DK•CERT

Trendrapport

It-sikkerhed i tredje kvartal 2011

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

Om DK•CERT

Det er DK•CERTs mission at skabe øget fokus på it-sikkerhed 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 it-sikkerhed. 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 Undervisningsministeriet.

DK•CERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om it-sikkerhed med grundidé i CERT/CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DK•CERT om it-sikkerhed 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.

Indholdsfortegnelse

1. Resume

Aldrig tidligere har DK•CERT modtaget så mange henvendelser om kompromitterede danske websites, der lægger plads til malware og phishing-sider. Her satte tredje kvartal 2011 rekord.

Problemet er også udbredt internationalt. Det handler om, at hackere trænger ind på websteder. Men deres formål er ikke at få fat i data, der ligger på webstederne. I stedet placerer de skjulte skadelige programmer på dem. Når webstedet får besøg, forsøger de skadelige programmer at inficere gæsternes pc'er ved at udnytte kendte sårbarheder i dem.

Fordelen for bagmændene er, at slutbrugerne har tillid til det inficerede websted og derfor ikke venter at møde noget skadeligt. Samme ræsonnement ligger bag de it-kriminelles brug af web-annoncer til at sprede skadelige programmer. Også her spredes truslen fra et websted, som offeret har tillid til.

Phishingsider er forfalskede udgaver af loginsider fra kendte firmaer. Når de placeres på hackede websteder, skyldes det som regel den troværdighed, et legitimt websted har. For bagmændene er der mindre risiko for, at et legitimt websted stemples som risikabelt af de sikkerhedsprogrammer, der beskytter mod farlige websteder.

Blandt kvartalets øvrige væsentlige tendenser er:

- Antallet af sikkerhedshændelser der rapporteres til DK•CERT, er steget i forhold til de seneste kvartaler.
- Svindlere fra call-centre i Indien ringede til danske borgere for at fortælle, at der var virus på deres computer. Målet var at skaffe sig adgang til deres computer, data og kreditkortinformationer.
- It-kriminalitet som politisk aktionsform, hacktivisme, er i stigning og har i tredje kvartal også nået Danmark.
- For første gang siden indførelsen af NemID i 2010 oplevede vi herhjemme vellykkede netbankindbrud.

De er beskrevet nærmere på de følgende sider. God fornøjelse med læsningen!

Shehzad Ahmad

Chef for DK•CERT

2. Tredje kvartal 2011 i tal

Skandalen med den engelske avis News of the Worlds systematiske brug af aflytning af telefonsvarere startede i medierne herhjemme en debat om manglende mobilsikkerhed. At debatten er aktuel viste en verdensomspændende undersøgelse foretaget af Symantec. Her svarede 47 procent af respondenterne, at de betragtede mobile platforme som den væsentligste udfordring for organisationernes it-sikkerhed.

Selvom andelen af mobile brugere stiger, udgjorde de ifølge Foreningen af Danske Interaktive Medier kun lidt over fem procent af de besøgende på danske hjemmesider i juli 2011. I takt med stigende udbredelse forventes de mobile enheder at få større bevågenhed, også hos de it-kriminelle. DK•CERT betragter derfor sikkerhed på de mobile platforme som et emne, der bør have større opmærksomhed, selvom vi kan konstatere, at angreb mod mobile enheder fylder forsvindende lidt i kvartalets statistikker.

I en undersøgelse over organisationernes udgifter forbundet med it-kriminalitet redegjorde Ponemon Institute i august 2011 for, at disse i USA var steget med 56 procent i forhold til undersøgelsen året før. Den væsentligste årsag er, at antallet af succesfulde angreb var steget med 44 procent. Selvom tallene ikke direkte kan overføres til danske forhold, beskriver de en tendens, som vi tror også gør sig gældende herhjemme, hvor omkostningerne i 2010 ifølge Symantec var på 1,7 milliarder kroner i direkte finansielle tab og 997 millioner kroner i tabt arbejdsfortjeneste..

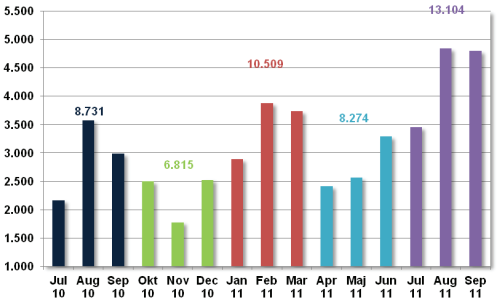
I nærværende afsnit beskrives kvantitative data fra de systemer og netværk, som DK•CERT har adgang til. Således beskrives tredje kvartal 2011 med udgangspunkt i det danske net til forsknings- og uddannelsesinstitutioner, Forskningsnettet. Hvor det er fundet nødvendigt, er disse suppleret og perspektiveret med data fra internettets åbne kilder. Afsnittet bør således også reflektere udviklingen på den øvrige danske del af internettet, men vil dog aldrig være fuldkomment.

