RSA attack taunted U.S.*".
Msnbc, 2011; "*Lockheed Martin says it thwarted 'tenacious' cyber attack*".
Rsa, 2011; "*Open letter to RSA customers*".
Rsa, 2011; "*Open letter to RSA SecurID customers*".
Rsa, 2011; "*Our first priority is to ensure the security of our customers and their trust*".
Slashdot, 2011; "*RSA admits SecurID tokens have been compromised*".
Wired, 2011; "*RSA agrees to replace security tokens after admitting compromise*".

10.3. Viral danskhostet Twitter-applikation

En dansk-hostet viral applikation ved navn OhYess dukkede op den 29. maj på Twitter. Applikationen kunne bruges til at kompromittere den udvalgte konto og sende falske tweets.

Med danske øjne handlede den mest opsigtsvækkende historie fra den 29. maj 2011 om en ny viral Twitter-applikation, som fik navnet OhYess. Applikationens kode bygger på en tidligere skadelig applikation, iMorpheus, som har været lagt til salg i den kriminelle undergrund.

Applikationen spredte sig ved at lokke brugere til at klikke på URL-forkortede links til applikationen i tweets afsendt fra andre brugeres profiler.

Efter at brugeren giver OhYess tilladelse til at tilgå sin Twitter-konto, har applikationen adgang til blandt andet at se hvem brugeren følger, følge andre Twitter-brugere, opdatere den ompromitterede profil og sende nye tweets fra den. Herefter sendes nye tweets med link til applikationen med opsigtvækkende titler som:

- "*New Twitter app is awesome*".
- "*Sexy Lithuanian Girl*".
- "*The Best new OhYess Twitter app*".
- "*How could she ?? Check this chick*".
- "*She cheated and now revenge*".
- "*Revenge on Lithuanian Girl*".

Applikationen blev via en række URL-forkortede links distribueret fra det danskhostede domæne elite4gaming.com. Forfatteren til OhYess benyttede ifølge CSIS en Hotmail-konto eddi-services@hotmail.com, som også optræder i den virale Twitter-app.

Historien understreger endnu engang behovet for at være kritisk over for den information man finder på nettet og de tilladelser, man giver til at tilgå ens data. Selv om det øjensynligt er mennesker man har tillid til, som opfordrer til at man klikker på links, installerer applikationer eller noget helt tredje – så kan det sagtens være et veltilrettelagt angreb uden deres vidende.

Stopmalvertising.com, 2011; "*Twitter viral application OhYess hijacks your account*".
Tdc, 2011; "*Pas på viral Twitter app*".

10.4. Malware rettet mod Macintosh i stigning

Macintosh-brugere har kunnet smile overbærende når talen faldt på malware. Men smilet er begyndt at stivne, for den stigende udbredelse af Macintosh er ikke gået ubemærket hen i det it-kriminelle miljø.

De it-kriminelle ser OS X platformen som et udyrket land, hvor antallet af brugere har været støt stigende siden lanceringen i marts 2001. En anden væsentlig faktor til den større fokus på Macintosh er, at mængden af ondsindet kode har været så forsvindende lille, at langt størstedelen af Macintosh-brugerne ikke har et antivirusprodukt installeret.

I februar måned advarede sikkerhedsvirksomheden CSIS om fremkomsten af et nyt "do it yourself" crimeware kit målrettet angreb på Macintosh-computere. Siden er truslerne mod denne platform vokset. For eksempel satte det falske sikkerhedsprodukt, Mac Defender, i andet kvartal 2011 en global skræk i livet på Macintosh-brugerne og Apple som organisation.

Hjemmesiden til Mac Defender, samt de annoncer der reklamerer for produktet, var yderst professionelt udført. Visuelt er programmet overbevisende. Det kræver viden og ekspertise at gennemskue, at dette produkt er falsk fra ende til anden.

Når Mac Defender er kommet ind på maskinen, oftest ved hjælp af sårbarheder i Safari-browseren, scanner det maskinen, hvor det finder flere falske malwareinfektioner. Som på Windows skræmmes brugerne til at tro, at deres computer er inficeret. Da Mac Defender endnu ikke er "licenseret", kan den ikke fjerne den "fundne" malware. Her bliver brugeren nødt til at bruge sit kreditkort til at betale for at få åbnet programmet.

På trods af, at pressen nåede at informere om Mac Defender, var Apple sene til at komme ramte brugere til hjælp. Det gik så vidt, at et internt notat blev lækket, hvor supporterne fik forbud mod at hjælpe brugerne.

Den generelle anbefaling til Macintosh-brugere er derfor, at man behandler sin computer på samme vis, som hvis den var udstyret med Windows. Det vil sige, at man holder operativsystem og øvrig software opdateret og sørger for at benytte et antivirusprogram.

Csis, 2011; "*Første gør det selv Crimekit til MacOSX publiceret*".
Csoonline, 2011; "*Mac malware goes from game to serious*".
I4u.com, 2011; "*Apple Mac Malware on the Rise, Interview with AppleCare Rep confirms this*".
Squidoo, 2011; "*Mac Defender*".
Zdnet, 2011; "*An AppleCare support rep talks: Mac malware is getting worse*".

10.5. Crimeware kits til fri download

Værktøjer til gør-det-selv-produktion af malware er ikke noget nyt. Habile programmører har solgt disse værktøjer i en årrække. Nu ligger flere af de mest berygtede værktøjer til fri afhentning på nettet.

Udviklingen af crimeware kits (også kaldet DIY for "Do-It-Yourself"), er på papiret en lukrativ forretning. Alt efter værktøjets potentiale har en forsker fundet frem til, at et kit kan købes fra mellem 2.000 og 50.000 kroner. Kildekoden til Zeus var angiveligt til salg i februar 2011 for den nette sum af 500.000 kroner.

Crimeware kits er ikke tilfældigt udviklet kode til de få – det er forretning. Nogle kits er så professionelt opbygget, at de har indbygget muligheden for versionsopdatering eller tilkøb af nye moduler rettet mod specifikke sårbarheder. Netop prisen samt at disse værktøjer handles i lukkede kredse, har tidligere sat begrænsninger for udbredelsen. Da man på kendte download sites nu kan hente kildekoden til de mest berygtede værktøjer, ser denne barriere ud til at være brudt.

Med muligheden for gratis at kunne hente professionelle crimeware kits fra nettet - er det blevet lettere at komme ind på den it-kriminelle løbebane. Det spørgsmål som it-sikkerhedsfolk nu stiller sig er, om dette læk er en bevidst strategi eller for

Derfor malware til Macintosh

Når en given platform bliver populær, vil det uundgåeligt aflede et fokus, hvor profit er den motiverende faktor. Denne sandhed er nu begyndt at overgå Macintosh-brugerne. Med lokale markedsandele på over 16 procent i Schweiz, Luxemburg og USA er mængden af Macintosh-brugere nået en kritisk masse, der gør dem til et attraktivt mål for malwareudviklerne.

Netop markedsandele på 16 procent blev af sikkerhedsforskeren Adam O'Donnell i 2008 angivet som skæringspunktet for, hvornår det var attraktivt at udvikle malware til Macintosh. Han benyttede spilteori med forudsætningerne, at alle Windows-computere er beskyttet af antivirus med en effektivitetsgrad på 80 procent, og ingen Macintosh-computere er beskyttet af antivirus.

Med disse forudsætninger bliver 16 procent markedsandele vendepunktet for, hvornår det bedst kan betale sig at udvikle malware til Macintosh. Man kan simpelthen her kompromittere flere computere med et givent stykke ondsindet kode.

at kamuflere sig i mængden.

Vælger man at se det som en ren strategi fra bagmændenes side, så tyder det på, at forretningsmodellen er ved at blive finpudset med en art distributionskanal. De kan trække sig ud af søgelyset og udvikle add-on moduler, frem for at eksponere sig ved direkte salg af applikationen. Det er den såkaldte freemiumforretningsmodel.

Omvendt kan det også tolkes som et desperat forsøg på at kamuflere sig i mængden. Bagmændene ved, at de er jagtet vildt og har muligvis følt jorden brænde under sig. I et forsøg på at sløre deres spor er værktøjerne kastet i grams. Håbet er, at flere nu begynder at benytte koden og dermed afleder opmærksomheden. Et digitalt røgslør så at sige.

En sidste tese er, at det er rivaler der bekæmper hinanden. Ved at lække rivalens kildekode forsøger de at eliminere modparten.

Infosecurity-magazine, 2011; "*M86 VP technical strategy claims Zeus source code release planned*".
Wikipedia.org; "*Freemium*".

10.6. NemID styrer uden om smartphones

Af sikkerhedsårsager vil smartphones ikke få en applikation, der kan generere NemID-koder. Det vil kompromittere NemID-setuppet, da det vil indeholde information om, hvordan koderne dannes.

It- og telepolitisk redegørelse 2011 sætter fokus på regeringens initiativer på IKTområdet og målsætninger for de kommende år. En af de politiske mærkesager er NemID-løsningen fra juli 2010. Til trods for, at NemID nu har et år på bagen, har det ikke skortet på kritik. Det er specielt stabiliteten, brugen af Java og det papirbaserede nøglekort, som har været i modvind.

Som supplement til nøglekortet har der været arbejdet på elektroniske løsninger. Her har det været nærliggende også at fokusere på mobiltelefonen som en potentiel løsning. Langt de fleste danskere har i dag en smartphone og ønsker at tilgå bank og offentlige services ad den vej.

Trods regeringens IKT-udspil blev NemID-løsningen til smartphones definitivt stillet i bero i juni 2011. Ud fra en sund risikoanalyse vurderede man mobilplatformen til at være for usikker på nuværende tidspunkt.

Hvis en smartphone skal generere nøglekoderne vil den nødvendigvis skulle indeholde information om, hvordan koderne dannes. Da det ikke har været teknisk muligt at indkapsle den kritiske del til generering af koderne, har beslutningen om at fravælge smartphones været forholdsvis let.

Man arbejder dog på en anden mobilløsning, men der er i skrivende stund ikke frigivet detaljer. Et er dog sikkert: Den bliver ikke baseret på java-appletter, som på pc-platformen, da det ikke understøttes af alle smartphones.

