DK•CERT

Trendrapport

It-sikkerhed i tredje kvartal 2010

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Jens Borup Pedersen, 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

Tredje kvartal af 2010 bød på mange sager om piratkopiering. DK•CERT modtog markant flere henvendelser angående distribution af kopibeskyttet materiale fra udenlandske rettighedsindehavere.

Til gengæld var der et fald i antallet af sager om hacking. Det er dog ikke nødvendigvis udtryk for et fald i mængden af sager, men kan skyldes problemer med at kategorisere sagerne korrekt. Af samme grund blev en uforholdsmæssigt stor del af sagerne i tredje kvartal kategoriseret som "Andet."

Mængden af *scanninger* har stabiliseret sig på kvartalsplan, men med store udsving fra måned til måned. I tredje kvartal var *scanningerne* målrettet mod færre systemer og tjenester: Kun 64 forskellige porte og protokoller blev der *scannet* efter.

Færre danske computere blev inficeret med skadelig software: 4.404 infektioner mod 7.347 i første kvartal. Derimod steg mængden af spam: 93 procent af alle mails sendt til danske mailkonti var spam.

Blandt de mere interessante tilfælde af skadelig software var sagen om en bærbar Macintosh, der lod andre computere bruge sig som proxy-server. Sagen viser, at Apples platform nu også er offer for angreb.

Derudover blev flere danske computere ramt af *Stuxnet*, der udnyttede en hidtil ukendt *sårbarhed* i Windows' behandling af genveje.

120 danske web-steder blev inficeret med skadelig software eller *phishing*-sider. Det er flere end i andet kvartal, men færre end i første.

DK•CERT foretog i tredje kvartal 2010 sårbarhedsscanning af mere end 10.000 danske IP-adresser. Der blev fundet *sårbarheder* på knap 3,5 procent af dem. Af de fundne *sårbarheder* var hver fjerde kritisk.

Dansk Industri har fremsat forslag om, at staten går mere aktivt ind i bekæmpelsen af it-kriminalitet. Organisationen mener, at internetudbyderne kan deltage ved at blokere for adgangen til inficerede websteder. Endvidere er der brug for at give de berørte brugere hjælp og vejledning.

DK•CERT er enig og ser den nyoprettede GovCERT-funktion som et oplagt sted at placere ansvaret for at organisere og koordinere indsatsen på nationalt plan.

2. Tredje kvartal 2010 i tal

Mens det kan være vanskeligt at beskrive, hvor udviklingen fører os hen, er det straks nemmere at beskrive, hvordan enkelte områder af it-kriminaliteten har udviklet sig i forhold til tidligere. I dette afsnit lader vi tallene tale og forsøger at tage pulsen på it-sikkerheden i tredje kvartal af 2010.

Den væsentligste kilde til afsnittets data er de systemer og netværk, som vi i DK•CERT har adgang til, suppleret og perspektiveret med data fra internettets åbne kilder. Således beskriver data hovedsageligt udviklingen på det danske *Forskningsnet*. Vi mener dog, at de enkelte statistikker er med til at tegne et billede af it-kriminalitetens udvikling i hele Danmark. Et billede som ikke er fuldstændigt, men i kombination med egne erfaringer og systemer kan give et fingerpeg om, hvordan vi i fremtiden skal beskytte vores it-aktiver.

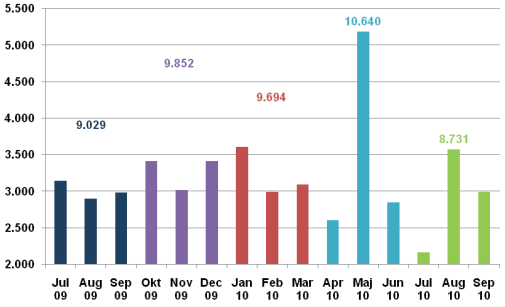
Afsnittet indledes med data, der beskriver sikkerhedshændelser anmeldt til DK•CERT i tredje kvartal af 2010. Derefter graver vi os ind i statistikkerne og beskriver, hvorledes udviklingen har været med hensyn til mængden og typen af de *scanninger*, som er blevet anmeldt til os, samt udvikling og spredning af *malware*. Begge emner er med til at præge de overordnede tal. Der afsluttes med data, der beskriver kvartalets nye offentliggjorte *sårbarheder*, samt enkelte overordnede tal vedrørende de *sårbarheder* vi finder ved *scanning* af vores kunders it-systemer.