Der indledes med en beskrivelse af udviklingen med hensyn til de hændelser, der gennem kvartalet er blevet rapporteret til DK•CERT. En væsentlig del af de rapporterede hændelser udspringer af malware. Vi forsøger derfor efterfølgende at give en status på udvikling og spredning af malware, samt heraf afledte hændelser som spam og phishing. Der afsluttes med data vedrørende de sårbarheder, der udnyttes ved it-kriminalitet. Her beskrives dels kvartalets nye sårbarheder, de sårbarheder som er forsøgt udnyttet og de sårbarheder, vi fandt ved scanning af vores kunders systemer og netværk.

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*".
Ponemon Institute, 2011; "*Second annual cost of cyber crime study*".
Symantec, 2011; "*2011 State of security survey*".
Symantec, 2011; "*Internetkriminalitet koster danskerne 1,7 milliarder om året*".

2.1. Kvartalets sikkerhedshændelser

I tredje kvartal 2011 steg antallet af henvendelser om sikkerhedshændelser til 13.104, hvilket er en stigning på 58 procent i forhold til andet kvartal (Figur 1). I alt



Figur 1. Sikkerhedshændelser rapporteret til DK•CERT.

gav det anledning til registrering af 12.411 unikke sikkerhedshændelser, som havde sit udspring i 6.439 forskellige IP-adresser.

Kun to hændelser blev i tredje kvartal kategoriseret som vellykkede hackerangreb. En del computere er dog blevet kompromitteret på anden vis. Således registrerede vi 56 hændelser, der omhandlede danske computere, som indgik i botnet. Også for danske websites, der var blevet inficeret med malware eller phishingsider, er der sket en stigning.

Antallet af hændelser, hvor kompromitterede danske websites blev udnyttet til hosting af malware og phishing-sider, steg i tredje kvartal til 284 (Figur 2), hvilket er det højeste, vi hidtil har registeret. Flere af de kompromitterede websites modtog vi henvendelser om fra mange forskellige kilder. I enkelte tilfælde blev samme host på ny kompromitteret, efter at hostingudbyderen var informeret og øjensynligt havde løst problemet. I andre tilfælde blev den skadelige kode ikke fjernet selv efter gentagne henvendelser. Til billedet hører, at sårbare legale websites er den væsentligste kilde til spredning af malware.

I alt modtog vi i tredje kvartal 893 rapporter om download af enkeltstående værker fra fil-delingstjenester, som blev overvåget af repræsentanter for rettighedshaverne. Her var 299 forskellige IP-adresser på det danske Forskningsnet ansvarlige for rapporterne fra repræsentanter for de udenlandske rettighedshavere.

Den generelle stigning i antallet af sikkerhedshændelser, som blev rapporteret til DK•CERT, kan primært tilskrives en stigning i hændelser om scanninger. Efter et fald gennem de seneste fire kvaraler, steg antallet af sikkerhedshændelser, der blev kategoriseret som scanninger (Figur 3). Således registrerede DK•CERT i tredje kvartal 10.467 hændelser om scanninger, hvilket er det højeste antal siden 2008. Da størstedelen skyldes automatiske rapporter fra kilder, vi har benyttet gennem flere år, er der ingen umiddelbar forklaring på denne stigning. Kategorien dækker scanninger, der har til formål at identificere tilgængelige host, services og sårbarheder på enkelte host samt på større netsegmenter. Derudover dækker en mindre andel hændelser, som reelt bør kategoriseres som forsøg på brute-force af SSH-tjenester.

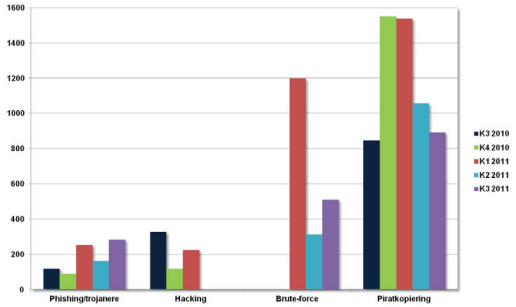
Som noget nyt fik vi i tredje kvartal 2011 flere henvendelser fra borgere, der var blevet forsøgt udsat for svindel via telefonen. Fra call-centre i Indien udgav man sig for at være fra Microsoft og fortalte, at brugerens computer var inficeret med virus. Herefter var målet at skaffe sig adgang til borgerens computer og kreditkortinformationer. I de tilfælde som blev rapporteret til DK•CERT, havde de snarrådige borgere dog lugtet lunten og afbrød opkaldet.