Den kommende mobilplatform forventes frigivet i september 2011. Her vil det i første omgang være adgangen til mobilbankerne der er i fokus. En løsning til

andre offentlige og private tjenester skal først i udbud før den udvikles.

Computerworld.dk, 2011; "*Her er den mobile NemID-kodegenerator*".
Signatursekretariatet, 2011; "*OCES - Digital Signatur*".
Version2, 2011; "*Derfor dropper DanID NemID som mobil-app*".
Vtu, 2011; "*It- og telepolitisk redegørelse 2011*".

10.7. Udsættelse af cookiedirektivet

De nye EU-regler til sikring af privatlivets fred, der omfatter cookies, skulle være trådt i kraft den 25. maj 2011. I sidste sekund meddelte IT og Telestyrelsen, at cookie-lovgivningen var udskudt.

Ifølge de nye regler dækkes computerens harddisk i store træk ind under reglerne om privatlivets fred. Det betyder, at gemmes der noget lokalt på maskinen, uden brugerens forudgående accept, så kan det betragtes som ulovlig indtrængen.

Det er EU-kravet om informeret samtykke under e-databeskyttelsesdirektivet (direktiv 2002/58/EF) artikel 5 stk. 3, der sætter rammerne. Det lyder således:

"*Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv 95/46/EF at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen.*"

Forbrugerne skal med andre ord gives muligheden for at styre, hvad eksempelvis hjemmesider placerer eller tilgår af lokal information. Men i samme forbindelse differentierer lovgivningen typen af cookies. Det specificeres videre i stykke 3:

"*Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.*"

Et eksempel herpå er handel på nettet, hvor det er lovligt at placere en cookie, der husker indholdet af en indkøbskurv – da det er nødvendigt for shoppens funktion. Den grå zone blev med ét bredere og langt mere kompleks.

I elvte time meddelte IT- og Telestyrelsen, at de nye danske regler udskydes indtil videre. Man ønskede en nærmere afklaring af, hvordan de bagvedliggende EUregler skulle fortolkes. Dette affødte et lettelsens suk fra onlinebranchen, da man spåede et større kaos, hvis reglerne skulle håndhæves som skrevet.

EU-Tidende, 2009; "*nr. L 337 af 18/12/2009 s. 0011 - 0036*".
Itst.dk, 2011; "*Nye cookie-regler fra EU kræver nærmere afklaring*".
Version2.dk, 2011; "*Forvirret? Få styr på de nye cookie-regler*".

10.8. Hvidvaskning gennem applets

Det vakte mistanke, da en eksplosion i næsten ubrugelige kinesiske apps pludselig figurerede på top-ti-listen i Apples danske App Store. Der var tilsyneladende tale om en hvidvaskningsoperation.

Sort økonomi er ikke meget værd, hvis den ikke kan omsættes til købekraftige finanser. Det er ikke første gang at sådan en fremgangsmåde er benyttet - men det har aldrig været så systematisk som i dette tilfælde.

Ved at udvikle et bredt antal næsten ubrugelige apps og sætte dem til salg i Apples App Store har kinesiske bagmænd angiveligt haft delvis succes med en hvidvaskningsoperation. Men grådighed har det med at give bagslag.

I dette tilfælde var det mistænkeligt, at flere næsten ubrugelige kinesiske apps blev solgt til overpris, samt at de pludselig figurerede på top-ti-listen over bedst sælgende apps på den danske del af Apple App Store. Det er usandsynlig, at danske brugere vil købe kinesiske apps, der er op til 20-30 gange dyrere end normalt.

Det er mere sandsynligt, at de it-kriminelle har fået adgang til en større liste af stjålne kreditkort-informationer. Ved herefter at købe egenudviklede apps, konstrueret til formålet, har de kunnet hvidvaske de økonomiske transaktioner. De 30 procent som Apple tager i handelsomkostninger, er ligegyldige, når man bruger andres folks penge.

Det er ikke småpenge vi taler om. En topsælgende app kan omsætte for i gennemsnit 4-5.000 kroner per land om dagen. Med 20-25 apps i den kategori solgt til overpris kan den samlede daglige omsætning let snige sig op på 100.000 kroner for hvert af de lande de udbydes i. Et par dage efter at det danske onlinemedie Iphoneguide publicerede deres mistanke om hvidvaskning, fjernede Apple de omtalte apps fra App Store.

Det vides ikke med sikkerhed, hvor meget bagmændene har indkasseret. Men det kom efterfølgende frem, at samme fænomen var set i andre udvalgte lande. Årsagen er sandsynligvis, at man har handlet i kreditkortenes udstederlande. Alt dette indikerer gennemtænkt planlægning, koordinering og afvikling.

Iphoneguide.dk, 2011; "*Apple stopper hvidvaskning og smider kinesiske apps ud af App Store*".
Iphoneguide.dk, 2011; "*Kinesere hvidvasker penge i den danske App Store?*".

10.9. LulzSec takker af

Efter 50 dages virke valgte hackergruppen Lulz Security at indstillet deres aktiviteter. Gruppen er mest kendt for deres angreb på Sony, men har en stribe andre angreb bag sig.

Søndag den 26. juni 2011 annoncerede Lulz Security på Twitter, at deres planlagte 50 dages kampagne nu var kommet til vejs ende. De havde få dage forinden gjort et stort nummer ud af deres alliance med hackergruppen Anonymous i kampen mod uretfærdig censur på nettet, den såkaldte "Operation AntiSec".

Som en sidste salut lagde LulzSec en torrent-fil ud på The Pirate Bay. Den henviste

til en 480 MB pakket fil, der indeholdt en bred vifte af informationer indsamlet i forbindelse med deres aktioner.

Indholdet bestod blandt andet af 550.000 brugernavne og krypterede passwords til spillere af betaversionen af Battlefield Heroes. Hertil kom 200.000 brugerkonti med krypterede passwords til websiden Hackforums.net. Der var også små 50.000 brugerkonti med krypterede passwords til forskellige andre spillefora samt cirka 12.000 brugernavne og læsbare passwords til NATO's E-Book Shop.

Materialet indeholdt også et notat fra AOL om deres netværkskonfiguration, et stack trace der skulle være fra fbi.gov, IP-adresser på forskellige virksomhedsnetværk og et PNG-billede der angives at være fra et angreb på navy.mil. Yderligere var der en liste over standard-password til forskellige routere samt en stor mængde RAR-pakkede filer fra teleselskabet AT&T.

Selvom LulzSec i deres sidste kommunikation forsøger at bagatellisere deres tilbagetrækning, så har arrestationen af Ryan Cleary, der angiveligt skulle have hostet deres IRC-server, sandsynligvis været en katalysator i beslutningen. Det samme gælder den lækkede information som "The A-Team" gruppen stod for, hvor mulige LulzSec-medlemmer fra USA, England, Holland og Sverige eksponeres.

Det virker som en hastig retræte med hovedet holdt højt, hvor de nævnte 50 dage mere er en kærkommen undskyldning end et egentligt mål. Med deres populistiske stil er det er svært at tro, at LulzSec bare lukker ned fra den ene dag til den anden. Med mindre de fanges vil de med stor sandsynlighed dukke op under andre alias og i andre grupper.

Alexanderhiggins, 2011; "*Alleged identities of LulzSec and Anonymous hackers revealed*".
H-online, 2011; "*Last LOL for LulzSec as hackers disband group*".
Lulzsecurity, 2011; "*50 Days of Lulz*".
TechWorld, 2011; "*LulzSec hackers feel the heat as FBI raid linked to manhunt*".
Twitter, 2011; "*The Lulz Boat*".

10.10. Statoil lukkede nordiske kundeportaler

Statoil lukkede adgangen til deres skandinaviske kundeportaler efter mistanke om at fortrolige kundedata var kompromitteret. Selvom der ikke er offentliggjort kundeinformation, tyder angrebet på at være en del af Operation AntiSec.

Onsdag den 28. juni lukkede Statoil for adgangen til deres norske, svenske og danske kundeportaler. I en pressemeddelelse dagen efter fortalte virksomheden, at det var sket efter mistanke om at kundeinformationer kunne være lækket som resultat af et angreb, og at de respektive landes datatilsyn var blevet orienteret.

"*There are indications that client data may have been compromised. We are taking this very seriously. At this time we do not have a total overview of the scale of the incident, but are working to establish it as soon as possible. As an immediate measure we have closed down these three portals to prevent unauthorised access while we work to identify the problem and install additional security measures*", fortalte Bård Standal fra Statoil Fuel & Retail i pressemeddelelsen.

Statoil undskyldte al ulejlighed, som lukningen af deres kundeportaler måtte forårsage, og lovede at publicere yderligere information om hændelsen, når den er tilgængelig. Man havde på daværende tidspunkt ikke kendskab til misbrug af

Kort om Lulz Security

LulzSec er en af de mere populistiske hackergrupper der har været på banen. Navnet er en forvanskning af LOL, der er en forkortelse for Laughing Out Loud. Gruppen oplyste, at dens formål med hacking er at have det sjovt.

Ud fra de lækkede oplysninger bestod LulzSec af følgende: Sabu, Topiary, Joepie91, Anonakomis, Tflow, Kayla og Avunit. Hertil følger Uncommon, EE/ EEKDACAT, Laurelai, Nigg og Madclown/ BERRI.

Der er som det seneste dukket aktive grupper op i Brasilien og USA, hvor "Lulz" indgår som en del af deres gruppenavn. Om de på nogen måde støttes af de officielle medlemmer af Lulz Security skal være usagt.

Selvom FBI nu officielt er gået ind i jagten på disse bagmænd, og anti-Lulz-grupper som "The A Team" og "LulzSec Exposed" er begyndt at lække information om gruppen – så har gruppens aktiviteter været med til at starte AntiSec-bevægelsen. Det et startskud på en ny æra, hvor ingen virksomhed kan føle sig sikker.

kundekort, men igangsatte overvågning af korttransaktioner med henblik på at identificere eventuelt misbrug.

Noget tyder dog på, at angrebet er sket en lille uges tid forinden. Allerede den 23. juni blev der på bloggen "Security for the masses" offentliggjort, hvad der øjensynligt er tabelnavne fra databasen under Statoils nordiske kundeportaler. Angrebet skulle være udført af en brasiliansk hacker, som kalder sig Z3R0C00L.