2.1. Sikkerhedshændelser i tredje kvartal 2010

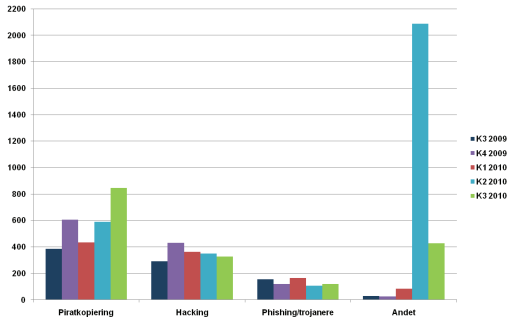
Når vi ser bort fra de usædvanligt mange sikkerhedshændelser, som blev anmeldt til DK•CERT i maj måned, cementerede tredje kvartal en svagt faldende tendens (Figur 1). Kvartalet bød på i alt 8.731 hændelser eller i gennemsnit 2.910 pr. måned. Det er et fald i forhold til de næsten 3.400 hændelser, der i gennemsnit blev anmeldt i første halvdel af 2010. Juli måneds 2.167 anmeldelser var således det laveste antal gennem mere end seks år. Mens antallet af automatisk registrerede og behandlede angrebsforsøg er faldende, kræver flere af anmeldelserne nu manuel indgriben.

Ud over de behandlede og registrerede anmeldelser har DK•CERT i august og september modtaget flere end 6.000 anmeldelser vedrørende danske IP-adresser, der har forsøgt at logge på en udenlandsk Postfix-tjeneste og derfor blev blokeret. Da disse sager også er sendt til de retmæssige ansvarlige, er de ikke medtaget i statistikkerne.

Mens sager vedrørende websites inficeret med *phishing*-sider eller *trojanske heste* har holdt sig nogenlunde konstant, har der gennem de seneste kvartaler været et fald i hændelser kategoriseret som "Hacking" (Figur 2). Dette kan bero på tilfældigheder, da kategorien ikke er entydig. Fx dækker kategorien over både vellykkede systemkompromitteringer såvel som i enkelte tilfælde mistanke om og forsøg på kompromittering. En del af de sager der tidligere blev kategoriseret som "hacking", kan formodes i tredje kvartal at være blevet kategoriseret som



Figur 1. Sikkerhedshændelser anmeldt til DK•CERT



Figur 2. Væsentligste hændelsestyper anmeldt til DK•CERT

"Andet". Det forklarer til dels at antallet af anmeldelser i denne kategori er så relativ stort i tredje kvartal. Det kan dog også være et udtryk for it-kriminalitetens stigende kompleksitet. Et stigende antal sager lader sig kun vanskeligt kategorisere entydigt, inden for de rammer DK•CERT systemer i øjeblikket muliggør

Tredje kvartal af 2010 bød på en markant stigning i antallet af henvendelser angående distribution af kopibeskyttet materiale fra udenlandske rettighedsindehavere (Figur 2). Ifølge en undersøgelse af den ikke uvildige organisation BSAA (Business Software Alliance of Australia) var 25% af al piratsoftware inficeret med *malware*[1]. Selv om det kan lyde af meget, har der i andre medier og sammenhænge tidligere været nævnt tal på over 80%. Piratkopiering kan således ikke blot være i strid med ISP'ernes retningslinjer og organisationernes it-sikkerhedspolitik, men også medføre kompromittering af de computere, der henter, bruger og distribuerer piratsoftware.

2.2. Scanninger

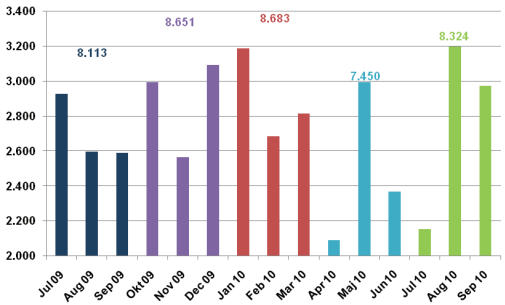
Med andet kvartal som en undtagelse har antallet af anmeldelser om *portscanninger* til DK•CERT stabiliseret sig gennem de seneste to år. Tredje kvartals 8.324 anmeldelser rammer således gennemsnittet, der det seneste halvandet år er på 2.750 månedlige anmeldelser, om end der har været store månedlige variationer (Figur 3). Fx var juli måneds 2.153 anmeldelser under normalen, mens der i både august og september kom flere anmeldelser end normalt.

Hvor der i både første og andet kvartal blev anmeldt *scanninger* mod 254 forskellige porte og protokoller, var de i tredje kvartal målrettet færre systemer og applikationer på kun 64 forskellige porte og protokoller. Tilsvarende havde de anmeldte *scanninger* udspring i kun 810 forskellige IP-adresser mod næsten 4.000 i andet kvartal. Hver IP-adresse gav således i gennemsnit anledning til lidt over tre anmeldelser.