Et af de implicerede Call-centre har siden vist sig at være en Microsoft-partner. Microsoft har nu afbrudt samarbejdet med det.

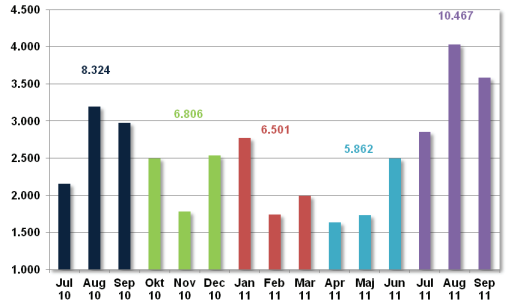
2.2. Malware, spam og phishing

Følgende citat af Randall Sutherland fra Toptenreviews.com sammenfatter de udfordringer vi i dag står overfor.

"Hackers continue to imagine and deploy malware that is a testament to the cunning genius of evil."



Figur 2. Væsentligste sikkerhedshændelser rapporteret til DK•CERT i tredje kvartal 2011.



Figur 3. Antal scanninger rapporteret til DK•CERT.

Stadig mere kompliceret og udspekuleret malware i form af virus, orme, trojanske heste og botnet-programmer er i dag de hyppigste angrebsformer. Alle medvirkende organisationer i en amerikansk undersøgelse foretaget af Ponemon Institute havde således oplevet angreb med en eller flere af disse typer skadelig kode.

I tredje kvartal 2011 identificerede antivirusproducenten F-Secure 1.910 malware-inficererede computere hos virksomhedens danske kunder. Med 39,2 procent af inficeringerne udgør trojanske heste stadigvæk den største trussel, som er steget en smule fra 35,2 procent i andet kvartal (Figur 4). Også andelen af malware, der kategoriseres som adware, steg fra 20,8 procent i andet kvartal til 25,1 procent i tredje kvartal.

Derudover er eneste væsentlige forskydning i de danske malware-inficeringer, at falske antivirusprodukter fra at udgøre 6,6 procent nu kun udgør 1,2 procent. Således er de på listen over de otte hyppigste danske malware-inficeringer blevet overgået af virus, som i tredje kvartal udgjorde 2,5 procent af inficeringerne.

Antallet af danske websites, som blev kompromitteret, med de formål at inficere de besøgende med malware og eller at franarre dem følsomme informationer steg i tredje kvartal 2011. Således registrerede vi 284 sikkerhedshændelser om danske websites, inficeret med trojanske heste eller phishing-sider, hvilket er det højeste antal vi hidtil har registreret. Der er tale om en stigning på 72 procent, som dog dækker over store månedlige udsving (Figur 5).

Symantec identificerede i august og september dagligt lige under 3.500 malware-inficerede websites, mens tallet i juli måned var næsten dobbelt så højt. Det er en stigning på godt 10 procent i forhold til kvartalet inden.

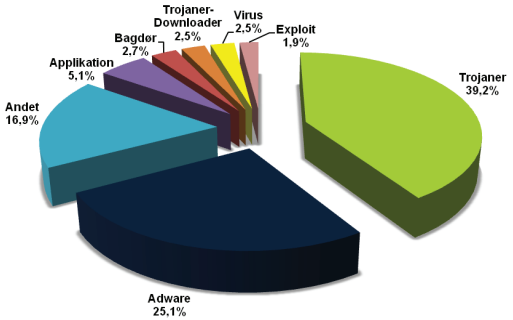
Spammængden har i tredje kvartal holdt sig relativt lav omkring 75 procent både globalt og i Danmark. I september udgjorde spam således 75,9 procent af alle mails på verdensplan, mens det herhjemme var 75,2 procent. Mere end 90 procent af de reklamerede produkter og tjenester i spam- mails faldt inden for kategorierne medicin, casino/gambling, uønskede nyhedsbreve, ure og smykker samt erotiske sider og sexdating.

