DK•CERT

Trendrapport

It-sikkerhed i andet kvartal 2011

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Jens Borup Pedersen, Tonny Bjørn og Dennis Panduro Rand, 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

DK•CERT modtog 21 procent færre henvendelser af sikkerhedshændelser i andet kvartal end i det foregående kvartal. Henvendelser om scanninger udgjorde over halvdelen af de 8.274 rapporter, som DK•CERT modtog.

Når det gælder skadelig software, var der også et fald: Sikkerhedsfirmaet F-Secure registrerede kun 847 infektioner. Det er mere end en halvering i forhold til første kvartal. Det lave tal kan enten skyldes, at færre pc'er blev inficerede, eller at flere infektioner slipper ubemærket forbi antivirusprogrammerne. Trojanske heste udgjorde en tredjedel af de registrerede infektioner.

De fleste angreb på it-systemer udnytter sårbarheder. I andet kvartal blev der offentliggjort 1.104 nye CVE-nummerede sårbarheder, hvilket er på niveau med de seneste kvartaler.

Adobe udsendte flere rettelser til Flash Player og Reader. Nogle af dem var til sårbarheder, som angribere udnyttede aktivt, før rettelserne blev udsendt. Der kom også en række kritiske rettelser fra Microsoft, Apple og Oracle.

Det store emne i sikkerhedsverdenen var angrebene på Sonys PlayStation Network og websteder. Flere både kendte og ukendte hackergrupper var involveret i angrebene, der medførte afsløring af informationer om millioner af brugere.

En udløber af Sony-angrebene var stiftelsen af hackergruppen LulzSec. Den offentliggjorde en række personoplysninger fra hackede servere, før den lukkede ned igen.

Kvartalet bragte også det første kendte eksempel på et angreb, der udnyttede data fra hackerangrebet på sikkerhedsfirmaet RSA i marts. Ved dette angreb kom nogle oplysninger om firmaets SecurID-teknologi til to-faktor-autentifikation i hackernes hænder. Det ser ud til, at disse oplysninger blev brugt i et angrebsforsøg rettet mod Lockheed Martin og flere andre leverandører til det amerikanske militær.

Falske antivirusprogrammer har længe plaget Windows-brugere. I andet kvartal kom Macintosh-brugerne i svindlernes søgelys. Programmet Mac Defender blev markedsført aggressivt, og mange faldt for svindlen og købte det virkningsløse sikkerhedsprogram.

I slutningen af maj skulle EU's såkaldte cookie-direktiv være trådt i kraft. Men det blev udskudt, da IT- og Telestyrelsen ønsker en afklaring af, hvordan reglerne skal fortolkes. Online-branchen havde frygtet kaos, hvis det ville blive et krav, at brugeren skal godkende det, hver gang der gemmes en cookie på vedkommendes pc.

2. Andet kvartal 2011 i tal

Mens der herhjemme ikke har været registreret succesfulde indbrud i danske netbanker det seneste halve år, formodes tabene ved svindel med kreditkortinformationer at være steget fra de 1,5 milliarder, vi i 2009 oplevede i Europa. En indikator på denne stigning er brugen af muldyr, som er registreret af Interpol.

Kreditkortdata indsamles ved hjælp af målrettede malware- og social enginering-metoder, som skal få folk til at afsløre deres kreditkortdata. Der har blandt andet været eksempler på telefonopkald, der havde til formål at franarre brugeren kreditkortinformation ved at foregive, at man repræsenterede en bank eller kreditkortselskab.

Sidstnævnte praksis lettes herhjemme ved den efter vores mening lemfældige omgang med personfølsomme data. I tide og utide afkræves vi cpr-nummer eller kreditkortinformation af sælgere af alt fra forsikringer til aviser og ugeblade, som blot ønsker at give os "den bedst mulige service" ved, at vi automatisk tilmeldes betalingsservice eller lignende. Det er helt almindelig praksis både på internettet, i de fysiske butikker og når en repræsentant for den service vi ønsker, ringer os op.