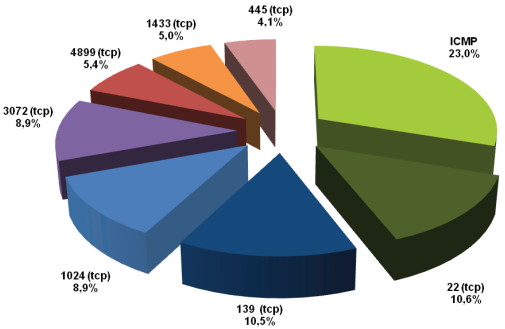
Næsten en fjerdedel af de anmeldte *scanninger* vedrørte netværksafsøgning af store netsegmenter med ICMP ping (Figur 4). Disse indgik i andet kvartal kun i 18,4% af de anmeldte scanninger. Isoleret set betragter vi ikke ICMP ping som et sikkerhedsproblem. I disse tilfælde er det derfor mængden af trafik snare end arten, der har givet anledning til, at det bliver registreret som en *scanning*.

Antallet af *scanninger* mod TCP-port 1024, 4899 og 5900, som bl.a. bruges til fjernadgang og fjernstyring af it-systemer, var mere end halveret i forhold til kvartalet inden. De udgjorde i tredje kvartal kun ca. 15% af de anmeldte *scanninger*. Derimod er *scanninger* mod SSH på TCP-port 22 næsten fordoblet og udgjorde 10,6% af *scanningerne*. En del af disse dækker over *brute-force*-angreb, hvor der forsøges login på tjenesten ved at "gætte" kombinationer af brugernavne og passwords. Tilsvarende er der sket en mindre stigning i antallet af *scanninger* mod henholdsvis Windows-systemer på TCP-port 139 og 445 samt Microsoft SQL Server på TCP-port 1433. *Scanninger* mod websystemer, der benyttes over HTTP og HTTPS på henholdsvis TCP-port 80 og 443, udgjorde i tredje kvartal i alt kun ca. 2% af de anmeldte *scanninger*.

1 *Computerworld.com.au, 2010; "The cloud will 'change piracy':BSAA".*



Figur 3. Scanninger anmeldt til DK•CERT



Figur 4. Hyppigst scannede portnumre i tredje kvartal 2010

2.3. Malware m.m.

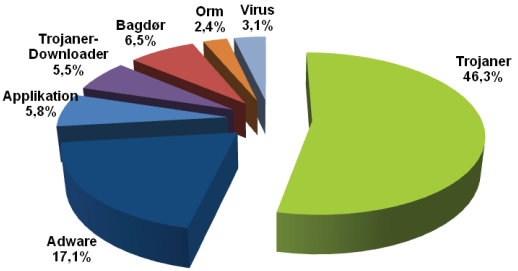
Mens sikkerhedsfirmaet F-Secure i tredje kvartal registrerede et faldende antal *malware*-inficerede danske computere svarende til 40% i forhold til første kvartal[2], har mængden af spam afsendt til de danske indbakker siden juli måned været stigende. Spammængden i Danmark udgjorde således i september 93,9% af alle mails, hvilket gjorde os til det 5. mest spammede land i verden, hvor gennemsnittet var på 91,7%[3].

I tredje kvartal af 2010 registrerede F-Secure 4.404 *malware*-infektioner på danske computere mod 7.347 og 4.559 i henholdsvis første og andet kvartal. Tilsvarende var en mindre del af de inficerede computere inficeret med *orme*, hvor andelen faldt fra henholdsvis 3,2% og 2.8% i første og andet kvartal, til 2,4% i tredje kvartal (Figur 5). Også for inficeringer med *trojanske heste* skete der herhjemme et fald i såvel antal og andel, mens infektioner med trojaner-droppere er steget. Hvorvidt og evt. hvordan *botnet*-programmer indgår i statistikken vides ikke. Det kan dog formodes at en del af disse detekteres som *trojanske heste*.

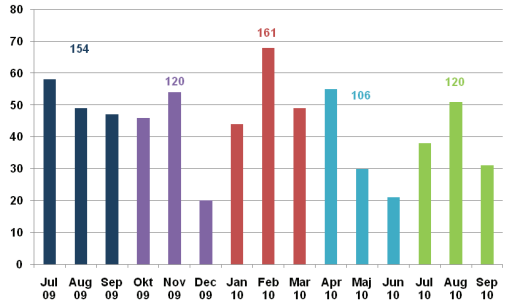
Når forskydningerne i danske inficeringer med *malware* over tid er så relativt beskedne, er det et udtryk for, at vi i 2010 har været forskånet for større udbrud af *vira* eller netværksbaserede *orme*. Mest bemærkelsesværdigt var det, da flere større danske virksomheder i slutningen af juli sloges med *ormen Stuxnet*. Fra vores eget perspektiv i DK•CERT gav en kundes inficerede bærbare Macintosh-computer anledning til løftede øjenbryn. Med Apples stigende markedsandele kan det dog forventes, at vi vil se mere skadelig kode, som er designet til eller som også virker på platforme fra denne producent.