Mens mængden af spam herhjemme har været på niveau med den globale mængde, har vi i højere grad været forskånet for både virus- og phishing-mails. Ifølge Messagelabs udgjorde virusmails herhjemme en ud af 489 mails i september måned, mod en ud af 203 mails globalt. Mens der globalt har været en mindre stigning i forhold til august, har vi herhjemme oplevet et mindre fald.

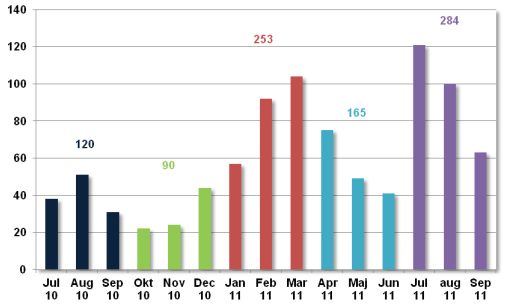
Samme tendens gør sig gældende for phishing-mails, om end det her er mere udtalt. I september var en ud af 208 mails på verdensplan forsøg på phishing, mens det i Danmark kun var en ud af 1.071 mails. Det var mere end en halvering i forhold til august, hvor en ud af 508 mails, der havnede i danskernes indbakker var en phishing-mail. Globalt set indeholdt de fleste phishing-mails links til sider, der var hostet i henholdsvis USA, Tyskland og England.

Metoderne der lokker brugere til sider med skadeligt indhold, er blandt andet brugen af URL-forkortelsestjenester, søgemaskineoptimering og spam udsendt på mail såvel som sociale netværkstjenester. Særligt de sociale netværkssiders udbredte brug af URL-forkortelser får i mange tilfælde brugere til at klikke på links, de ellers ikke ville have klikket på.

Kompromitterede populære og respekterede websites udgør ifølge virksomheden



Figur 4. Danske malware-infektioner identificeret af F-Secure i tredje kvartal i 2011.



Figur 5: Websites med trojanske heste og phishing-sider rapporteret til DK•CERT.

Bluecoat den største trussel i forbindelse med malwarespredning. Mange af de tjenester vi til dagligt benytter os af, er i dag gratis. Den primære årsag er, at de bliver finansieret af reklamer, som er blevet en uundgåelig del af vores hverdag. Det er ikke gået de it-kriminelles næse forbi, hvorfor malvertising fremstår blandt de væsentligste web-baserede metoder til spredning af malware.

I al sin enkelthed går metoden ud på, at man i reklamefællesskaberne får skabt tillid til sit domæne og de reklamer, man benytter til at promovere det. Først efter et stykke tid starter man sit angreb, typisk i weekenden, hvor sikkerhedsfolkene har fri. Sikkerhedsvirksomheden Bluecoat har beskrevet et angreb, hvor reklamen blev eksponeret på det gratis indiske nyhedssite Screenindia.com:

1. Et tredjepartsreklamelink pegede på det respekterede reklamedomæne Doubleclick.net.
2. Fra Doublecklick.net blev reklamen via et Javascript hentet fra Daniton.com, som var del af et større reklamefællesskab.
3. Ved første eksponering af reklamen skete der ingenting. Efterfølgende eksponeringer medførte , at der blev hentet et krypteret Javascript.
4. Scriptet udførte en iframe-injektion på siden, som hostede reklamen.
5. Iframen hentede herefter i al stilhed et PDF-exploit, som passede til den version af Adobe Reader, som blev benyttet. Siden hvorfra exploitet blev hentet, skiftede fra dag til dag.

Ovenstående eksempel skitserer, hvordan spredningen af malware foregår gennem stadig mere komplekse sammenhænge, som det er vanskeligt at gennemskue. For brugere af internettet er det bedste værn, at man sørger for at holde sine programmer opdaterede og benytter sig af software, som potentielt kan detektere og slette malware.

Microsoft fortsatte i september kampen mod botnet. Botnet er ansvarlig for megen af den internetkriminalitet, vi ser i dag, hvad enten det drejer sig om udsendelse af spam- og phishingmails, informationstyveri eller DDoS-angreb. Sidst på måneden lykkedes det med en domstolskendelse i hånden virksomheden at lukke 21 domæner, som blev benyttet af botnettet Kelihos. Det relativt lille botnet, hvis centrale servere var hostet i Tjekkiet, var ansvarlig for udsendelse af op mod 4 milliarder daglige spammails. Den ansvarlige for registreringen af det centrale domæne kan nu se frem til at komme for retten i Tjekkiet.