En fiktiv konkurrence på forbrugerrådets hjemmeside, taenk.dk, har senest sat fokus på dette problem. I håb om at vinde en iPad 2 afgav halvdelen af de 6.000 deltagere data i et felt til indtastning af cpr-numre. Hvorvidt cpr-numrene var valide, vides dog ikke, da man ikke gemte de indtastede data. Men resultatet af denne test er foruroligende.

Vi tager nu afsæt et helt andet sted - nemlig i de systemer og netværk, som DK•CERT har adgang til. I dette afsnit beskrives udviklingen i andet kvartal 2011 med udgangspunkt i data fra det danske net til forsknings- og uddannelsesinstitutioner, Forskningsnettet. Disse data er suppleret og perspektiveret med data fra internettets åbne kilder. Vi mener derfor, at afsnittet er beskrivende for udviklingen på den danske del af internettet.

Billedet vil dog aldrig være fuldkomment, da lokale omstændigheder kan medføre, at man nogle steder er mere udsat for industrispionage, denial of service eller phishing end andre steder. Vi håber, at afsnittet fremadrettet, i kombination med egne erfaringer og risikovurderinger, kan være med til at beskytte danskernes it-aktiver.

Afsnittet indledes med en kvantitativ beskrivelse af de forskellige hændelsestyper, som i løbet af kvartalet er rapporteret til DK•CERT. Herefter følger statistikker vedrørende udvikling og spredning af malware. Vi runder afsnittet af med at beskrive kvartalets nye sårbarheder, de sårbarheder vi finder ved scanning af vores kunders systemer, samt de sårbarheder der er set forsøgt udnyttet i løbet af perioden.

Europol.europa.eu, 2011; "*EU Organised Crime Threat Assessment - OCTA 2011*".
Finansrådet, 2011; "*Netbankindbrud - statistik*".
Taenk.dk, 2011; "*Forbrugerrådet kimet ned af vrede quizdeltagere*".

2.1. Sikkerhedshændelser i andet kvartal 2011

I forhold til årets første kvartal har vi i andet kvartal 2011 registreret et fald på 21 procent i antallet af henvendelser om sikkerhedshændelser. Vi modtog i alt 8.274 rapporter mod 10.509 i første kvartal 2011 (Figur 1), eller i gennemsnit næsten 2.760 henvendelser om måneden. Dette gav anledning til registrering af i alt 7.409 unikke sikkerhedshændelser, som udsprang af 3.134 forskellige IP-adresser placeret over hele verden.

Mængden af sikkerhedshændelser, hvor legale danske websites blev kompromitteret og herefter udnyttet til at hoste malware og/eller phishing-sider, faldt i andet kvartal. Vi registrerede kun 165 hændelser, som blev kategoriseret som phishing-sider eller malware. Det er et fald på 35 procent i forhold til første kvartal 2011 (Figur 2). På trods af dette fald tegner tallene et billede af, hvordan udnyttelse af sårbare legale websites indgår som en væsentlig del af de it-kriminelles aktiviteter.

På flere af de websites, som var blevet kompromitteret med phishing-sider eller malware, modtog vi henvendelser fra flere forskellige kilder. I enkelte tilfælde oplevede vi, at samme host på ny blev kompromitteret efter at udbyderen var informeret og øjensynligt havde løst problemet. I andre tilfælde oplevede vi, at man ikke fik fjernet skadelig kode på trods af gentagne henvendelser.

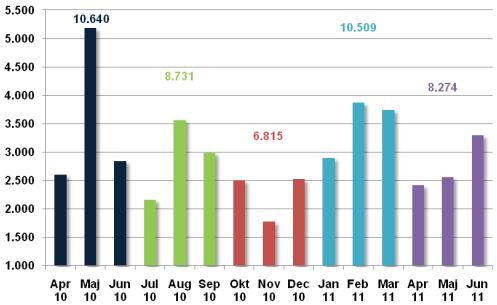
Tilsvarende modtog vi i andet kvartal 2011 færre henvendelser angående krænkelse af ophavsretten til film, musik og software foretaget fra danske IP-adresser, primært placeret på Forskningsnettet. I alt modtag vi 1.057 henvendelser mod 1.538 i første kvartal 2011. I alle tilfælde var der tale om download af enkeltstående værker fra fildelingstjenester, som blev overvåget af repræsentanter for rettighedshaverne.