Antallet af websites inficeret med *trojanske heste* eller *phishing*-sider, som i år er blevet anmeldt til DK•CERT, har været svingende. Hvad der i første halvdel af året lignede et fald er vendt, således at vi i tredje kvartal igen oplevede en stigning. I alt modtog vi anmeldelser om 120 danske websites, som var blevet inficeret med *phishing*-sider eller *trojanske heste*. Vi er dog stadig under niveauet fra årets første kvartal (Figur 6).

Mens vi hen over året har oplevet et mindre fald i de i mange tilfælde legale websites, der udnyttes til spredning af *malware*, tegner andre organisationer et andet billede. Således estimerede organisationen Dasient, at der i andet kvartal af 2010 på verdensplan var 1,3 millioner websites, der var inficeret med skadelig kode. Dette var en fordobling i forhold til kvartalet inden[5]. Tilsvarende blokerede Symantec i september et stigende antal websites, der var blevet inficeret med *malware*, der i mere end en femtedel af tilfældene var ny. I alt blev der dagligt blokeret 2.997 websites[6].



Figur 5. Hyppigste danske malware-infektioner identificeret af F-Secure i tredje kvartal i 2010[4]



Figur 6. Websites med trojanske heste og phishing-sider anmeldt til DK•CERT

2 *F-secure.com, 2009; "F-Secure security lab - virus world map".*

3 *Messagelabs.com, 2010; "MessageLabs intelligence september 2010".*

4 *F-secure.com, 2009; "F-Secure security lab - virus world map"*

5 *Dasient.com, 2010; "Continued growth in web-based malware attacks".*

6 *Messagelabs.com, 2010; "MessageLabs intelligence september 2010".*

2.4. Sårbarheder

I tredje kvartal af 2010 blev der offentliggjort i alt 1.021 nye *CVE-nummererede sårbarheder* (Figur 7). Det er et fald på ca. 28% i forhold til kvartalet inden. 277 eller 27% af de nye *sårbarheder* var *sårbarheder*, der typisk findes og kan udnyttes på webapplikationer (Figur 8). Det er tilsvarende et fald i forhold til andet kvartal, hvor de samme typer *sårbarheder* udgjorde 30% .

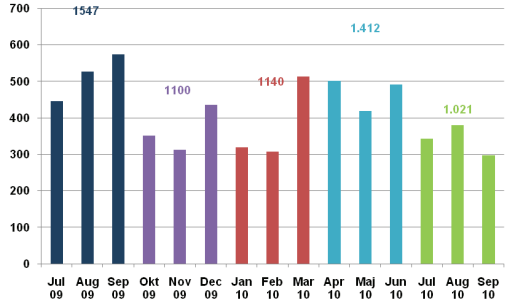
En analyse foretaget af organisationen Veracode viste, at otte ud af ti web-applikationer havde velkendte *sårbarheder*. Analysen bygger på data fra 3.000 applikationer og viste desuden, at tredjepartskomponenter var mindre sikre end den software, som organisationerne selv havde udviklet. *Cross-site-scripting* var den hyppigst konstaterede *sårbarhedstype* på de testede webapplikationer[7].

Blandt de applikationer der i tredje kvartal af 2010 hyppigst blev konstateret nye *CVE-nummerede sårbarheder* i, var forskellige versioner af Windows (Figur 9). Listen toppes dog af browsere fra henholdsvis Google og Mozilla, hvorimod hverken Microsoft Internet Explorer eller Apples styresystem Mac OS X (hverken klient- eller serverversion), heller ikke denne gang var at finde i top tyve. I tillæg til de *sårbarheder* der offentliggøres med et *CVE-nummer*, vil mange organisationer have *sårbarheder*, der knytter sig til deres specifikke implementering af systemer og applikationer.