Z3R0C00L associerer sig med operation AntiSec og gruppen LulzSecBrazil, der tidligere har angrebet offentlige brasilianske hjemmesider.

Blogspot.com, 2011; "*//Z3R0C00L// Hacks Swedish Statoil Website*".
Deathandtaxesmag.com, 2011; "*LulzSec and Anonymous launch Operation AntiSec, claim secret hacking underway*".
Matogrossogoiano.com.br, 2011; "*Goiânia na rota dos hackers*".
Pastebin, 2011; "*LulzSec_BR*".
Pastebin, 2011; "*Nicks in #AntiSec on irc.AnonOps.net*".
Pastebin, 2011; "*Untitled*".
Statoilfuelretail, 2011; "*Statoil Fuel & Retail closes three customer portals*".

Operation AntiSec

Operation AntiSec var en fælles global opfordring fra grupperne LulzSec og Anonymous til at angribe offentlige hjemmesider, banker og lignende med det formål at offentliggøre fortrolige data. Målet var sikring af privatlivets fred og den frie adgang til data, eller snarere transparens ved brug og lagring af data for hermed at gøre verden til et bedre sted at være.

11. Artikler fra tredje kvartal

Flere af kvartalets nyhedsartikler havde deres udspring i udlandet. Konsekvenserne ved hackerangrebet mod RSA's SecurID-tokens blev i dette kvartal klart for brugerne. Tilsvarende medførte afdækningen af den engelske avis News of the Wolds systematiske brug af telefonsvareraflytning herhjemme en debat om sikkerheden hos de danske teleoperatører og deres tjenester. En debat som i vores optik var delvist forfejlet.

I enkelte historier lå også en fortælling om, hvordan man i nogle dele af samfundet føler, at målet helliger midlet. Som med News of the World synes dette at gøre sig gældende i historien om, hvordan researchkollektivet Redox tilvejebragte og offentliggjorde informationer om den højreradikale undergrund. Offentliggørelse af informationer som kan kompromittere modstanderen eller dennes motiver og troværdighed, er i stigende grad blevet et politisk værktøj.

Samlet set var kvartalets overskrifter med til at beskrive, hvorledes internetkriminalitetens mål og virkemidler er blevet stadig mere differentierede og diffuse. Hvor vi på den ene side så flere lavteknologiske metoder taget i brug for at opsnappe fortrolige informationer fra et veldefineret mål, så vi også, hvordan teknologisk avancerede metoder og værktøjer blev brugt til på samme tid at ramme dybt og bredt. Tilsammen var det med til at beskrive, hvorledes internetkriminalitet udføres med et veldefineret økonomisk eller politisk motiv af folk, som har de fornødne tekniske, psykologiske og organisatoriske kompetencer.

11.1. RSA hacket ved hjælp af gammel og ny teknik

Ved hjælp af en e-mail med et vedhæftet regneark indeholdende et Flash-exploit startede hackerangrebet mod sikkerhedsfirmaet RSA den tredje marts 2011. Da regnearket blev åbnet, aktiverede det bagdørsprogrammet Poison Ivy. Herefter var der skabt adgang til virksomhedens øvrige systemer.

Den mest udbredte teori er, at RSA-kompromitteringen blot var et nødvendigt skridt på vejen for hackerne, så de efterfølgende kunne bryde ind hos Lockheed-Martin og Northrop-Grumman for at stjæle militære hemmeligheder.

Selve optakten på RSA-kompromitteringen var hverken ukendt eller avanceret. Faktisk startede den på den mest klassiske måde, hvor e-mails blev sendt til udvalgte EMC-medarbejdere over en periode på to dage (EMC ejer RSA).

Vedhæftet mailen var en Excel-fil, der angiveligt skulle indeholde RSA's rekrutteringsplan for 2011. Men Excel-filen indeholdt et Flash-objekt, der udnyttede en sårbarhed i Adobe Flash (CVE-2011-0609) til at afvikle kode. Sårbarheden blev her udnyttet til at installere bagdørsprogrammet Poison Ivy.

Via bagdøren havde hackerne fuld adgang til maskinen og dens tilknyttede netværksressourcer. De kunne herefter bruge maskinen som et springbræt til at bryde længere ind i systemerne, indtil de fik fat i SecurID-information.

Det sammenfald af omstændigheder der skulle til for at få dette hack til at lykkes, kan dårligt gøres bedre i en Hollywoodfilm. For det første brugte hackerne en gammel teknik med at sende en e-mail med en vedhæftet fil. Oven i købet med en filtype som ethvert moderne mailsystem vil flage op som mistænkeligt.

For det andet benyttede de et zero-day exploit, som ikke kunne tjekkes af mailfiltret. Resultatet af omstændighederne endte med, at e-mailen blev gemt i spam-mappen, hvorefter en nysgerrig bruger kunne sætte angrebet i gang.

Trods alskens filtre og oplysningskampagner så er RSA-kompromitteringen et lysende bevis på, at den menneskelige faktor stadig udgør det svageste led.

F-Secure, 2011; "*How we found the file that was used to hack RSA*".

11.2. CSC-konflikten i et it-sikkerhedsperspektiv

Konflikten mellem it-selskabet CSC og fagforeningen PROSA sluttede den 23. juni med, at PROSA mistede sin overenskomst på virksomheden. Konflikten indeholder dog nogle problemstillinger, der rækker ud over det arbejdsretslige, da også driften af en række centrale it-systemer blev berørt og hermed potentielt itsikkerheden.

Konflikten rummer interessante perspektiver set fra et itsikkerhedssynspunkt. It-sikkerhed handler om at beskytte information. Opgaven opdeles traditionelt i tre delopgaver: At beskytte tilgængelighed, integritet og fortrolighed.

Når en faglig konflikt rammer en virksomhed, der leverer it-ydelser, som berører mange mennesker, er tilgængeligheden ofte det første offer. Det så vi også i CSCkonflikten. CSC driver CPR-systemet for den danske stat. I slutningen af maj advarede KMD landets kommuner om, at der i værste fald kunne opstå problemer med udbetaling af sociale ydelser. Det ville ske, hvis data i CPR ikke blev opdateret.

Ligeledes medførte en overenskomststridig arbejdsnedlæggelse hos CSC den 13. april problemer for Skat i flere måneder. Helt fremme i juni kunne hverken borgere eller Skat selv se ændringer, når der blev indberettet til årsopgørelsen. Også forsikringsselskabet Trygs systemer blev berørt af konflikten.

Foruden tilgængeligheden kan også integriteten af data blive truet under en konflikt. PROSA anmeldte CSC til politiet i maj måned. Fagforbundet mente, at CSC ulovligt havde anvendt brugernavne og adgangskoder tilhørende bortviste ansatte. De blev brugt af andre ansatte til at logge ind i systemerne.

Problemet med den procedure set fra et it-sikkerhedsperspektiv er, at man mister oplysninger til brug for datarevision: Virksomheden får svært ved senere at afgøre, hvilken medarbejder der har foretaget bestemte ændringer i systemet. CSC oplyste, at der var tale om en nødprocedure, som blev anvendt en kort overgang. Firmaet mente ikke, at det udgjorde nogen sikkerhedsrisiko, blandt andet fordi alle medarbejdere, der arbejdede på systemer, som kræver sikkerhedsgodkendelse, var sikkerhedsgodkendte.

Sagen om genbrug af bruger-ID'er er for øjeblikket til juridisk vurdering hos politiet. Vurderingen skal afklare, om der er grundlag for at rejse en straffesag.

Comon, 2011; "*SKAT ramt af CSC-konflikten på ubestemt tid*".
Computerworld.dk, 2011; "*KMD: CSC-konflikt truer udbetaling af sociale ydelser*".
Computerworld.dk, 2011; "*CSC efter politianmeldelse: Vi brugte nødprocedure*".
Økonomistyrelsen, 2011; "*Orientering om CSC konflikt og SLS-drift*".

11.3. Målrettet svindel, nu også på telefonen

De it-kriminelle bliver stadig mere målrettede og direkte i deres forsøg på at skaffe sig adgang til danskernes kreditkort. Også i tredje kvartal var der herhjemme målrettede phishing-forsøg, som havde til formål at franarre kreditkortinformationer. Som noget nyt oplevede vi, at man fra udenlandske call-centre ringede til danskere med henblik på at narre dem til at købe virkningsløse antivirusprodukter og/eller installere malware på deres computere.

Bølgen af dansksprogede phishing-mails, hvor PBS, Visa og tilsvarende finansielle institutioner bliver misbrugt som afsender, er efterhånden blevet dagligdag. PBS/NETS måtte igen den 25. august udsende en pressemeddelelse, som advarede mod en mail, der opfordrede modtageren til at oprette en kode til Verified by Visa eller MasterCard SecureCode. Mailen var selvfølgelig falsk og havde til formål at lokke kreditkortinformationer ud af modtageren.

Senere var det Skat, der den 14. september igen blev misbrugt i en mail, der fortalte modtageren, at hun havde 647,21 kr. til gode i overskydende skat. Mailen var en dansksproget kopi af en mail, som florerede allerede i februar. Også denne mail var falsk og havde til formål at narre modtageren til at afsløre sine kreditkortinformationer.

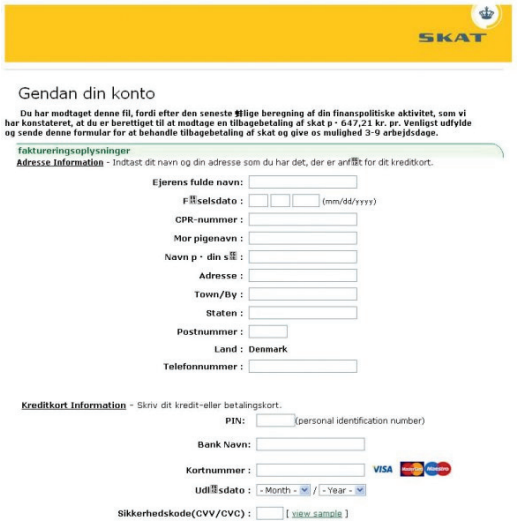
Fælles for de seneste phishing-forsøg er, at de ofte er skrevet på et næsten perfekt dansk, øjensynligt er sendt fra en legal og troværdig e-mail adresse og benytter legale virksomheders grafik. For den uopmærksomme kan det derfor være vanskeligt at afgøre, at der er tale om et forsøg på svindel.