I mange tilfælde udgør piratsoftware ikke blot et brud på kunsternes rettigheder - men også et brud på organisationens it-sikkerhedspolitik. Da det tidligere har været fremme, at op mod 25 procent af al piratsoftware indeholder malware, er der ikke blot tale om et ophavsretsligt problem, men i særdeleshed også en it-sikkerhedsmæssig problemstilling.

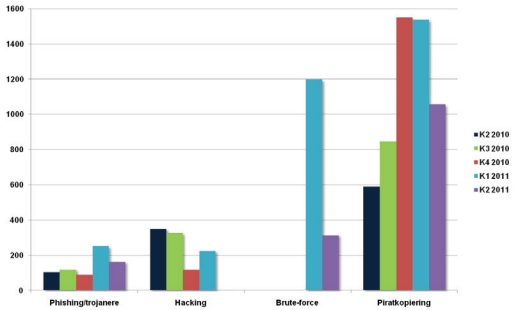
Antallet af sager kategoriseret som henholdsvis hacking og brute-force angreb, er der sket et væsentligt fald i forhold til tidligere. For disse hændelser formoder vi, at faldet primært skyldes DK•CERTs implementering af et nyt system til registrering af sikkerhedshændelser med heraf følgende nye hændelseskategorier. I forhold til første kvartal kan faldet tilsvarende tilskrives det generelle fald i rapporterede hændelser.

Der blev registreret 5.862 sikkerhedshændelser kategoriseret som scanninger. Det er et fald på 9,8 procent i forhold til første kvartal 2011. Kategorien dækker scanninger, der har til formål at identificere specifikke applikationer på store netsegmenter, forsøg på at afklare tilgængelige services og sårbarheder på enkelte host - samt i nogle tilfælde forsøg på brute-force angreb med brug af standardbrugernavne og passwords (Figur 3).

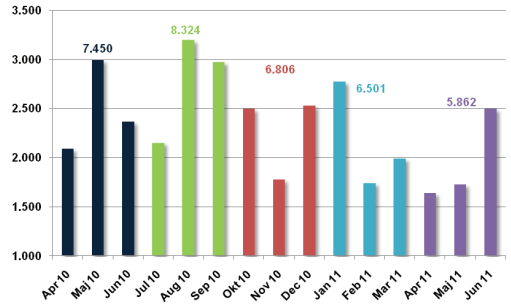
Scanninger mod større netsegmenter er i dag ikke i samme grad en del af den it-kriminelles værkstøjskasse, hvorfor DK•CERT betragter dem som et mindre alvorligt problem. En stor del af de scanninger vi registrerer, formodes at have rod i malware, som florerer i egne af verden, hvor nyeste softwareversioner og opdateringer er mindre udbredte end i Danmark. Her kan ældre malware stadig sprede sig, hvilket vi kan aflæse i statistikkerne.



Figur 1. Sikkerhedshændelser rapporteret til DK•CERT.



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



Figur 3. Antal scanninger rapporteret til DK•CERT.

2.2. Malware, spam og phishing

Teknisk direktør i PandaLabs, Luis Corrons, afspejler meget rammende en af de mange udfordringer som it-sikkerhedsbranchen stadig står overfor, når det drejer sig om bekæmpelse af malware.

"Users continue to fall victim to malicious links offering to take them to an exciting video or the new episode of their favorite TV show. This technique has become a weapon of choice for hackers as it requires minimum investment and attracts a large number of victims. Most of these sites download Trojans onto users' computers without their knowledge."

Mange klikker ukritisk på en spændende overskrift eller et link, når det dukker op på en vens Facebook-væg - eller tilsyneladende er ankommet med en vens e-mail-adresse som afsender.

Følsomme data handles i dag på det sorte marked, hvor de har deres eget segment i den kriminelle undergrundsøkonomi. Efterspørgslen på kreditkortinformationer, person- og virksomhedsdata har medført et stigende udbud af metoder til indsamling af data.

Metoderne er alt fra phishing i alle afskygninger til malwareudvikling og -spredning, hacking, specialiseret hosting af kode og infrastrukturer, som understøtter kommunikation, distribution, kodeindsamling og handel med data.