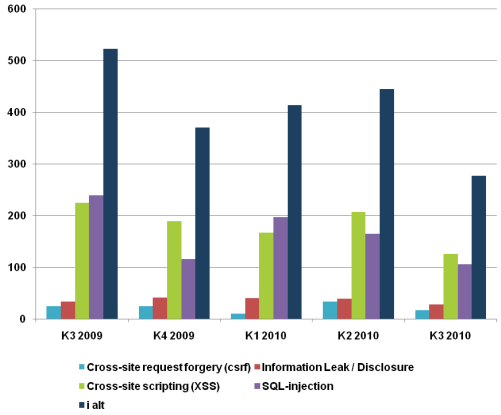
Kvartalets væsentligste *sårbarhed* blev opdaget af Microsoft allerede den 16. juni. *Sårbarheden* (CVE-2010-2568), der blev klassificeret som kritisk, muliggjorde eksekvering af kode ved at udnytte en fejl i Windows' måde at håndtere genveje på. *Sårbarheden* var tilgængelig i Windows XP og senere versioner af Windows. Inden Microsoft den 2. august frigav en rettelse til *sårbarheden*, var den flere gange blevet udnyttet af *malware*[9]. Blandt andet blev *sårbarheden* udnyttet til spredning af *Stuxnet* via USB-nøgler .

DK•CERT foretog i tredje kvartal 2010 *sårbarhedsscanning* af mere end 10.000 forskellige IP-adresser, som primært er placeret på det danske *Forskningsnet*. Af de *scannede* IP-adresser svarede lidt over 10%. De øvrige adresser må formodes at være tilknyttet en maskine, der på tidspunktet for *scanningen* var slukket, ikke var i brug eller beskyttet bag en firewall. Næsten 3,5% af de *scannede* IP-adresser var *sårbare* med i gennemsnit næsten 17 *CVE-nummererede sårbarheder* hver. Dette er en stigning i forhold til kvartalet inden, hvor de sårbare systemer i gennemsnit kun havde 9 *sårbarheder*. Af de fundne *sårbarheder* blev næsten hver fjerde kategoriseret som kritisk.

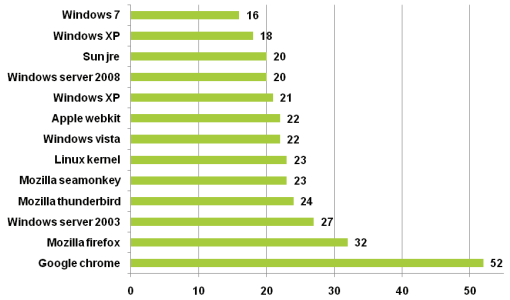
De konstaterede *sårbarheder* var fordelt på 82 forskellige porte og protokoller. Web-applikationer, der benytter TCP-port 80 og 443 var også i tredje kvartal de mest sårbare; Tre fjerdedele af alle *sårbarheder* blev konstateret på disse porte. Derudover udgjorde mailsystemer, der svarede på TCP-port 25, 993 og 995, et nyt problem. På disse blev der konstateret i alt mere end 5% af alle *sårbarheder*. Set i lyset af en stigende mængde spam, er dette problematisk. Et andet hidtil uset



Figur 7. Offentliggjorte CVE-nummererede sårbarheder



Figur 8. Offentliggjorte CVE-nummererede websårbarheder pr. kvartal[8]



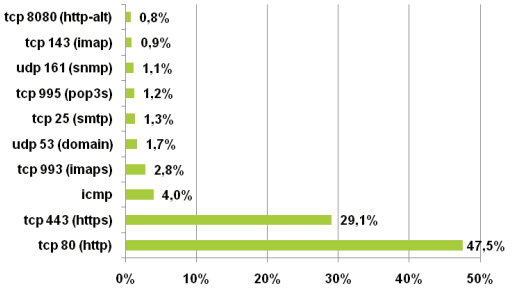
Figur 9. CVE-nummererede sårbarheder offentliggjort i tredje kvartal 2010

7 *Veracode.com, 2010; "State of software security report".*

8 *nvd.nist.gov; "CVE and CCE statistics query page".*

9 *Pandasecurity.com, 2010; "Quarterly Report PandaLaps (july-september 2010)".*

problem er *sårbarheder* på UDP-port 53, der benyttes til navneopslag (DNS) på internettet (Figur 10).



Figur 10. CVE-nummererede sårbarheder konstateret ved scanning i tredje kvartal 2010

3. Overskrifter fra tredje kvartal 2010

Nedenfor beskrives nogle af de begivenheder, som var med til at præge tredje kvartal af 2010. Afsnittet beskriver både historier, der ramte medierne samt en enkelt begivenhed fra vores egen funktion som CERT for *Forskningsnettet*. Fælles er, at de enkelte hændelser er med til at tegne et billede af udviklingen, som vi i it-sikkerhedsbranchen og samfundet som helhed bliver nødt til at forholde os til.

3.1. Det skulle være så Nemt

Ved at lægge det centrale cpr-registers it-systemer ned gik det nye NemID 1. juli i luften med et brag. NemID er en fælles dansk login-løsning til netbanker og offentlige hjemmesider. Løsningen lanceres som en brugervenlig erstatning for den digitale signatur, der aldrig rigtigt er slået igennem hos borgerne. Den er således et kompromis mellem sikkerhed og brugbarhed. Efter planen vil alle danske netbankbrugere modtage NemID inden udgangen af 2010.