Bluecoat, 2011; "*2011 Mid-Year Web Security Report*".
Computerworld.com, 2011; "*Striking a domain provider, Microsoft kills off a botnet*".
F-secure, 2011; "*F-Secure security lab– virusworld map*".
Google online security blog, 2011; "*Trends in circumventing web-malware detection*".
Symantec, 2011; "*Symantec intelligence report: August 2011*".
Symantec, 2011; "*Symantec intelligence Report: September 2011*".
Ponemon Institute, 2011; "*Second annual cost of cyber crime study*".
Toptenreviews, 2011; "*Malware Trends According to Symantec*".

2.3. Sårbarheder

Mens det samlede antal nye CVE-nummererede sårbarheder i tredje kvartal faldt til det laveste antal, vi hidtil har registreret, steg antallet af CVE-nummererede sårbarheder, som findes og udnyttes på webapplikationer. I alt blev der offentliggjort 988 nye CVE-nummererede sårbarheder i tredje kvartal (Figur 6). Af disse udgjorde websårbarhederne 330 eller cirka 33 procent (Figur 7).

Hvor antallet af offentliggjorte CVE-nummererede websårbarheder for de fleste typer har holdt sig relativt konstant, er der sket en stigning i offentliggørelsen af websårbarheder, der giver mulighed for informationslækage. Antallet af disse er i tredje kvartal steget til 169. De er årsag til, at det samlede antal websårbarheder er steget med 60 procent i forhold til kvartalet inden. De hyppigst udnyttede sårbarheder på webapplikationer er ifølge Securityweek muligheden for SQL-injection, remote file inclusion, directory traversal og cross-site scripting.

Blandt kvartalets nye CVE-nummererede sårbarheder blev flere end halvdelen konstateret i browsere eller programmer og plugins, der typisk afvikles i browseren. Således var de fire applikationer med flest nye sårbarheder i tredje kvartal Google Chrome, Opera, Apples Safari og Mozillas Firefox (Figur 8). Længere nede på listen som nummer 13 var Adobe Flash Player. Sårbarheder i netop denne type programmer er også blandt de mest udnyttede til malware-inficering.

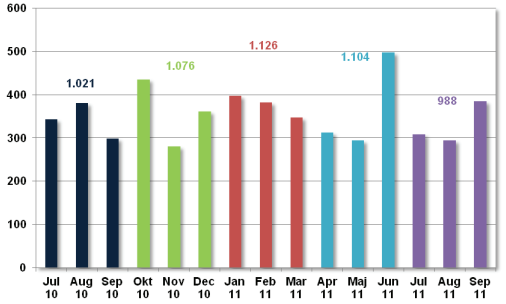
Derudover domineres listen over de programmer, hvori der blev offentliggjort flest nye sårbarheder, af Microsoft Windows i forskellige versioner. De stod for fem af de øverste 15 pladser. Det skyldes, at der er en høj grad af overlap mellem sårbarhederne, der konstateres i de forskellige Windows-versioner.

Antallet af sårbarheder, der konstateres og offentliggøres i en applikation er ikke nødvendigvis et udtryk for det enkelte produkts generelle sikkerhedsstatus. I lige så høj grad siger det noget om udbredelsen af applikationen, samt producentens fokus på sikkerhed, da mange sårbarheder først offentliggøres, når der er en opdatering. Endelig fortæller antallet heller ikke noget om den potentielle kompromitteringsgrad eller tilgængeligheden af exploits der udnytter sårbarheden. I sidste ende er det producentens evne til at rette sårbarhederne og forbrugernes villighed til at installere rettelserne, der afgør produktets aktuelle sikkerhedsstatus.

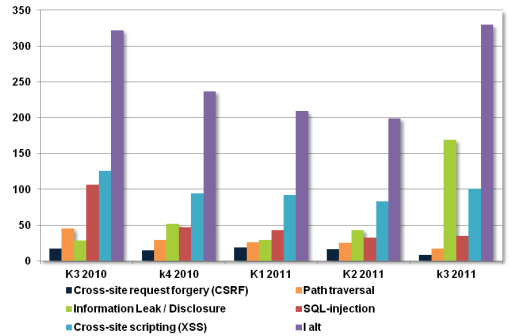
I tredje kvartal udførte DK•CERT analyse af 11 sårbarhedsscanninger mod i alt 3.664 forskellige IP-adresser på institutioner tilknyttet det danske Forskningsnet. Af de scannede IP-adresser modtog vi svar fra 138 som på scanningstidspunktet var tilgængelige fra internettet. Af disse blev der på 50, eller ca. 36 procent af de svarende adresser, fundet i alt 426 CVE-nummererede sårbarheder, eller i gennemsnit 8,5 på hver sårbar host. 89 af de fundne sårbarheder blev risikovurderet som kritiske. Kun 37 af de fundne sårbarheder var offentliggjort i 2011, mens resten var ældre.