Sikkerhedsfirmaet F-Secure identificerede 847 danske malware-inficeringer i andet kvartal 2011, hvilket er et fald på 59,3 procent i forhold til første kvartals 2.082 registrerede inficeringer. Det er svært at komme med en forklaring på et så markant drop. På den positive side kan det skyldes, at danskerne er blevet bedre til at beskytte deres computere. Modsat kan det også skyldes, at antivirusproducenterne har stadig sværere ved at detektere den nyeste malware.

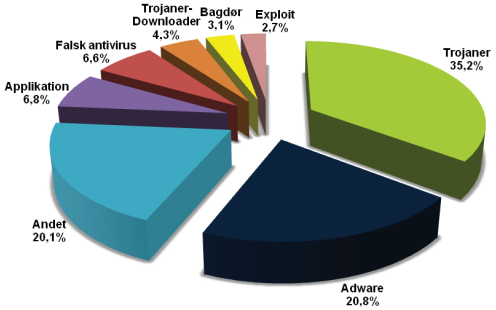
Den hyppigst identificerede form for malware i Danmark er stadig trojanske heste. De stod for 35,2 procent af inficeringerne (Figur 4). Malware, der blev kategoriseret som trojaner-downloader, stod for 4,3 procent. Det afspejler en tendens, hvor det er brugernes data, som har interesse for dem som distribuerer malware.

Yderligere forskydninger i danske inficeringer skal hovedsageligt findes i stigende andele af malware, som ikke har til formål at skaffe sig adgang til brugerens data. Således steg andelen af adware fra 14,7 procent i første kvartal 2011 til 20,8 procent i andet kvartal. Derudover er falske antivirusprogrammer ny på listen. De stod for 6,6 procent af inficeringerne. Ikke overraskende er de traditionelt definerede orme og virus igen fraværende på listen over danske inficeringer.

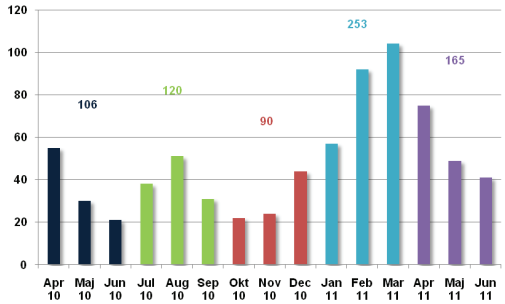
Inficeringer der blev kategoriseret som "andet", stod for 20,1 procent af de danske inficeringer i andet kvartal 2011. Det afspejler også antivirusproducenternes vanskeligheder med entydigt at kategorisere den malware som florerer.

Niveauet af sikkerhedshændelser, hvor danske websites blev inficeret med trojanske heste eller phishing-sider, var i andet kvartal 2011 stadig relativt højt set med danske øjne. Dog er der sket et fald på 34,8 procent i forhold til første kvartal (Figur 5). Det skal ses i relation til, at mængden af phishing-mails, der havnede i danskernes indbakker, tilsvarende er faldet.

Generelt afspejler vores tal de globale tendenser. I maj måned 2011 blokerede Mes-



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



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

sageLabs dagligt 3.170 websites med skadelig kode, hvilket var en stigning på 30,4 procent i forhold til april måned. Ifølge MessageLabs var næsten 25 procent af den webbaserede malware ny.

Video, installationsprogrammer, nøglegeneratorer og sociale netværk udgjorde i første kvartal 2011 lokkemidlet på mere end 75 procent af de inficerede websites, der blev blokeret af Panda Security. Der er ingen grund til at tro, at denne tendens har ændret sig væsentligt. Teknisk direktør i PandaLabs, Luis Corrons, siger i den forbindelse:

"Attackers exploit hot topics and users' morbid curiosity. Who is not interested in watching the latest footage of such a devastating natural disaster as Japan's recent earthquake?"

Midlerne til at få brugeren til at besøge sider med skadeligt indhold er URL-forkortelsestjenester samt promovering af links til skadelig kode gennem søgemaskineoptimering og spam udsendt på mail såvel som via sociale netværkstjenester.