NemID har gennem hele dets korte levetid været udsat for kritik om, at det ikke var sikkert nok. Blandt andet er løsningen blevet kritiseret for at:

- Anvende en Java-applet, der har adgang til alle brugerens data.
- Brugernes personlige nøgler opbevares centralt.

Grundlæggende vil NemID i forhold til de etablerede netbankløsninger give forøget sikkerhed for både brugerne og bankerne. Også i forhold til de øvrige tjenester, der forventes at bruge NemID, vil løsningen tilbyde bedre beskyttelse mod misbrug af private oplysninger og data.

3.2. Ormehuller i industrielle it-systemer

I slutningen af juli måned udsendte Microsoft en advarsel mod *ormen Stuxnet*, der udnyttede en *sårbarhed* i den måde, Windows behandler genveje på. Der var på daværende tidspunkt ingen rettelse til *sårbarheden*. Den avancerede *orm* indeholder en *trojansk hest* og angriber primært industrielle kontrolsystemer.

I første omgang spredte *ormen* sig hovedsageligt i Asien og Mellemøsten, men senere blev også danske virksomheder ramt. Således blev det i pressen blandt andet beskrevet, hvordan man i A.P. Møller-Mærsk gennem flere uger måtte slås med oprydningen, efter at 300 computere var blevet ramt. Udbruddet skabte dog ifølge virksomheden selv ikke afbrydelser i forretningen[10].

NemID

NemID er en fælles dansk login-løsning til netbanker og offentlige hjemmesider. Løsningen blev taget i drift i 1. juli 2010 og bliver drevet af firmaet DanID. NemID kan benyttes fra en hvilken som helst computer uden foregående installation af software.

NemID kræver et certifikat til den offentlige digitale signatur og består af en personlig adgangskode og et nøglekort, hvor hver kode kun bruges én gang. Ad-gangen til netbank eller andre tjenester, der benytter NemID er således sikret mod at blive afluret, da den vil være forskellig fra gang til gang.

Stuxnet

Stuxnet udnytter en *sårbarhed* i Windows behandling af genveje. Efter udnyttelse af Windows-*sårbarheden* angriber *Stuxnet* Siemens WinCC SCADA, der blandt andet anvendes i elforsyning og industriproduktion. *Ormen* synes at være målrettet informationstyveri fra industrien.

Ormen spredes via USB-nøgler og inficerer system- og programfiler, på samme måde som en traditionel *virus*. Koden muterer, hvilket gør det vanskeligt at kategorisere og spore den. *Stuxnet* indeholder en *trojansk hest*, der opdaterer sig selv og kommunikerer via signerede *P2P*-forbindelser.

Stuxnet er blandt de mest målrettede og avancerede orme, vi endnu har set. Flere mener, at den er udviklet med statssupport og -finansiering. Fx mener nogle, at *ormen* er målrettet indsamling af data fra det iranske atomprogram[11].

10 *Version2.dk, 2010; "Viruskrig på to fronter: Mærsk også ramt af genvejsvirus på kontrolsystemer".*

11 *Wikipedia.org , 2010; "Stuxnet".*

3.3. PBS-phishing igen-igen

Den 23. august ramte endnu en *phishing*-mail danskerne. Mailen var øjensynlig afsendt af PBS og opfordrede modtageren til at oprette koder til hhv. MasterCard SecureCode og Verified by Visa. Formålet var at lokke modtageren over på en hjemmeside hostet af internetfirmaet Yahoo, hvor man kunne fiske modtagernes kreditkortdata. Ifølge sikkerhedsfirmaet CSIS er angrebet udført af den samme bande, der stod bag et næsten identisk forsøg i 2009[12].

Et tilsvarende *phishing*-angreb ramte Danmark en uge senere. Den 27. august kunne man igen i sin indboks møde en mail, der angiveligt var afsendt fra PBS og opfordrede modtageren til at oprette en Verified by Visa-kode. Denne gang var mailen vedlagt et HTML-dokument, som linkede til en *phishing*-side.[13]

Som kontrast til angrebenes omfang blev de ikke vurderet at være lige så succesfulde som tidligere. På trods af et fejlfrit dansk og en korrekt beskrivelse af de to sikkerhedskoder fra Visa og Mastercard blev mailen mange steder blokeret, inden den nåede danskernes indbakke. En væsentlig årsag til dette er, at PBS har implementeret *Sender Policy Framework, SPF*, på deres mailserver. De organisationer der tilsvarende havde implementeret *SPF* på deres mailserver, blokerede herefter mailen.