De seneste forsøg på at narre danskerne handler dog ikke om mere eller mindre troværdige mails. DK•CERT modtog i tredje kvartal flere henvendelser fra borgere, som var blevet ringet op og fik fortalt, at deres computer var inficeret af virus. I alle tilfælde undlod de snarrådige borgere at lade sig "hjælpe" af personen, som med udenlandsk accent fortalte, at man repræsenterede Microsoft, en internetudbyder eller lignende organisation.

Ved at kontakte ofret så direkte har man skruet op for brugen af social engineering-metoder og øget henvendelsens troværdighed. Ofte kan svindleren guide brugeren til at få vist filer og biblioteker, der for den mindre sikkerhedskyndige opfattes som tegn på, at computeren er inficeret med vira. Herfra er der ikke langt til at få ofret til at købe og installere programmer, der angiveligt kan fjerne den skadelige kode.

Tilsvarende svindelforsøg udført fra indiske call-centre rullede i 2010 hen over England, men har angiveligt eksisteret siden 2008. Selv om andelen af brugere der hopper på svindelnummeret, må formodes at være relativt høj sammenlignet med traditionel phishing, er det vanskeligt at forstå, at det herhjemme kan være en god forretning. Trods alt er en indisk accent stadig ikke almindelig i Danmark, og tilsammen med henvendelsens unormale karakter vil mange nok fatte mistanke.

Som resultat af svindelopkaldene afbrød Microsoft i september måned samarbejdet med sin indiske guldpartner Comantra. Medarbejdere fra virksomheden havde angiveligt gennem mindst 18 måneder ringet til computerbrugere i blandt andet England, Australien og Canada og fortalt dem, at deres computer var inficeret med virus. Formålet med opkaldene var at skaffe sig fjernadgang til brugernes computer og få dem til at udlevere kreditkortinformationer.



Figur 14. Phishing mail med Skat som afsender.

I betragtning af, at vi herhjemme fra tid til anden afkræves cpr-nummer eller kreditkortinformationer over telefonen, handler det for de kriminelle om at øge opkaldets troværdighed. For eksempel vil et dansk telefonnummer i displayet, en mindre udpræget udenlandsk accent og nogle få personlige oplysninger fra for eksempel Facebook øge troværdigheden af opkaldet betragteligt. En udvikling der kan ligne den, vi gennem de seneste år har set med den mailbaserede svindel.

Guardian.co.uk, 2010; "*Virus phone scam being run from call centres in India*".
Nets, 2011;"*Advarsel mod phishing-mail med PBS som afsender*".
Skat, 2011; "*Falsk e-mail lover skat tilbage*".
Sophos, 2011; "*Microsoft dumps partner over telephone scam claims*".

11.4. Telefonaflytning som journalistisk virkemiddel

Den 10. juli udkom den britiske tabloidavis News of the World for sidste gang. Årsagen var, at avisens journalister havde anvendt hackermetoder til research. Det medførte så stor en skandale, at moderselskabet News Corporation valgte at lukke avisen. Sagen førte i den danske presse ikke til selvransagelse, men til debat om hvorvidt tilsvarende metoder var teknisk mulige hos de danske teleoperatører.

Journalisterne på News of the World brugte blandt andet aflytning af telefonsvarere, der ikke tilhørte dem selv. Det engelske politi udarbejdede en liste over 4.000 potentielle ofre for aflytningen. Blandt dem var skuespillere, politikere, sportsfolk og medlemmer af kongehuset.

Telefonhackingsager havde været offentligt kendt siden 2007. Men i juli kom det frem, at avisen også havde aflyttet telefonsvarere tilhørende et mordoffer, afdøde britiske soldater og ofre for terrorbomberne i London i juli 2005. Flere ledende medarbejdere ved avisen blev arresteret som følge af sagen.

Aflytningen foregik typisk ved, at journalisterne ringede til offerets mobilsvarer og indtastede den standardadgangskode, som den var udstyret med. Hvis offeret ikke havde ændret koden, var der direkte adgang til at aflytte beskeder. Hvis den var blevet ændret, kunne man i nogle tilfælde afprøve andre koder og derved få adgang.

I Danmark afprøvede avisen Ekstra Bladet i august sikkerheden på folketingsmedlemmernes smartphones. Det viste sig, at partileder Margrethe Vestagers (R) iPhone havde en sårbarhed, som gjorde det muligt at aflytte den.

Testen, der blev foretaget i samarbejde med sikkerhedsfirmaet CSIS, viste to ting: Politikernes mobiltelefoner kan få sikkerhedsproblemer, hvis de inficeres med skadelig software. Og data kan opsnappes, hvis de anvender åbne trådløse lokalnet.

Angribere ville kunne installere skadelig software ubemærket på mobiltelefonen på grund af en sårbarhed, der ikke var blevet rettet. Margrethe Vestager oplyste, at hun var blevet adviseret om en opdatering til mobiltelefonen, men havde sprunget den over. Derfor var den sårbar.

BBC, 2011; "*Q&A: News of the World phone-hacking scandal*".
CSIS, 2011; "*CSIS' medvirken i Ekstra Bladet søndag d. 14 august*".
Ekstra Bladet, 2011; "*Ekspert rystet over Folketings-sikkerhed*".
Wikimedia, 2011; "*News International phone hacking scandal*".

11.5. Hacking – den nye politiske slagmark

2011 blev året, hvor hacktivisme gik fra mere eller mindre uskyldige defacements over kravet om informationsfrihed og offentlighed i den globale forvaltning til egentlige angreb på de politiske modstandere. Også herhjemme oplevede vi politisk motiverede it-angreb, som havde til formål at afsløre og udstille den politiske modstander.

Whistleblower-tjenesten WikiLeaks, DDoS-angreb foretaget af gruppen Anonymous, samt LulzSecs offentliggørelse af fortrolige myndighedsdokumenter, har indvarslet en ny æra, hvor internet kriminalitet i nogle kredse er et legalt politisk værktøj. Kampen kæmpes mod storkapitalen og de etablerede politiske systemer, for anonym adgang til internettet og informationsfrihed. Således siger den amerikanske internetaktivist Richard Stallman i et interview med det progressive tyske dagblad TAZ:

"*Det 'Anonymous' gør, er protest. Det er legitimt. Og de er i højeste grad politiske. Men glem ikke, at disse begivenheder kun er del af en større politisk sammenhæng, hvori bl.a. Sony saboterer deres kunders computere.*"

Årets aktiviteter har deres udspring i en video med Tom Cruise, der i 2008 lækkes på internettet. På imageboardet 4chan.org, hvor man under synonymet Anonymous kan lægge billeder op, protesterer brugerne mod Scientologys forsøg på at censurere videoen. Protesterne medfører chikane og hacking af Scientology, og i februar 2008 gennemfører man de første fysiske protester mod kirken i Australien, Europa og USA.

Den politiske bevægelse manifesterede sig yderligere, da gruppen i september 2010 udførte DDoS-angreb mod Motion Picture Association of America (MPAA) og Recording Industry Association of America (RIAA). Angrebene blev udført efter beskyldninger om, at disse organisationer stod bag tilsvarende angreb på fildelingstjenesten The Pirate Bay.

Da Paypal og MasterCard i december 2010 stoppede med at overføre pengedonationer til WikiLeaks skabte det yderligere grobund for protester. Gruppen udførte som reaktion herpå DDoS-angreb mod Paypal og MasterCard, og den globale protestbevægelse Anonymous var født. Siden fulgte i 2011 angreb mod blandt andet Sony PlayStation Network og etableringen af gruppen LulzSec, som stod bag flere højt profilerede angreb mod myndigheder og internationale virksomheder.

Inspireret af Anonymous' aktiviteter blev også flere offentlige filippinske hjemmesider i 2011 angrebet. Blandt de deltagende grupper var PrivateX, som har fokus på at udstille, hvad de ser som korrupte myndigheder. Tilsvarende har den digitale protestbølge rullet under det arabiske forår. Ud over angreb på myndighedssider har kampen for informationsfrihed blandt andet givet sig udslag i etablering af illegale internetforbindelser via modemer og masseudsendelse af fax-beskeder med for eksempel instruktioner om behandling efter tåregasangreb. Også her har den løst definerede bevægelse Anonymous været aktive.

Herhjemme blev den nye politiske agenda konkret, da Politiken i august offentliggjorde informationer om den højreradikale undergrund. Informationerne var fremskaffet af researchkollektivet Redox øjensynlig ved kompromittering af it-systemer, som blev benyttet af den hemmelige organisation ORG, som befinder sig på den yderste politiske højrefløj.

Figur 15. Fysisk protestaktion arrangeret i Anonomous-regi (whyweprotest.net).

Ovenstående begivenheder beskriver, hvordan løst knyttede digitale fællesskaber danner grobund for politisk indikation og protest. Hvor kravet om tilstedeværelse og potentiel afgivelse af anonymitet er en barriere for deltagelse i fysiske politiske aktioner, gør tilgængeligheden af værktøjer og sikkerhedsmæssigt komplekse systemer det nemt at være globalt politisk aktiv i den digitale verden. Vi tror derfor, at 2011 betegner starten på en ny æra, hvor hacktivisme i nogles øjne er en legal politisk aktionsform, som udspringer og rammer både lokalt og globalt.

Autonominfoservice, 2011; "*Kendt hacker-pionér: "Vi har et stort slag foran os""*.
Cnet, 2010; "*4chan takes down RIAA, MPAA sites*".
Democracynow, 2011; "*Hacktivism's global reach, from targeting scientology to backing WikiLeaks and the arab spring*".
Gmanews.tv, 2011; "*Prelude to ROOTCON: The state of Philippine hacktivism*".
Politiken, 2011; "*Dokumentation: Sådan har vi gjort*".
Redox, 2011; "*Politiken afslører højreekstrem loge*".
Whyweprotest, 2011; "*Why We Protest*".
Wikipedia; "*Hactivism*".

11.6. Storebror vil være med på en kigger

Sociale medier og smartphone-services er blevet en de facto standard for moderne kommunikation. Ved urolighederne i London blev BlackBerry-smartphones benyttet til organisering af optøjer. En politiker foreslog suspendering af beskeder fra disse enheder for at inddæmme urolighederne.