Der blev ved scanningerne konstateret sårbarheder på i alt otte forskellige porte og/eller protokoller (Figur 9). Også i tredje kvartal var det webapplikationer, som lytter på TCP-port 80 (HTTP) og 443 (HTTPS), der var de mest sårbare. I alt blev 90,6 procent af de fundne CVE-nummererede sårbarheder konstateret på webapplikationer.

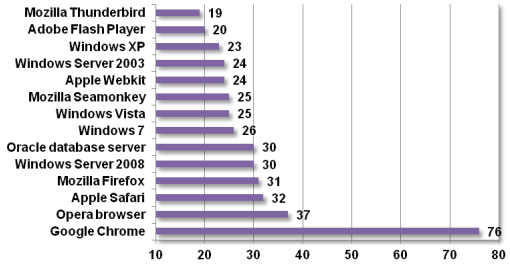
Den 9. august udgav Microsoft en opdatering til Internet Explorer (MS11-057), som rettede syv CVE-nummererede sårbarheder i version 6 til 9 på forskellige Windows-



Figur 6. Nye CVE-nummererede sårbarheder offentliggjort af NIST.



Figur 7. Nye CVE-nummererede websårbarheder offentliggjort af NIST.



Figur 8. Nye CVE-nummererede produktsårbarheder offentliggjort i tredje kvartal 2011.

konfigurationer. 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. De blev begge offentliggjort dagen før.

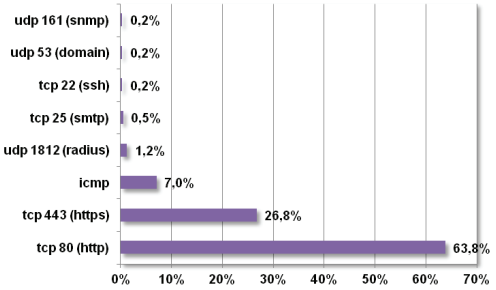
Også Adobe måtte den 9. august udsende en opdatering (APSB11-21), som rettede flere kritiske sårbarheder i Flash Player. Opdateringen rettede i alt 14 CVE-nummererede sårbarheder, der var tilgængelige på Windows, Macintosh, Linux, Solaris og Android. Sårbarhederne er tilgængelige i Flash Player i versioner tidligere end 10.3.183.5 og kan potentielt medføre, at en angriber får fuld kontrol over det angrebne system.

Også Mozilla havde i august måned været ved tasterne og 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.

Adobe, august 2011; "*Security update available for Adobe Flash Player*".
Adobe, september 2011; "*Security update available for Adobe Flash Player*".
Adobe, 2011; "*Security updates available for Adobe Reader and Acrobat*".
DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*".
Microsoft, 2011; "*Microsoft security bulletin MS11-057 – Critical*".
Mozilla, 2011; "*Mozilla foundation security advisory 2011-29*".
Nvd.nist.gov; "*CVE and CCE statistics query page*".
Securityweek, 2011; "*The most prevalent attack techniques used by today's hackers*".
Sophos, 2011; "*Vulnerability: MS11-057 - Critical cumulative security update for Internet Explorer (2559049*".



Figur 9. CVE-nummererede sårbarheder konstateret ved scanning i tredje kvartal 2011.

3. Overskrifter fra tredje kvartal 2011

Flere af kvartalets nyhedsartikler har deres udspring i udlandet og peger for nogles vedkommende tilbage på begivenheder, vi tidligere har beskrevet. Således blev konsekvenserne ved hackerangrebet mod RSA's SecurID-tokens først 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 ligger måske også en fortælling om, hvordan man i nogle dele af samfundet føler, at målet helliger midlet. Eller hvordan man går efter manden i stedet for bolden. 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 nemlig i stigende grad blevet et politisk værktøj, hvor den frie adgang til information i nogle tilfælde helliger de midler, der benyttes.

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

3.1. 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 derskabt 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 havdehackerne 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*".

3.2. 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 it-sikkerheden.

Konflikten rummer nogle interessante perspektiver set fra et it-sikkerhedssynspunkt. 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 CSC-konflikten. 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.

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

3.3. 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 danskerne 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

Figur 10. Phishing mail med Skat som afsender.

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.

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*".
Sophos, 2011; "*Microsoft dumps partner over telephone scam claims*".
PBS, 2011;"*Advarsel mod phishing-mail med PBS som afsender*".
Skat, 2011; "*Falsk e-mail lover skat tilbage*".