Globalt set var mængden af spam relativt lav i andet kvartal 2011. Spam udgjorde i maj måned 75,8 procent af alle mails, mens den herhjemme udgjorde 73,9 procent. Det skal ses i forhold til, at spammængden i perioder af 2010 var oppe på over 90 procent.

En del af årsagen til denne udvikling skal muligvis findes i, at det i løbet af det seneste år er lykkedes at få lukket flere af de store spam-botnet. Mest interessant er i denne sammenhæng, at spammerne er begyndt at drive deres egne URL-forkortelsestjenester, som ikke har noget offentligt interface og ikke figurerer i søgemaskinerne.

Hvor den globale mængde af malware- og phishingmails generelt var konstant i forhold til første kvartal 2011, faldt den herhjemme. MessageLabs rapporterer, at kun én ud af 1.197 mails i maj måned var spam – samt én ud af 2.262 mails var relateret til phishing.

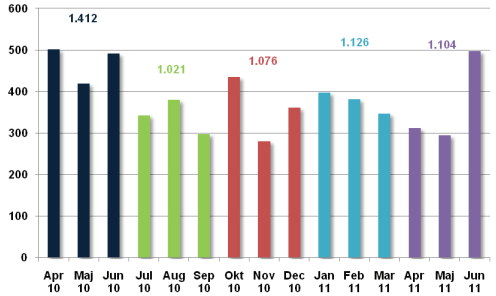
Europol.europa.eu, 2011; "*EU Organised Crime Threat Assessment - OCTA 2011*".
F-secure.com, 2011; "*F-Secure security lab – virus world map*".
Messagelabs.com, 2011; "*May 2011 intelligence report*".
Pandasecurity.com, 2011; "*Videos, Installers, Cracks and Social Media, Most Popular Baits Used by Hackers to Infect Users*".

2.3. Sårbarheder

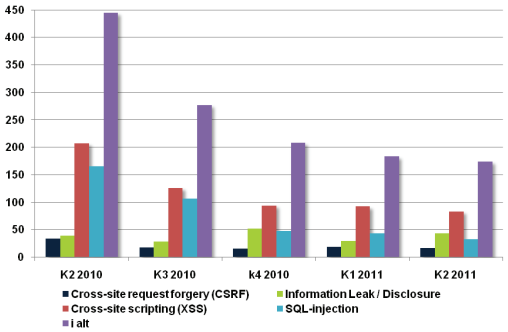
Andet kvartal 2011 bød på offentliggørelse af 1.104 nye CVE-nummererede sårbarheder, hvilket var på niveau med tidligere kvartaler (Figur 6). Set månedsvis kan dette tilskrives offentliggørelsen af en række sårbarheder i Microsofts produkter i juni måned, da både april og maj lå under det normale niveau.

Andelen af CVE-nummererede sårbarheder, der findes på standard webapplikationer, udgjorde 15,7 procent af de nye sårbarheder i andet kvartal, eller i alt 174 sårbarheder (Figur 7).

Hvor nye sårbarheder, som kunne medføre cross-site scripting, cross-site request forgery og SQL-injection er faldet svagt, er der sket en stigning på næsten 50 procent i offentliggørelsen af sårbarheder, som kan udnyttes til informationslækage.



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



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

Også i andet kvartal 2011 var cross-site scripting-sårbarheder de hyppigst offentliggjorte websårbarheder.

Microsofts styresystem Windows i stort set alle versioner stod i andet kvartal 2011 for en stor del af de applikationer, hvortil der blev offentliggjort nye CVE-nummererede sårbarheder (Figur 8). Linux-kernen og Apples styresystem Mac OS X var også at finde på denne liste. Som i første kvartal 2011 var det dog Googles browser Chrome, der toppede listen med offentliggørelsen af 57 nye sårbarheder.

Fraværet af sårbarheder i Adobe-produkter er iøjnefaldende. Kun Shockwave Player har fundet plads på listen over de 15 applikationer, hvortil der hyppigst blev offentliggjort nye sårbarheder. Netop sårbarheder i Shockwave, Flash, Acrobat og Adobe Reader har været et attraktivt middel for malwaredistribution.