London har mere end 8.000 overvågningskameraer – såkaldte CCTV-systemer (Closed Circuit Television). Her kan de engelske myndigheder følge med i folks færden og ageren. Men da urolighederne brød ud flere steder i august måned, var det organiseret digital hit-and-run-taktik ved hjælp af sociale medier og smartphone–services, der blev taget i brug. Kraftig røg fra påsatte brande medførte, at CCTV kom til kort.

Det fik det engelske folketingsmedlem David Lammy til at foreslå på Twitter og BBC Radio, at man suspenderede alle BlackBerry Messenger-beskeder (BBM), medens urolighederne stod på. Baggrunden for denne opfordring var, at BBM beskeder blev benyttet i udbredt grad til at organisere urolighederne.

Der er to facetter af denne opfordring. Det er nemlig ikke uden grund, at det var BlackBerry Messenger beskeder, man ønskede at stoppe. For det første er BlackBerry den foretrukne martphone hos 40 procent af de unge i London mellem 14 og 24 år.

For det andet så krypteres BBM-beskeder, hvilket gør det svært eller umuligt at overvåge de meddelelser, som balladeмagerne og urostifterne sendte til hinanden. David Lammy ville med sin opfordring rive nælden op ved rode ved helt at stoppe BBM-beskeder, medens urolighederne stod på.

Efterfølgende blev det foreslået, at myndighederne skulle kunne få adgang til de dekrypteringsnøgler, som BlackBerry BBM-servicen bruger på sine servere. Et skridt som de saudiarabiske myndigheder angiveligt satte i gang i august sidste år – og som de indiske myndigheder ligeledes har krævet for at kunne bekæmpe militante grupper og it-sikkerhedstrusler.

I England gik borgerrettighedsorganisationer straks til angreb på denne

opfordring. De henviste til, at privatlivets fred er beskyttet i FNs menneskerettighedserklærings artikel 12, hvor der blandt andet står:

"Ingen må være genstand for vilkårlig indblanding i private forhold, familie, hjem eller korrespondance..."

Spørgsmålet er, om ukrænkeligheden af privatlivets fred ophører, når medierne og teknologien bruges til at organisere og udføre ulovligheder i den størrelsesorden, som London oplevede.

Bigbrotherwatch.org.uk, 2011; "*London riots and social media*".
News.yahoo.com, 2011; "*MP calls for BlackBerry Messenger suspension to calm UK riots*".

11.7. Usikre certifikater og økonomisk konsekvens

Hængelåsikonet i browseren mistede noget af sin troværdighed, da certifikatudstederen Comodo blev hacket i marts måned. Men den fulde økonomiske konsekvens kom i september måned, hvor den hollandske udsteder DigiNotar drejede nøglen om efter at være kompromitteret i juni måned.

En iransk hacker stod i marts måned frem og tog ansvaret for at have knækket certifikatudstederen Comodo. Han havde fundet en sårbarhed i en DLL-fil som blev benyttet af samarbejdspartnere til at generere certifikater. DLL-filen blev benyttet til at forbinde sig til backend-systemet – men det benyttede password lå ukrypteret i filen.

Han oprettede efterfølgende falske certifikater til Skype, Yahoo, Windows Live, Google Mail og addons.mozilla.org. I bedste AntiSec-stil blev informationen derefter lagt ud på nettet – herunder med kodeeksempler og interne filer som bevis på hackets ægthed. En hjørnesten i it-sikkerheden var kompromitteret.

I midten af juni måned fik den hollandske certifikatudsteder DigiNotar den tvivlsomme fornøjelse at dele skæbne med Comodo. I en efterfølgende undersøgelse betalt af den hollandske regering blev det afsløret, at hackerne slap væk med mere end 500 certifikater.

Problemet var, at DigiNotar først opdagede kompromitteringen den 19. juli og samtidig fortiede hændelsen over for browser-producenterne og den hollandske regering. Den hollandske regering benyttede selv en stor mængde certifikater fra DigiNotar på deres hjemmesider. Certifikaterne blev kort efter inddraget og efterlod store dele af den hollandske infrastruktur ubrugelig.

Efter offentliggørelsen valgte browserproducenterne Apple, Google, Microsoft, Mozilla og Opera at udsende en opdatering, der forhindrede adgang til sider sikret med DigiNotar-certifikater.

Den 19. september kom konsekvensen af kompromitteringen. DigiNotar erklærede sig konkurs i en hollandsk retssal. Den amerikanske ejer af DigiNotar, Vasco Data Security International, havde året forinden betalt omkring 70 millioner kroner for virksomheden.

Kompromitteringen af certifikatudstederne har efterfølgende afledt en større debat om, hvordan man i fremtiden sikrer sig mod lignende tilfælde. Der er

kommet mange forslag frem – men endnu ingen konkrete løsninger, som alle eksperter bakker op om.

Comon, 2011; "*DigiNotar går konkurs efter hacker-sag*".
Guardian.co.uk, 2011; "*DigiNotar SSL certificate hack amounts to cyberwar, says expert*".
Theregister.co.uk, 2011; "*Comodo-gate hacker brags about forged certificate exploit*".
Wikipedia; "*HTTP Secure*".

11.8. Manglende opdatering af Internet Explorer giver lav sikkerhed

Næsten et halvt år efter frigivelsen af Microsoft Internet Explorer 9 den 14. marts 2011 havde kun cirka halvdelen af Windows 7-brugerne opdateret browseren til nyeste version. Med usikre internetsider som malwareskribenternes primære angrebsvektor udsætter de sig hermed for unødvendige risici.

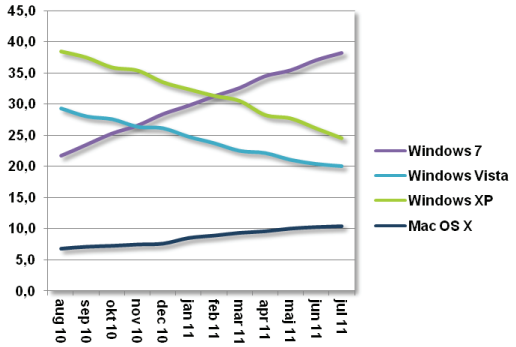
I juli måned blev Internet Explorer 9 benyttet af 18,0 procent af de danske internetbrugere, mens Windows 7 var installeret på 38,3 procent af deres computere (Figur 16). Kun for en mindre del kan forskellen tilskrives, at man i stedet har valgt en alternativ browser som for eksempel Firefox eller Chrome. Med Internet Explorer 9 som en valgfri del af Windows Update har de Windows 7-brugere, der endnu ikke har opdateret browseren, foretaget et aktivt fravalg, der vækker bekymring.

Microsofts valgfrihed ved browseropdatering har samlet set betydet, at der til stadighed benyttes minimum tre versioner af Internet Explorer på en række forskellige Windows-platforme. Dette selvom der ikke medregnes den halve procent, som stadig benytter Internet Explorer 6. I juli måned blev den mindre sikre Internet Explorer 8 således benyttet af 26,5 procent af de danske besøgende på danske internetsider, mens version 7 af browseren blev benyttet af 16,4 procent.

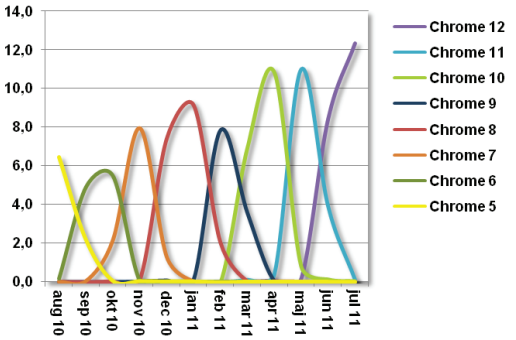
I kontrast hertil står Googles automatiske opdateringscyklus af Chrome, som sikrer, at der på intet tidspunkt er mere end to versioner i omløb hos brugerne (Figur 17). Ud over fordele fra en supportbetragtning betyder det, at Chrome uden skelen til de aktuelle versioner fremstår som et mere sikkert alternativ.

Når opdatering af browseren er aktuel, skyldes det, at drive-by-attacks, der udnytter sårbarheder i browseren og tilknyttede programmer, i dag er den primære kilde til kompromittering af internetbrugernes computere. En ny browserversion giver sikkerhed for, at der ikke er gamle sårbarheder, som kan udnyttes. I tilfældet Internet Explorer fremstår version 9 som et mere sikkert alternativ end version 8. I perioden marts til juli 2011 blev der således offentliggjort 19 nye sårbarheder, der kunne udnyttes i Internet Explorer 8, mod kun seks i Internet Explorer 9.

Flere af de største virksomhedssystemer til økonomistyring, Business Intelligence (BI), Enterprise Ressource Planning (ERP) og lignende, supporterer i dag primært brug af Internet Explorer, og kun sjældent i den seneste version. Automatisk opdatering af browseren til nyeste version kan således give problemer i forhold til de systemer, browseren skal tilgå. Problemet handler her primært om softwareproducenternes manglende overholdelse af gældende standarder. Det er årsag til, at virksomhederne kan have vanskeligt ved at overholde egne standarder for it-sikkerhed og udsættes for unødige sikkerhedsrisici.



Figur 16. Udbredelsen af Windows 7 og Internet Explorer hos danske internetbrugere.



Figur 17. Udbredelsen af Google Chrome hos danske internet brugere.

DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*".
Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Browserbarometer*".
Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*".

11.9. Phishingsvindlere knækkede sikkerheden i NemID

I slutningen af september kom det for første gang frem, at svindlere havde haft held med at phishe NemID-informationer, som efterfølgende blev misbrugt. Otte bankkunder var ude for, at svindlere overførte penge fra deres konti til udenlandske bankkonti. Det skete, selvom netbanken var beskyttet med NemID.

Nets DanID, der driver NemID, oplyser, at kunderne har afleveret bruger-ID, adgangskode og en nøgle fra nøglekortet til en person bag en falsk hjemmeside.

Ifølge webmediet Version2 foregik svindlen ved, at bagmændene sendte en mail ud til de potentielle ofre. I mailen blev modtageren bedt om at gå ind på Nordeas websted for at verificere sin konto. Men linket i mailen førte ikke til Nordeas websted, Nordea.dk, men til en forfalskning på adressen Nordea-dk.com. Her blev offeret mødt af en loginside, der fuldstændig lignede den ægte side.