3.4. Staten bør bekæmpe it-kriminelle

Den 8. september fortalte Dansk Industri i pressen, at man nu anså it-kriminalitet som så stort et problem, at den danske stat burde gå til angreb på de it-kriminelle. Særligt bekæmpelsen af *botnet* blev anset for et fælles nationalt anliggende. Således udtalte chefkonsulent Henning Mortensen til Danmark Radio:

"Vi betragter bot-netværk som værende blandt de mest aktuelle trusler i det danske it-sikkerhedsbillede. Det er samtidig en trussel, som vi vurderer vil blive forværret i de kommende år".

Dansk Industri foreslår en tostrenget strategi, hvor man dels i ISP'ernes netværk blokerer adgangen til inficerede sites på samme vis som børneporno-filteret, og dels hjælper brugerne, som er blevet inficeret. Dansk Industri forslår, at der udpeges en offentlig myndighed som IT & Telestyrelsen, som i samarbejde med ISP'erne skal varetage opgaven[14].

DK•CERT har flere gange tidligere påpeget it-kriminalitet som et fællesnationalt anliggende, som vi mener ISP'erne bør indgå aktivt i bekæmpelsen af. Den nyoprettede nationale *GovCERT*-funktion vil være et oplagt sted at placere ansvaret for at organisere og koordinere indsatsen.

---

12 *Version2.dk, 2010; "Antispam-våbnet SPF begrænser dansk PBS-phishing".*

13 *Version2.dk, 2010; "Pas på igen: Ny mail fra 'PBS' er også humbug".*

14 *Dr.dk, 2010; "DI: Staten bør bekæmpe it-kriminelle".*

3.5. Macintosh-trojansk hest på dansk universitet

Malware er oftest noget, vi hører, rammer Windows-systemer, men i september måned blev en bærbar Macintosh-computer på et dansk universitet ramt. Dette er, trusselsbilledet taget i betragtning, ikke bemærkelsesværdigt. Det bemærkelsesværdige er snarere, hvordan denne ene Macintosh havde indflydelse på det meste af instituttets netværksdrift.

Den inficerede maskine svarede på *DHCP*-forespørgelser fra det lokale net, hvor den udleverede sin egen IP-adresse som henholdsvis gateway og navneserver. Derved fungerede den som proxy for de maskiner, der benyttede den som *DHCP*-server. Således ville det fx være muligt at opsnappe brugernavne og passwords eller lade maskinen indgå som *Man in the Middle*.

Heldigvis udleverede den inficerede computer IP-adresser i et netsegment, der ikke var gyldigt på det lokale net. Det medførte, at de maskiner, som benyttede den som *DHCP*-server, ikke kunne komme på nettet. At computeren var bærbar og sandsynligvis var blevet inficeret et andet sted medførte således, at hændelsen blev opdaget og afværget. Hvad der ramte maskinen er i skrivende stund uvist. Flere *trojanske heste*, heriblandt nogle målrettet Macintosh, har udvist samme adfærd.

Hvorvidt stigende mængder *malware* målrettet Macintosh-systemer skal tages som succesparameter for udbredelsen af Apples computere, vil vi her lade være usagt.

3.6. Museballade på Twitter

Om morgenen den 21. september dukker de første rapporter om en *cross-site-scripting (XSS) sårbarhed* på Twitter.com op. *Sårbarheden* i Twitters indbyggede linkfortolker gjorde det muligt at udløse Javascripts, fx når brugeren bevæger musen over et link. Der gik ikke lang tid, før de første *tweets* med skadelig kode blev postet og *sårbarheden* blev udnyttet i *drive-by-angreb*[15].

Senere på dagen meddelte Twitter på sin blog, at det aktuelle hul nu var blevet lukket, og man samtidig havde lukket for en relateret *sårbarhed*. *Sårbarheden* var blevet opdaget og rettet en måned tidligere, men var i forbindelse med en opdatering af sitet ved en fejl igen blevet aktiv. Fra Twitters side mente man ikke at *sårbarheden* havde været udnyttet til andet end "sjov" [16].

15 *Version2.dk, 2010; "Museballade på Twitter: Sårbarhed udnyttes til angreb via 'tweets'*

16 *Twitter.com , 2010; "All about the 'onMouseOver' incident".*

4. Ordliste

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.

Clickjacking: Angreb, hvor besøgendes klik på en hjemmeside udnyttes til at aktivere indhold, som denne ikke er klar over eller ikke kan se. Herved risikerer brugeren fx at klikke på indhold eller aktivere funktioner på anden webside uden at vide det. Click-jacking kan således benyttes til informationsindsamling fra fx brugerens sociale netværksprofiler, spredning af malware og egentlig systemkompromittering.