3.4. 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*".
Wikimedia.org, 2011; "*News International phone hacking scandal*".
Ekstra Bladet, 2011; "*Ekspert rystet over Folketings-sikkerhed*".
CSIS, 2011; "*CSIS' medvirken i Ekstra Bladet søndag d. 14 august*".

3.5. 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 it-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.

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*".
Wikipedia; "*Hactivism*".
Whyweprotest, 2011; "*Why We Protest*".

3.6. 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.

Figur 11. Fysisk protestaktion arrangeret i Anonomous-regi (whyweprotest.net).

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 smartphone 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 balladerne 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*".

3.7. 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*".

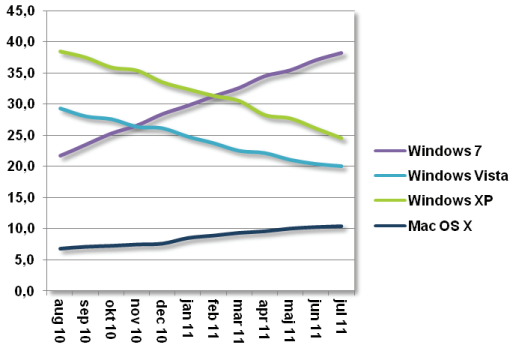
3.8. Manglende opdatering af Internet Explorer giver lav sikkerhed

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.

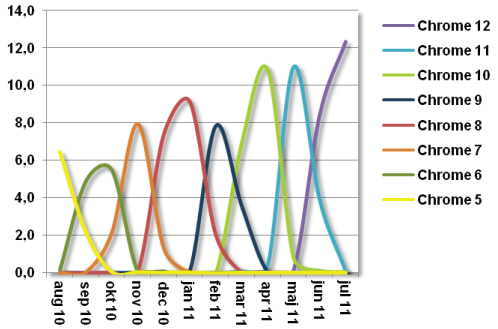
I juli måned blev Internet Explorer 9 benyttet af 18,0 procent af de danske internetbrugere, mens Windows 7 var installeret på 38,3 procent af deres computere (Figur 12). Kun for en mindre del kan forskellen tilskrives, at man i stedet har valgt en alternativ browser som for eksempel Firefox eller Chrome. 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 13).



Figur 12. Udbredelsen af Windows 7 og Internet Explorer hos danske internetbrugere.



Figur 13. Udbredelsen af Google Chrome hos danske internet brugere.

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.

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

3.9. 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*".
Version2, 2011; "*NemID phishet – 8 bankkunder frastjålet penge i netbank*".
Version2, 2011; "*Her er bagmanden: Sådan snød Arthur Williams NemID og stjal fra Nordea-kunder*".
Finansrådet, 2011; "*Netbankindbrud – statistik*".

4. 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: 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 det som de anser som censur og misbrug af nettet. Er særlig kendt for dens modstand mod scientologikirken og for sin støtte til Wikileaks og The Pirate Bay. Gruppen stod angiveligt bag det første angreb på Sony PlayStation Network og operation AntiSec i foråret 2011.

Bagdørsprogram: Et bagdørsprogram har til formål at skabe skjult adgang til et program, en service eller hele computeren. Man vil efterfølgende kunne bruge den etablerede forbindelse til at fjernstyre eller fjernovervåge den pågældende computer.

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 mellem de kommunikerende parter.

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 metode, hvor adressen på et sårbart website udnyttes til at vise yderlig information eller afvikle programmer. 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.

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).

Exploit: Et eksploit er kode, som forsøger at udnytte sårbarheder i software programmer med det formål at kompromitterer 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.

Hacking: Vi benytter i rapporten den gængse forståelse af begrebet, som dækker over en person, der uden foregående tilladelse forsøger at kompromittere computersystemers sikkerhed. Andre definitioner skelner 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-krininalitet. Vores brug af ordet dækker således over crackere og black hat hackere.

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.

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

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

Orm: Et program, der spreder sig i netværk ved at udnytte sårbarheder i dets computere. I TCP/IP-verdenen sker det typisk ved, at ormeprogrammet kontakter den port, som det sårbare program lytter på.

Phishing: Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på phishing optræder ofte i e-mails, der henviser til websider. Websiden angiver at tilhøre offerets bank eller kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol.

Pirate Bay: The Pirate Bay blev grudlagt i slutningen af 2003, som en del af det svenske Piratbyrån og 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.