Hvor mange sårbarheder, der findes og offentliggøres i enkelte systemer, må ikke tages som umiddelbart udtryk for det enkelte produkts generelle sikkerhedsstatus. Det kan til dels skyldes, at den enkelte producent kan have en politik om at offentliggøre sårbarheder i klumper frem for i takt med, at de findes.

Derudover inddrages der ikke faktorer som kompromitteringsgraden af de enkelte sårbarheder, udbredelsen af det enkelte system og/eller tilgængeligheden af exploits, der udnytter sårbarheden.

I andet kvartal 2011 foretog DK•CERT sårbarhedsscanninger af lige under 4.500 forskellige IP-adresser for institutioner på det danske Forskningsnet.

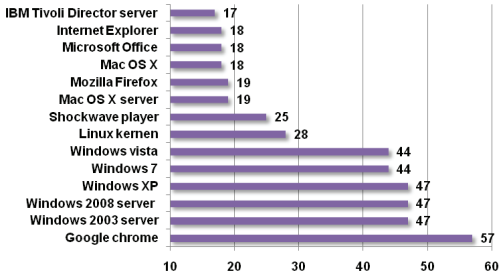
Andelen af svarende adresser var denne gang på næsten 12 procent, hvilket sandsynligvis må tilskrives en konfigurationsfejl på et Check Point VPN-modul, hvor administrationsporten (TCP-port 18264) sendte svar på vegne af klienterne bag firewallen. Det reelle antal svarende hosts må derfor påregnes at være væsentlig mindre, ligesom det fundne antal sårbarheder således også er relativt.

Medtages sårbarheder konstateret på TCP-port 18264, blev der på 44 procent af de svarende hosts konstateret i gennemsnit 2,8 sårbarheder. Cirka 20 procent af de konstaterede sårbarheder blev vurderet som kritiske, mens 75 procent er vurderet at udgøre en middel risiko. I alt blev der konstateret sårbarheder med 150 forskellige CVE-numre fordelt på i alt 14 forskellige TCP porte. Kun 16 af disse CVE-numre blev offentliggjort i 2011, 12 i 2010 mens resten var offentliggjort tidligere.

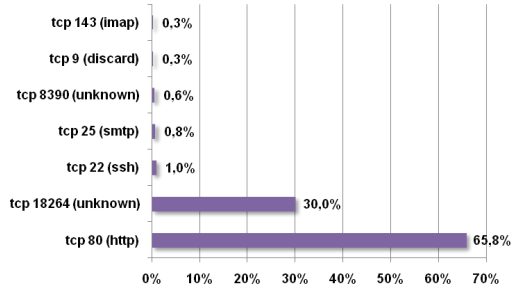
Ved scanningerne af vores kunders netsegmenter konstaterede vi igen i andet kvartal 2011 flest sårbarheder på TCP-port 80 (HTTP). Den benyttes af webapplikationer og var ansvarlig for 65,8 procent af alle fundne sårbarheder (Figur 9). Frasorteret sårbarheder på TCP-port 18264 udgjorde sårbarheder på webapplikationer 94 procent af den totale mængde.

I maj 2011 kom der en opdatering af Microsoft Safety Scanner. De første syv dages 420.000 downloads afslørede 20.097 inficerede computere med i gennemsnit 3,5 skadelige filer på hver.

Blandt de 10 hyppigst fundne skadelige filer indeholdt syv exploit-kode til sårbarheder i Suns Java Runtime Enviroment (JRE). Blandt disse var CVE-2008-5353, CVE-2010-0840, CVE-2010-0094 og CVE-2009-3867, der alle vurderes som kritiske. Fælles for sårbarhederne er, at de potentielt kan udnyttes på flere platforme. Ingen af dem var nye og burde derfor være rettet. Det skal hertil næves, at NemID benytter JRE.



Figur 8. CVE-nummererede produktsårbarheder offentliggjort i andet kvartal 2011.



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

Blandt kvartalets øvrige udnyttede sårbarheder var to sårbarheder i Flash Player, Acrobat og Adobe Reader. Begge sårbarheder (CVE-2011-0609 og CVE-2011-0611) blev offentliggjort i april og er kategoriseret som kritiske. Der blev inden offentliggørelsen fundet exploits til begge sårbarheder, der potentielt kan udnyttes på flere platforme.