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 fx 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 fx 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.

DHCP, Dynamic Host Configuration Protocol: DHCP er en del af TCP/IP protokolsuiten, der administrerer tildeling af IP-adresser til computere på netværket. DHCP-klienten sender en UDP forespørgsel på det lokale net, hvorefter DHCP serveren sørger for, at den får tildelt en ofte dynamisk IP-adresse samt informationer om netværkstrukturen (subnetmaske, gateway, DNS oplysninger m.fl.).

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 (Government Computer Emergency Response Team) funktionen, 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.

Man in the Middle: En angrebsform, hvor kommunikationen mellem to parter uden parternes viden, relæs gennem en "mand i midten", der aktivt kan kontrollere kommunikationen. I praksis kan et Man in the Middle angreb fx foregå ved en ændring af DNS-registrering enten på DNS-serveren eller ved ændring af hosts-filen.

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

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

Phishing: Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på phishing optræder ofte i e-mails, der henviser til websider. Websiden angiver at tilhøre offerets bank 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.

SPF, Sender Policy Framework: En udvidelse til SMTP-protokollen, som muliggør filtrering af e-mails baseret på den afsendende mailservers IP-adresse og den benyttede e-mailadresse. Ved registreringen af et domæne angives en SPF record, der fortæller hvilke(n) mailservere, der må benytte dette. Benyttes SPF af den modtagne mailserver, foretager den et opslag på afsenderdomænets SPF-record og hhv. afviser eller godkender mailen på baggrund af dette.

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.

Stuxnet: Stuxnet er blandt de hidtil mest avancerede orme. *Ormen* spreder sig via USB-nøgler ved at udnytte en *sårbarhed* i Windows' behandling af genveje. Herefter angriber den industrielle Siemens WinCC SCADA-systemer. *Ormen* indeholder en *trojansk hest*, hvorfor det menes, at den er målrettet informationstyveri fra industrien.

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, *botnet*programmer og lignende. Trojanske heste identificeres ofte af antivirus- og antispywareprogrammer.

Tweet: En tweet er en tekst besked på op til 140 karakterer postet på en brugerprofil i den sociale netværkstjeneste Twitter.

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

Computerworld.com.au, 2010; "*The cloud will 'change piracy':BSAA*"; http://www.computerworld.com.au/article/361149/cloud_will_change_piracy_bsaa/

Dasient.com, 2010; "*Continued growth in web-based malware attacks*"; http://blog.dasient.com/2010/09/continued-growth-in-web-based-malware_9357.html

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

F-Secure.com, 2010; "*F-Secure security lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

Messagelabs.com, 2010; "*MessageLabs intelligence september 2010*"; http://www.messagelabs.com/mlireport/MLI_2010_09_September_FINAL_EN.PDF

Messagelabs.co.uk, 2010; "*MessageLabs intelligence*"; http://www.messagelabs.co.uk/intelligence.aspx

Nvd.nist.gov, 2010; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Pandasecurity.com, 2010; "*Quarterly Report PandaLaps (july-september 2010)*";http://prensa.pandasecurity.com/wp-content/uploads/2010/09/Quarterly-Report-PandaLabs-3-Q-2010.pdf

Twitter.com , 2010; "*All about the 'onMouseOver' incident*"; http://blog.twitter.com/2010/09/all-about-onmouseover-incident.html

Veracode.com, 2010; "*State of software security report*"; http://www.veracode.com/images/pdf/soss/executive-summary-veracode-state-of-software-security-report-volume2.pdf

Version2.dk, 2010; "*Antispam-våbnet SPF begrænser dansk PBS-phishing*"; http://www.version2.dk/artikel/15951-antispam-vaabnet-spf-begraenser-dansk-pbs-phishing

Version2.dk, 2010; "*Museballade på Twitter: Sårbarhed udnyttes til angreb via 'tweets'*"; http://www.version2.dk/artikel/16289-museballade-paa-twitter-saarbarhed-udnyttes-til-angreb-via-tweets

Version2.dk, 2010; "*Pas på igen: Ny mail fra 'PBS' er også humbug*"; http://www.version2.dk/artikel/16008-pas-paa-igen-ny-mail-fra-pbs-er-ogsaa-humbug

Version2.dk, 2010; "*Viruskrig på to fronter: Mærsk også ramt af genvejsvirus på kontrolsystemer*"; http://www.version2.dk/artikel/15663-viruskrig-paa-to-fronter-maersk-ogsaa-ramt-af-genvejsvirus-paa-kontrolsystemer

Wikipedia.org , 2010; "*Stuxnet*"; http://en.wikipedia.org/wiki/Stuxnet

Kontakt:

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

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