Når brugeren havde indtastet bruger-ID og password, blev det sendt til den ægte Nordea-side. Den svarede med at bede om en kode med et bestemt nummer på brugerens nøglekort. Dette nummer blev vist på den falske loginside, hvor brugeren efterfølgende indtastede den ønskede nøglekode. Dermed havde bagmændene fri adgang til brugerens konto.

Domænet Nordea-dk.com er registreret af en person, der kalder sig Arthur Williams. Navnet, der sandsynligvis er et dæknavn, er tidligere forbundet med andre registreringer af tvivlsomme domænenavne.

Informationschef Claus Christensen fra Nordea oplyser til Version2, at de otte bankkunder undtagelsesvis fik refunderet det fulde beløb, som de var blevet franarret. Normalt er der ellers en selvrisiko ved den slags sager. For alle kunderne var det mindre end 8.000 kroner, der blev stjålet.

En statistik fra Finansrådet viser, at der frem til den aktuelle sag ikke har været andre tilfælde af netbankindbrud i Danmark i år. Sidste år var der 12 tilfælde, hvoraf halvdelen medførte tab. Det samlede tab var på under 500.000 kroner.

DanID, 2011; "*Nets DanID advarer mod IT-kriminalitet*".
Finansrådet, 2011; "*Netbankindbrud – statistik*".
Version2, 2011; "*NemID phishet – 8 bankkunder frastjålet penge i netbank***".**
Version2, 2011; "*Her er bagmanden: Sådan snød Arthur Williams NemID og stjal fra Nordeakunder*".

12. Ordliste

Adware: Software, der viser reklamer mens applikationen afvikles. Adware betegner både legale applikationer, som er gratis at benytte mod fremvisning af reklamer, samt malware der har til formål at eksponere reklamer på den inficerede computer.

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

Botnet: Et botnet er et netværk af computere, som en angriber kan fjernstyre fra centralt hold. Navnet kommer af "robot" og "net". Ejerne af computerne ved ikke, at deres pc er inficeret med et botnet-program og indgår i botnettet. Angriberen udnytter gerne sine "robotter" til at foretage koordinerede denial of service-angreb eller udsende spam- og phishing-mails.

Brute force: Dækker i datalogien over en udtømmende afsøgning af et løsningsrum. Inden for it-sikkerheden betegner det afprøvningen af kombinationer af brugernavne og kodeord, ofte ud fra foruddefinerede lister og ordbøger.

Certifikat: Et digitalt certifikat bruges i forbindelse med udveksling af krypterede data, hvor certifikatets indhold bekræfter ægtheden af en af de kommunikerende parter.

Crimeware kit: Et crimeware kit er software beregnet til udvikling, tilretning og distribution af malware via en grafisk grænseflade.

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.

Cookie: En cookie er en slags datapakke, der blandt andet indsamler oplysninger om forbrugerens gøren og laden på nettet. Cookies findes overalt på nettet og er med til at gøre det lettere at navigere på forskellige hjemmesider. Det er for eksempel en cookie, der sørger for, at ens mailadresse allerede står i adressefeltet, så man kun behøver at skrive sit password, når man skal tjekke mails.

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.

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

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 samtidigt, og kaldes i de tilfælde for distributed denial of service (DDoS).

Drive-by attacks: 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 eksploit er kode, som forsøger at udnytte sårbarheder i software med det formål at kompromittere systemet.

Forskningsnettet: Et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner Forskningsnettet brugerne med en række tjenester til forskning, samarbejde og kommunikation.

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: 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 og ISO 27006 en række standarder med retningslinjer for, hvordan en organisation kan implementere og overholde de normative standarder.

LulzSec: Hackergruppe, der udspringer af Anonymous. Navnet er en forvanskning af LOLs (Laughing Out Loud) og security. Gruppen oplyste, at dens formål var at have det sjovt, men har enkelte gange offentliggjort politiske budskaber. Er kendt for højt profilerede DDoS-angreb samt hacking og efterfølgende offentliggørelse af fortrolige informationer fra myndigheder og store virksomheder.

Malvertising: Sammentrækning af malware og advertising (reklame). Metode til spredning af malware ved hjælp af inficerede reklame-bannere, der optræder på ellers legale websider.

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

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 fx foregå ved en ændring af DNS-registrering enten på DNS-serveren eller ved ændring af hosts-filen.

Muldyr: Person, der stiller sin bankkonto til rådighed for overførsel af penge fra kompromitterede netbankonti. Muldyret rekrutteres ved hjælp af falske jobtilbud og videreoverfører pengene ad andre kanaler end bankens mod en procentsats af

det overførte beløb. Muldyrsaktivitet er herhjemme ulovlig og kan straffes efter straffelovens hæleribestemmelse.

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.

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.

P2P, Peer-to-peer: P2P er en betegnelse for et decentralt netværk, hvor de enkelte noder (peers), i modsætning til i en client/server arkitektur, kommunikerer direkte med hinanden. Ansvaret for nettets funktionalitet er tilsvarende distribueret ligeligt mellem de enkelte computere i netværket. En hyppig anvendelse af P2P er fildelingsprogrammer som fx BitTorrent, eDonkey og KaZaA, samt internetbaserede telefonforbindelser som Skype.

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.

Pirate Bay: The Pirate Bay blev grundlagt i slutningen af 2003, som en del af det svenske Piratbyrån. Den er i dag verdens største Bittorrent-tracker. Den åbne server indeholder links til torrent-filer og hoster således ikke selv ophavsretsligt beskyttet materiale. Den 26. november 2008 stadfæstede landsretten en kendelse om at filtrere adgangen til The Pirate Bay for alle abonnenter hos internetudbyderen Tele2. Siden har de fleste danske internetudbydere fulgt trop og filtreret adgangen til The Pirate Bay.

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 udføre handlinger som for eksempel at klikke på links, svare på mails eller installere malware.

Software as a Service (SaaS): Cloud-baserede tjenester, der tilbyder online brug af programmer efter behov. Det kan være programmer som tekstbehandling, regneark eller CRM-services. Eksempler på SaaS er Google Docs, Hotmail og lignende.

Spam: Uopfordrede massedistribuerede reklamemails med henblik på salg af produkter eller services.

SPF, Sender Policy Framework: En udvidelse til SMTP-protokollen, som muliggør filtrering af e-mails baseret på den afsendende mailservers IP-adresse og den

benyttede e-mailadresse. Ved registreringen af et domæne angives en SPF record, der fortæller, hvilke(n) mailservere der må benytte dette. Benyttes SPF af den modtagne mailserver, foretager den et opslag på afsenderdomænets SPF-record, og afviser eller godkender mailen på baggrund af dette.

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.

Spear phishing: Phishing-angreb, der er rettet mod en specifik målgruppe. Typisk nøglemedarbejdere i den organisation som er mål for angrebet.

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 flertalsformen af software.

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

13. Figuroversigt

14. Referencer

708media.com, 2010; "*SCAM: Asian/China domain name scam*"; www.708media.com/small-business-scams/scam-asianchina-domain-name-scam/

Adobe, 2011; "*Security advisory for Adobe Flash Player, Adobe Reader and Acrobat*"; www.adobe.com/support/security/advisories/apsa11-01.html

Adobe, juni 2011; "*Security updates available for Adobe Reader and Acrobat*"; www.adobe.com/support/security/bulletins/apsb11-16.html

Adobe, august 2011; "*Security update available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb11-21.html

Adobe, september 2011; "*Security update available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb11-26.html

Adobe, september 2011; "*Security updates available for Adobe Reader and Acrobat*"; www.adobe.com/support/security/bulletins/apsb11-24.html

Adobe, december 2011; "*Security updates available for Adobe Reader and Acrobat*"; www.adobe.com/support/security/advisories/apsa11-04.html

Alexanderhiggins, 2011; "*Alleged identities of LulzSec and Anonymous hackers revealed*"; blog.alexanderhiggins.com/LulzSec-And-Anonymous-Hacker-Identities.html

Anonymous, 2012; "*Anonymous - #opeurope - Expect us!*"; pastebin.com/aUuuhLyD

Anonymous CPH, 2011;"*Hvem ejer Occupy bevægelsen teori og løgn om de få eller mange 99%*"; anonkbh.dk

APWG, 2011; "*Global phishing survey: Trends and domain name use in H12011*"; www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2011.pdf

Apple, 2011; "*About the security content of Mac OS X v10.6.8 and security update 2011-04*"; support.apple.com/kb/HT4723

Apple, 2011; "*How to avoid or remove Mac Defender malware*"; support.apple.com/kb/ht4650

Attrition, 2011; "*Absolute sownage - A concise history of recent Sony hacks*"; attrition.org/security/rants/sony_aka_sownage.html

Autonominfoservice, 2011; "*Kendt hacker-pionér: "Vi har et stort slag foran os""*; www.autonominfoservice.net/2011/07/04/kendt-hacker-pionprocentC3procentA9r-vi-har-et-stort-slag-foran-os/

AVG, 2011; "*AVG community powered threat report - Q2 2011*"; www.avg.com.au/files/media/avg_threat_report_2011-q2.pdf

BBC, 2011; "*Q&A: News of the World phone-hacking scandal*"; www.bbc.co.uk/news/uk-11195407

Bigbrotherwatch.org.uk, 2011; "*London riots and social media*"; www.bigbrotherwatch.org.uk/home/2011/08/london-riots-and-social-media.html

Blogspot.com, 2011; "*//Z3R0C00L// Hacks Swedish Statoil Website*"; securityforthemasses.blogspot.com/2011/06/z3r0c00l-hacks-swedish-statoil-website.html

Business.dk, 2011; "*IT-salget satte rekord i 2010*"; www.business.dk/tech-mobil/it-salget-satte-rekord-i-2010

Channelregister, 2011; "*Rustock Takedown: How the world's worst botnet was KO'd*"; www.channelregister.co.uk/2011/03/23/rustock_takedown_analysis/

Cnet, 2010; "*4chan takes down RIAA, MPAA sites*"; news.cnet.com/8301-1009_3-20016961-83.html