Scanning, portscanning: Kortlægning af åbne porte på internettet, der har til formål at identificere sårbare services knyttet til dem. En portscanning foregår typisk ved, at der forespørges efter mange porte på få maskiner, eller én port på mange maskiner. Oftest benyttes et program til at foretage portscanninger. Brugen af firewalls vil som udgangspunkt lukke for adgangen til maskinens åbne porte.

Social engineering: Manipulation, der har til formål at få folk til at bidrage med informationer eller at udfører handlinger, som fx at klikke på links, svare på mails eller installere malware.

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.

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.

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 antispyware-programmer.

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 nu også gøre det. Virus spredes ofte som mail vedlagt en trojansk hest, der indeholder virussen selv.

Warez, pirat software: 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.

5. Figuroversigt

6. Referencer

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

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

Bluecoat, 2011; "*2011 Mid-Year Web Security Report*"; www.bluecoat.com/doc/16622

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

Computerworld.com, 2011; "*Striking a domain provider, Microsoft kills off a botnet*"; www.computerworld.com/s/article/9220321/Striking_a_domain_provider_Microsoft_kills_off_a_botnet

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

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

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/

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

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

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*"; http://sdb.cert.dk/login.php

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

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

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

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

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

Google online security blog, 2011;"*Trends in circumventing web-malware detection*"; static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/da//archive/papers/rajab-2011a.pdf

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

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

Mozilla, 2011; "*Mozilla foundation security advisory 2011-29*"; www.mozilla.org/security/announce/2011/mfsa2011-29.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, 2011; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

PBS, 2011;"*Advarsel mod phishing-mail med PBS som afsender*"; www.pbs.dk/da/temaer/nyheder/Pages/nyheder-20110825-advarsel-mod-phishing.aspx

Politiken, 2011; "*Dokumentation: Sådan har vi gjort*"; politiken.dk/indland/ECE1357129/dokumentation-saadan-har-vi-gjort/

Ponemon Institute, 2011; "*Second annual cost of cyber crime study*"; www.arcsight.com/library/download/second-annual-cost-of-cyber-crime-study

Redox, 2011; "*Politiken afslører højreekstrem loge*"; www.redox.dk/spip.php?article1170

Securityweek, 2011; "*The most prevalent attack techniques used by today's hackers*"; www.securityweek.com/most-prevalent-attack-techniques-used-todays-hackers

Skat, 2011; "*Falsk e-mail lover skat tilbage*"; www.skat.dk/SKAT.aspx?oId=1966219&vId=0

Sophos, 2011; "*Microsoft dumps partner over telephone scam claims*"; nakedsecurity.sophos.com/2011/09/21/microsoft-dumps-partner-telephone-support-scam/

Sophos, 2011; "*Vulnerability: MS11-057 - Critical Cumulative Security Update for Internet Explorer (2559049*"; www.sophos.com/support/knowledgebase/article/113983.html

Symantec, 2011; "*2011 State of security survey*"; www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf

Symantec, 2011; "*Internetkriminalitet koster danskerne 1,7 milliarder om året*"; www.symantec.com/content/da/dk/about/downloads/Internetkriminalitetkosterdanskerneprocent20_1.7milliarderomaret.pdf

Symantec, 2011; "*Symantec intelligence report: August 2011*"; www.symantec-cloud.com/da/dk/mlireport/SYMCINT_2011_08_August_FINAL_DK.pdf

Symantec, 2011; "*Symantec intelligence Report: September 2011*"; www.symantec-cloud.com/da/dk/mlireport/SYMCINT_2011_09_September_FINAL-DK.pdf

Theregister.co.uk, 2011; "*Comodo-gate hacker brags about forged certificate exploit*"; www.theregister.co.uk/2011/03/28/comodo_gate_hacker_breaks_cover/

Toptenreviews, 2011; "*Malware trends according to symantec*"; anti-virus-software-review.toptenreviews.com/malware-trends-according-to-symantec.html

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; "*NemID phishet – 8 bankkunder frastjålet penge i netbank*"; www.version2.dk/artikel/breaking-nemid-hacket-31480

Wikipedia; "*Hactivism*"; en.wikipedia.org/wiki/Hacktivism

Wikipedia; "*HTTP Secure*"; en.wikipedia.org/wiki/HTTP_Secure

Wikimedia, 2011; "*News International phone hacking scandal*"; www.secure.wikimedia.org/wikipedia/en/wiki/News_International_phone_hacking_scandal

Whyweprotest, 2011; "*Why We Protest*" www.whyweprotest.net

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