Apple måtte i slutningen af maj frigive en sikkerhedsopdatering, som kunne finde og fjerne det falske sikkerhedsprodukt Mac Defender og alle dens afarter under OS X. Mac Defender har været en øjenåbner for Apple. De ved nu med sikkerhed, at de it-kriminelle har fået øje på deres styresystem og de potentielle muligheder, der ligger i at udnytte det.

Den 14. juni udgav Adobe igen en opdatering til Adobe Reader og Acrobat. Den rettede 13 CVE-nummererede kritiske sårbarheder, som var blevet offentliggjort i løbet af 2011. Sårbarhederne var tilgængelige og 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 i versionerne til og med 9. Den rettede otte sårbarheder, der kunne medføre kodeeksekvering, og tre sårbarheder som kunne resultere i informationslækage. Sårbarhederne var alle blevet offentliggjort tidligere på året.

Apple udsendte igen 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.

Adobe.com, 2011; "*Security updates available for Adobe Reader and Acrobat*".
Apple.com, 2011; "*About the security content of Mac OS X v10.6.8 and Security Update 2011-004*".
Apple.com, 2011; "*How to avoid or remove Mac Defender malware*".
Blogs.technet.com, 2011; "*Microsoft safety scanner detects exploits du jour*".
F-Secure.com, 2011; "*Internet Explorer cumulative security update*".
Nvd.nist.gov; "*CVE and CCE statistics query page*".

3. Overskrifter fra andet kvartal 2011

It-kriminaliteten har ifølge Europol medført et skift i de kriminelles demografiske profil, således at den adskiller sig fra andre organiserede transnationale kriminelle grupperinger. De individer som er engageret i it-kriminalitet, er i dag 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 har set som væsentlige. Enkelte af de begivenheder vi har udvalgt 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 it-sikkerhed som CERT for Forskningsnettet.

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

3.1. 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.org, 2011; "*Absolute Sownage - A concise history of recent Sony hacks*".
Computerworld.com, 2011; "*Sony says hacker stole 2,000 records from Canadian site*".
Dailytech.com, 2011; "*Anonymous engages in Sony DDoS attacks over GeoHot PS3 lawsuit*".
Networkworld.com, 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*".
Sophos.com, 2011; "*Sony BMG Greece the latest hacked Sony site*".
Sophos.com, 2011; "*Sony Pictures attacked again, 4.5 million records exposed*".

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-injection-sårbarheder. 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.

Veracode.com, 2011; "*Sony PSN Breach Infographic*".

3.2. RSA udsat for indbrud

Efter RSA var udsat for et hackerangreb, hvor informationer om SecurID Token-teknologien 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 sikkerhedsrisiko 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.com, 2011; "*Domains Used in RSA Attack Taunted U.S.*".
Msnbc.com, 2011; "*Lockheed Martin says it thwarted 'tenacious' cyber attack*".
Rsa.com, 2011; "*Open letter to RSA customers*".
Rsa.com, 2011; "*Open letter to RSA SecurID customers*".
Rsa.com, 2011; "*Our first priority is to ensure the security of our customers and their trust*".
Slashdot.org, 2011; "*RSA admits SecurID tokens have been compromised*".
Wired.com, 2011; "*RSA Agrees to Replace Security Tokens After Admitting Compromise*".

3.3. 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 kompromitterede 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.dk, 2011; "*Pas på viral Twitter app*".

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

3.5. 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 freemium-forretningsmodel.

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

3.6. 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 IKT-området 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.dk, 2011; "*OCES - Digital Signatur*".
Vtu.dk, 2011; "*It- og telepolitisk redegørelse 2011*".
Version2.dk, 2011; "*Derfor dropper DanID NemID som mobil-app*".

3.7. 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 EU-regler 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*".

3.8. 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?*".

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

3.10. 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 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

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.

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.com, 2011; "*LulzSec_BR*".
Pastebin.com, 2011; "*Nicks in #AntiSec on irc.AnonOps.net*".
Pastebin.com, 2011; "*Untitled*".
Statoilfuelretail.com, 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.

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.

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.

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

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.

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.

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

softwareprogrammer 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.

GovCERT: GovCERT-funktionen (Government Computer Emergency Response Team), der i Danmark varetages af It- og Telestyrelsen, 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.