Cnnic.net.cn, 2011; "*CNNIC accredited CDN domestic registrars*"; www.cnnic.net.cn/html/Dir/2005/10/11/3217.htm

Commtouch, 2011; "*Internet threats trend report October 2011*"; www.commtouch.com/download/2178?utm_source=1011&utm_medium=W&utm_campaign=IntroQ3rep

Commtouch, 2011; "*The State of hacked accounts October 2011*"; www.commtouch.com/hacked-accounts-report-Oct2011?utm_source=1011&utm_medium=W&utm_campaign=IntroSurveyResults

Comon, 2011; "*DigiNotar går konkurs efter hacker-sag*"; www.comon.dk/art/167213

Comon, 2011; "*SKAT ramt af CSC-konflikten på ubestemt tid*"; www.comon.dk/art/151947/

Compass Security AG, 2011; "*HTML5 web security December 6th, 2011*". media.hacking-lab.com/hlnews/HTML5_Web_Security_v1.0.pdf

Computerworld.com, 2011; "*Sony says hacker stole 2,000 records from Canadian site*"; www.computerworld.com/s/article/9217028/Sony_says_hacker_stole_2_000_records_from_Canadian_site

Computerworld.dk, 2011; "*CSC efter politianmeldelse: Vi brugte nødprocedure*"; www.computerworld.dk/art/115887/

Computerworld.dk, 2011; "*Her er den mobile NemID-kodegenerator*"; www.computerworld.dk/art/116458

Computerworld.dk, 2011; "*KMD: CSC-konflikt truer udbetaling af sociale ydelser*"; www.computerworld.dk/art/116470

CSIS; "*Heimdal*"; www.heimdalagent.com/da/home

CSIS, 2011; "*CSIS' medvirken i Ekstra Bladet søndag d. 14 august*"; www.csis.dk/da/csis/blog/3304/

CSIS, 2011; "*Første gør det selv Crimekit til MacOSX publiceret*"; www.csis.dk/da/csis/news/3196/

Csoonline, 2011;"*Mac malware goes from game to serious*"; www.csoonline.com/article/682167/mac-malware-goes-from-game-to-serious

Dailytech.com, 2011; "*Anonymous engages in Sony DDoS attacks over GeoHot PS3 lawsuit*"; www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm

DanID, 2011; "*Nets DanID advarer mod IT-kriminalitet*"; danid.dk/om_nets_danid/presse/28092011_nets_danid_advarer_mod_it_kriminalitet.html

Danmarks Radio, 2010; "*DI: Staten bør bekæmpe it-kriminelle*"; www.dr.dk/Nyheder/Penge/2010/09/08/072441.htm?rss=true

Dansk IT; "*Dansk IT*"; dit.dk/

Dansk IT, 2011; "*CIOViewpoint - Industrivirus og industrispionage*"; dit.dk/aktuelt/Nyt_fra_DIT/Nyheder/~/media/Files/Presse/CIO-Viewpoint_2011_it-sikkerhed.ashx

Dansk IT, 2010; "*CIOViewpoint - Krisens spor*"; dit.dk/aktuelt/Nyt_fra_DIT/Nyheder/~/media/Files/Presse/CIO-Viewpoint_2011_it-sikkerhed.ashx

Deathandtaxesmag.com, 2011; "*LulzSec and Anonymous launch Operation AntiSec, claim secret hacking underway*"; www.deathandtaxesmag.com/107061/lulzsec-and-anonymous-launch-operation-antisec-claim-secret-hacking-underway/

Democracynow, 2011; "*Hacktivism's global reach, from targeting Scientology to backing WikiLeaks and the arab spring*"; www.democracynow.org/2011/8/16/hacktivisms_global_reach_from_targeting_scientology

DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*"; sdb.cert.dk/login.php

DK•CERT, 2011; "*Dit webhotel tager ikke din it-sikkerhed alvorligt*"; www.cert.dk/artikler/artikler/CW20042011.shtml

DK•CERT, 2009; "*Smiley'er skal begrænse defacements*"; www.cert.dk/artikler/artikler/CW06102009.shtml

DK•CERT & KOMFO, 2010; "*Styr dit privatliv på Facebook*"; www.cert.dk/vejled/facebook_guiden_komfo&dkcert.PDF

DK•CERT, 2010; "*Trendrapport 2009*"; www.cert.dk/trendrapport2009/trendrapport2009.pdf

Ekstra Bladet, 2011; "*Ekspert rystet over Folketings-sikkerhed*"; www.ekstrabladet.dk/nyheder/samfund/article1600799.ece

Ernst & Young, 2011; "*Into the cloud, out of the fog*"; www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$File/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf

Europol, 2011; "*Eu organised crime threat assessment - OCTA 2011*"; www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.pdf

Europol, 2011; "*iOCTA: Threat assessment on internet facilitated organised crime*"; www.europol.europa.eu/sites/default/files/publications/iocta.pdf

EU-Tidende, 2009; "nr. L 337 af 18/12/2009 s. 0011 – 0036"; eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:DA:HTML

Finansrådet, 2011; "*Historisk få netbankindbrud*"; www.finansraadet.dk/nyheder/artikler-fra-finansraadets-nyhedsbrev/2011/januar/historisk-faa-netbankindbrud.aspx

Finansrådet, 2011; "*Netbankindbrud – statistik*"; www.finansraadet.dk/tal--fakta/statistik-og-tal/netbankindbrud---statistik.aspx

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Browserbarometer*"; www.fdim.dk/Statistik/teknik/browserbarometer

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*"; www.fdim.dk/Statistik/teknik/operativsystemer

F-Secure, 2011; "*Internet Explorer cumulative security update*"; www.f-secure.com/vulnerabilities/en/SA201106634

F-Secure, 2011; "*How we found the file that was used to hack RSA*"; www.f-secure.com/weblog/archives/00002226.html

F-secure.com, 2011; "*F-Secure Security Lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

Govcert.dk, 2011; "*Styrket samarbejde i bekæmpelsen af botnet*"; https://www.govcert.dk/news/9

Guardian.co.uk, 2011; "*DigiNotar SSL certificate hack amounts to cyberwar, says expert*"; www.guardian.co.uk/technology/2011/sep/05/diginotar-certificate-hack-cyberwar

Guardian.co.uk, 2010; "*Virus phone scam being run from call centres in India*"; www.guardian.co.uk/world/2010/jul/18/phone-scam-india-call-centres

Gmanews.tv, 2011; "*Prelude to ROOTCON: The state of Philippine hacktivism*"; www.gmanews.tv/story/231895/technology/prelude-to-rootcon-the-state-of-philippine-hacktivism

H-online, 2011; "*Last LOL for LulzSec as hackers disband group*"; www.h-online.com/security/news/item/Last-LOL-for-LulzSec-as-hackers-disband-group-1268090.html

IBM, 2011; "*IBM X-Force 2011 trend & risk report*"; www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-spsm-tiv-sec-wp&S_PKG=IBM-X-Force-2011-Mid-year

I4u.com, 2011; "*Apple Mac malware on the rise, interview with AppleCare rep confirms this*"; www.i4u.com/46611/apple-mac-malware-rise-interview-applecare-rep-confirms

Ingeniøren, 2011; "*Eksperter: Dagens aktivister kaster cyberbrosten*"; ing.dk/artikel/120076-eksperter-dagens-aktivister-kaster-cyberbrosten

Infosecurity-magazine, 2011; "*M86 VP technical strategy claims Zeus source code release planned*"; www.infosecurity-magazine.com/view/18506/m86-vp-technical-

strategy-claims-zeus-source-code-release-planned-

Iniqua.com, 2011; "*Hacking IPv6 III – IP6 spoofing in 6in4 tunnels*"; www.iniqua.com/2011/12/12/hacking-ipv6-iii-ipv6-spoofing-en-tuneles-6in4/?lang=en

Interpol, 2011; "*Cybercrime fact sheet*"; www.interpol.int/content/download/805/6671/version/10/file/FHT02.pdf

Iphoneguide.dk, 2011; "*Apple stopper hvidvaskning og smider kinesiske apps ud af App Store*"; iphoneguide.dk/nyheder/apple-smider-kinesiske-apps-ud-af-app-store/

Iphoneguide.dk, 2011; "*Kinesere hvidvasker penge i den danske App Store?*"; iphoneguide.dk/nyheder/kinesere-hvidvasker-penge-i-den-danske-app-store/

Itst.dk, 2011; "*Nye cookie-regler fra EU kræver nærmere afklaring*"; www.itst.dk/nyheder/nyhedsarkiv/2011/nye-cookie-regler-fra-eu-krever-nermere-afklaring

Kaspersky, 2011; "*Duqu FAQ*"; www.securelist.com/en/blog/208193178/Duqu_FAQ

Kaspersky, 2011; "*The Duqu saga continues: Enter Mr. B. Jason and TV's Dexter*"; www.securelist.com/en/blog/208193243/The_Duqu_Saga_Continues_Enter_Mr_B_Jason_and_TVs_Dexter

Kaspersky, 2011; "*The mystery of Duqu: Part six (The command and control servers)*"; www.securelist.com/en/blog/625/The_Mystery_of_Duqu_Part_Six_The_Command_and_Control_servers

Krebsonsecurity, 2011; "*Domains used in RSA attack taunted U.S.*"; krebsonsecurity.com/2011/03/domains-used-in-rsa-attack-taunted-u-s/

Lulzsecurity, 2011; "*50 Days of Lulz*"; lulzsecurity.com/releases/50%20Days%20of%20Lulz.txt

Matogrossogoiano.com.br, 2011; "*Goiânia na rota dos hackers*"; www.matogrossogoiano.com.br/site/politica/ultimas-noticias/goias/3163-goiania-na-rota-dos-hackers

McAfee, 2011; "*McAfee threats report: Third quarter 2011*"; www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

Microsoft, 2011; "*Microsoft safety scanner detects exploits du jour*"; blogs.technet.com/b/mmpc/archive/2011/05/25/microsoft-safety-scanner-detects-exploitsdu-jour.aspx

Microsoft, 2011; "*Microsoft security bulletin MS11-057 – Critical*"; technet.microsoft.com/en-us/security/bulletin/ms11-057

Microsoft, 2011; "*Microsoft security intelligence report (volume 11)*"; download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf

Microsoft, 2011; "*More information on MS11-087*"; blogs.technet.com/b/srd/archive/2011/12/13/more-information-on-ms11-087.aspx

Microsoft, 2011; "*Operation b107 - Rustock botnet takedown*"; blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx

Microsoft, 2011; "*Oversigt over sikkerhedsopdateringer fra Microsoft for december 2011*"; technet.microsoft.com/da-dk/security/bulletin/ms11-dec

Microsoft, 2011; "*Undvik bedrägeri som använder Microsofts namn*"; support.microsoft.com/gp/fraudulent-microsoft-name-use/da

Mozilla, 2011; "*Mozilla foundation security advisory 2011-29*"; www.mozilla.org/security/announce/2011/mfsa2011-29.html

Msnbc, 2011; "*Lockheed Martin says it thwarted 'tenacious' cyber attack*"; www.msnbc.msn.com/id/43199200/ns/technology_and_science-security/

Nets, 2011; "*Advarsel mod phishing-mail med PBS som afsender*"; http://www.nets.eu/dk-da/Om/nyheder-og-presse/Pages/Advarsel-mod-phishing-mail-med-PBS-som-afsender.aspx

Networkworld.com, 2011; "*PlayStation Network hack timeline*"; www.networkworld.com/news/2011/042711-playstation-network-hack.html

News.yahoo.com, 2011; "*MP calls for BlackBerry Messenger suspension to calm UK riots*"; news.yahoo.com/mp-calls-blackberry-messenger-suspension-calm-uk-riots-162318619.html

Nvd.nist.gov; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Nvd.nist.gov; "*National Vulnerability Database version 2.2*"; nvd.nist.gov/

Opdaterdinpc, 2011; "*Gode råd*"; opdaterdinpc.tdc.dk/publish.php?dogtag=tdc_ms_opdater_raad

Pastebin, 2011; "*LulzSec_BR*"; pastebin.com/EuuwGwua

Pastebin, 2011; "*Nicks in #AntiSec on irc.AnonOps.net*"; pastebin.com/XiT943GZ

Pastebin, 2011; "*Untitled*"; pastebin.com/EUuwGwua

Playstation.com, 2011; "*Update on PlayStation Network and Qriocity*"; blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/

Politiets Efterretningstjeneste, 2011; "*PET's indsats i forhold til politisk ekstremisme*"; www.pet.dk/upload/microsoft_word_-_politisk_ekstremisme__ukl.pdf

Politiken, 2012; "*Det Kgl. Teater bliver reduceret til provinsteater*"; politiken.dk/kultur/scenekunst/ECE1499721/det-kgl-teater-bliver-reduceret-til-provinsteater/

Politiken, 2011; "*Dokumentation: Sådan har vi gjort*"; politiken.dk/indland/ECE1357129/dokumentation-saadan-har-vi-gjort/

PwC, 2011; "*Cybercrime: protecting against the growing threat*"; www.pwc.com/es_MX/mx/prensa/archivo/2011-11-GECS.pdf

PwC, 2011; "*Virksomhedskriminalitet i Danmark 2011*"; www.pwc.dk/da/svig/virksomhedskriminalitet-i-danmark.jhtml

Redox, 2011; "*Politiken afslører højreekstrem loge*"; www.redox.dk/spip.php?article1170

Rsa, 2011; "*Open letter to RSA customers*"; www.rsa.com/node.aspx?id=3872

Rsa, 2011; "*Open letter to RSA SecurID customers*"; www.rsa.com/node.aspx?id=3891

Rsa, 2011; "*Our first priority is to ensure the security of our customers and their trust*"; www.rsa.com/node.aspx?id=3876

Scmagazineuk.com; "*IRISSCERT conference kicks off, as statistics reveal level of cyber crime against Irish websites*"; www.scmagazineuk.com/irisscert-cyber-crime-conference-kicks-off-as-statistics-reveal-level-of-cyber-crime-against-irish-websites/article/217457/

Secunia; "*Secunia Personal Software Inspector (PSI)*"; secunia.com/vulnerability_scanning/personal/

Signatursekretariatet, 2011; "*OCES - Digital Signatur*"; www.signatursekretariatet.dk/forside.html

Skat, 2011; "*Falsk e-mail lover skat tilbage*"; www.skat.dk/SKAT.aspx?oId=1966219&vId=0

Slashdot.org, 2011; "*RSA admits SecurID tokens have been compromised*"; yro.slashdot.org/story/11/06/07/129217/RSA-Admits-SecurID-Tokens-Have-Been-Compromised

Soe.com, 2011; "*Sony Online Entertainment announces theft of data from its systems*"; www.soe.com/securityupdate/pressrelease.vm

Sophos, 2011; "*Microsoft dumps partner over telephone scam claims*"; nakedsecurity.sophos.com/2011/09/21/microsoft-dumps-partner-telephone-support-scam/

Sophos, 2011; "*Sony BMG Greece the latest hacked Sony site*"; nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/

Sophos, 2011; "*Sony Pictures attacked again, 4.5 million records exposed*"; nakedsecurity.sophos.com/2011/06/02/sony-pictures-attacked-again-4-5-million-records-exposed/

Squidoo, 2011; "*Mac Defender*"; www.squidoo.com/mac-defender

Statoilfuelretail.com, 2011; "*Statoil Fuel & Retail closes three customer portals*"; www.statoilfuelretail.com/en/newsandmedia/news/Pages/HuginPressRelease_1527060.aspx

Stopmalvertising.com, 2011; "*Twitter viral application OhYess hijacks your account*"; stopmalvertising.com/spam-scams/twitter-viral-application-ohyess-hijacks-your-account.html

Symantec, 2011; "*Nortons rapport om cyberkriminalitet 2011*"; www.symantec.com/content/da/dk/home_homeoffice/html/cybercrimereport/

Symantec, 2011; "*Intelligence reports*"; www.symanteccloud.com/da/dk/globalthreats/overview/r_mli_reports
Tdc, 2011; "Pas på viral Twitter app"; sikkerhed.tdc.dk/publish.php?id=29289

TechWorld.com; 2011; "*LulzSec hackers feel the heat as FBI raid linked to manhunt*"; news.techworld.com/security/3288857/lulzsec-hackers-feel-the-heat-as-fbi-raid-linked-to-manhunt

Theregister.co.uk, 2011; "*Comodo-gate hacker brags about forged certificate exploit*"; www.theregister.co.uk/2011/03/28/comodo_gate_hacker_breaks_cover/

Trendmicro, 2011; "*Google Android rooted, backdoored, infected*"; countermeasures.trendmicro.eu/google-android-rooted-backdoored-infected/

Trendmicro, 2011; "*"Most Recent Earthquake in Japan" Searches Lead to FAKEAV*"; blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/

Toptenreviews, 2011; "*Malware trends according to Symantec*"; anti-virus-software-review.toptenreviews.com

Twitter, 2011; "*The Lulz Boat*"; twitter.com/#!/lulzsec

Version2, 2011; "*Dansk satellitfirma ramt af industrispion-bagdør*"; www.version2.dk/artikel/dansk-satellitfirma-ramt-af-industrispion-bagdoer-30101

Version2, 2011; "*Dells teknologichef: Sikkerhedsfolk skulle have et los bagi*"; www.version2.dk/artikel/dells-sikkerhedschef-de-fleste-sikkerhedsfolk-skulle-have-et-spark-bagi-33264

Version2, 2011; "*Derfor dropper DanID NemID som mobil-app*"; www.version2.dk/artikel/19313-derfor-dropper-danid-nemid-som-mobil-app

Version2, 2011; "*Eugene Kaspersky: Android bliver hackernes nye Windows*"; www.version2.dk/artikel/18277-eugene-kaspersky-android-bliver-hackernes-nye-windows

Version2, 2011; "*Fovirret? Få styr på de nye cookie-regler*"; www.version2.dk/artikel/18281-forvirret-faa-styr-paa-de-nye-cookie-regler

Version2, 2011; "*Her er bagmanden: Sådan snød Arthur Williams NemID og stjal fra Nordea-kunder*"; www.version2.dk/artikel/saadan-lokkede-kriminelle-nemid-logons-fra-8-nordea-kunder-31536

Version2, 2011; "*Hver anden danske webshop har alvorlige sikkerhedsfejl*"; www.version2.dk/artikel/18132-hver-anden-danske-webshop-har-alvorlige-sikkerhedsfejl

Version2, 2011; "*NemID phishet – 8 bankkunder frastjålet penge i netbank*"; www.version2.dk/artikel/breaking-nemid-hacket-31480

Vtu, 2011; "*It- og telepolitisk redegørelse 2011*"; vtu.dk/publikationer/2011/it-og-telepolitisk-redegoerelse-2011/it-og-telepolitsk-redegoerelse-2011.pdf

Vupen, 2011; "*Microsoft Windows SMB "mrxsmb.sys" remote heap overflow vulnerability*"; www.vupen.com/english/advisories/2011/0394
Whyweprotest, 2011; "*Why We Protest*" www.whyweprotest.net

Wikimedia, 2011; "*News International phone hacking scandal*"; www.secure.

wikimedia.org/wikipedia/en/wiki/News_International_phone_hacking_scandal

Wikipedia; "*Hactivism*"; en.wikipedia.org/wiki/Hacktivism

Wikipedia; "*HTTP Secure*"; en.wikipedia.org/wiki/HTTP_Secure

Wikipedia; "*Freemium*"; en.wikipedia.org/wiki/Freemium

Wired, 2011; "*RSA agrees to replace security tokens after admitting compromise*"; www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/

Ygnetworkltd.com; "*About us*"; www.ygnetworkltd.com/en.about.htm

Zdnet, 2011; "*An AppleCare support rep talks: Mac malware is getting worse*"; www.zdnet.com/blog/bott/an-applecare-support-rep-talks-mac-malware-is-getting-worse/3342

Økonomistyrelsen, 2011; "*Orientering om CSC konflikt og SLS-drift*"; www.oes.dk/Servicemenu/Nyheder/Nyhedsarkiv/Loen-og-Personale/SLS/Orientering-om-CSC-konflikt-og-SLSdrift

Kontakt:

DK•CERT, UNI•C
Centrifugevej, Bygn. 356
Kgs. Lyngby 2800

Tel. +45 3587 8887
URL: https://www.cert.dk
Email: cert@cert.dk