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.

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 taget i drift i 1. juli 2010 og bliver drevet af firmaet 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.

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.

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 udføre 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, 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.

5. Figuroversigt

6. Referencer

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

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

Apple.com, 2011; "*About the security content of Mac OS X v10.6.8 and Security Update 2011-004*"; support.apple.com/kb/HT4723

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

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

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

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

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

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

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

Csoonline.com, 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

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/

Europol.europa.eu, 2011; "*EU Organised Crime Threat Assessment - OCTA 2011*"; www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.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; "*Netbankindbrud - statistik*"; www.finansraadet.dk/tal--fakta/statistik-og-tal/netbankindbrud---statistik.aspx

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

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

H-online.com, 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

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

Infosecurity-magazine.com, 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-

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

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

Lulzsecurity.com, 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

Messagelabs.com, 2011; "*May 2011 intelligence report*"; www.messagelabs.com/mlireport/MLI_2011_05_May_FINAL-en.pdf

Msnbc.com, 2011; "*Lockheed Martin says it thwarted 'tenacious' cyber attack*"; www.msnbc.msn.com/id/43199200/ns/technology_and_science-security/

Networkworld.com, 2011; "*PlayStation Network hack timeline*"; www.networkworld.com/news/2011/042711-playstation-network-hack.html

Nvd.nist.gov, 2011; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Pandasecurity.com, 2011; "*Videos, installers, cracks and social media, most popular baits used by hackers to infect users*"; press.pandasecurity.com/news/videos-installers-cracks-and-social-media-most-popular-baits-used-by-hackers-to-infect-users/

Pastebin.com, 2011; "*LulzSec_BR*"; pastebin.com/EuuwGwua

Pastebin.com, 2011; "*Nicks in #AntiSec on irc.AnonOps.net*"; pastebin.com/XiT943GZ

Pastebin.com, 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/

Rsa.com, 2011; "*Open letter to RSA customers*"; www.rsa.com/node.aspx?id=3872

Rsa.com, 2011; "*Open letter to RSA SecurID customers*"; www.rsa.com/node.aspx?id=3891

Rsa.com, 2011; "*Our first priority is to ensure the security of our customers and their trust*"; www.rsa.com/node.aspx?id=3876

Signatursekretariatet.dk, 2011; "*OCES - Digital Signatur*"; www.signatursekretariatet.dk/forside.html

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.com, 2011; "*Sony BMG Greece the latest hacked Sony site*"; nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/

Sophos.com, 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/

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

Squidoo.com, 2011; "*Mac Defender*"; www.squidoo.com/mac-defender

Taenk.dk, 2011; "*Forbrugerrådet kimet ned af vrede quizdeltagere*"; taenk.dk/nyheder/forbrugerr%C3%A5det-kimet-ned-af-vrede-quizdeltagere

Tdc.dk, 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

Twitter.com,2011; "*The Lulz Boat*"; twitter.com/#!/lulzsec

Veracode.com; 2011; "*Sony PSN Breach Infographic*"; www.veracode.com/resources/sony-psn-infographic

Version2.dk, 2011; "*Derfor dropper DanID NemID som mobil-app*"; www.version2.dk/artikel/19313-derfor-dropper-danid-nemid-som-mobil-app

Version2.dk, 2011; "*Forvirret? Få styr på de nye cookie-regler*"; www.version2.dk/artikel/forvirret-faa-styr-paa-de-nye-cookie-regler-18281

Vtu.dk, 2011; "*It- og telepolitisk redegørelse 2011*"; vtu.dk/publikationer/2011/it-og-telepolitisk-redegoerelse-2011/it-og-telepolitsk-redegoerelse-2011.pdf

Wikipedia.org; "*Freemium*"; en.wikipedia.org/wiki/Freemium

Wired.com, 2011; "*RSA Agrees to Replace Security Tokens After Admitting Compromise*"; www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/

Zdnet.com, 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

Kontakt:

DK•CERT, UNI•C
Centrifugevej, Bygn. 356
Kgs. Lyngby 2800

Tel. +45 3587 8887
URL: https://www.cert.dk
Email: cert@cert.dk