DK•CERT

Trendrapport

It-sikkerhed i tredje kvartal 2012

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad og 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 informationssikkerhed ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DK•CERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DK•CERT bygger på en vision om at skabe samfundsmæssig værdi i form af øget informationssikkerhed. Det sker gennem offentliggørelse af viden om it-sikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen, samt internationale samarbejdspartnere.

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

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

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

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

Indholdsfortegnelse

1. Resume

"Så konklusionen er klar: Web-applikationer er sikkerhedsmæssigt et ømt punkt."

Den er helt gal med sikkerheden i web-applikationer. Det fremgår af DK•CERTs trendrapport for tredje kvartal. Når en organisation åbner sig for omverdenen via et websted, åbner den ofte også en ladeport, som hackere kan gå ind af.

Det blev illustreret af et hackerangreb på 100 universiteter i USA og resten af verden. Her brugte hackere helt simple angrebsmetoder til at få adgang til fortrolig information fra universiteternes databaser. De anvendte SQL-injection, hvor hackeren indtaster kommandoer i fx et søgefelt på en webside. Hvis systemet er sårbart, bliver kommandoerne udført af den database, som leverer indhold til websiden.

På verdensplan blev der fundet 85 procent flere nye sårbarheder end i det foregående kvartal. Og næsten hver tredje af dem lå i web-applikationer.

Ved DK•CERTs sårbarhedsscanninger på Forskningsnettet fandt vi 1.000 alvorlige sårbarheder. Tre ud af fire sårbarheder lå i web-applikationer og anden web-software.

Så konklusionen er klar: Web-applikationer er sikkerhedsmæssigt et ømt punkt. Heldigvis er det ikke vanskeligt at rette SQL-injectionsårbarheder. Så her er et oplagt indsatsområde for udviklere og webansvarlige.

Men ikke kun applikationerne på websteder er sårbare. Kvartalet bragte også to alvorlige sårbarheder i de programmer, brugerne anvender: Oracles Java og Microsofts Internet Explorer. Begge sårbarheder blev kendt, før der var udsendt rettelser til dem. Java-hullet blev endda udnyttet bredt, mens hullet i Internet Explorer foreløbig kun er set anvendt i begrænsede angreb.

V kan glæde os over, at de meget alvorlige sikkerhedshuller forholdsvis hurtigt blev lukket af leverandørerne.

Ud over statistikker over sikkerhedshændelser fra det forgangne kvartal indeholder trendrapporten også referat af de væsentligste nyheder inden for it-sikkerhed. Foruden historien om universitetshacking er det blandt andet konflikten på Restaurant Vejlegaarden, der fik en it-vinkel, samt et afværget angreb på NemID.

I forhold til tidligere trendrapporter har vi denne gang fokuseret mere på at perspektivere og videregive DK•CERTs holdning til hver enkelt nyhed.

God fornøjelse med læsningen!

Shehzad Ahmad

Chef for DK•CERT

2. Tredje kvartal 2012 i tal

I tredje kvartal måtte vi to gange advare mod sårbarheder, der blev udnyttet, inden de var offentliggjort og inden der var udgivet rettelser til dem. I august var det en sårbarhed i Java, som er nødvendig for at kunne benytte NemID. I september var det en sårbarhed i Internet Explorer, der i juli blev benyttet af cirka halvdelen af den danske befolkning. Den slags trusler kan være kritiske, da de selvsagt kan være vanskelige at gardere sig imod.

Det er ikke første gang, sårbarheder i Java er i søgelyset. De har nemlig vist sig at være de hyppigst udnyttede til drive-by-download af malware. Det viste blandt andet en side med statistik fra et exploit kit, som blev benyttet til spredning af politi-ransomwaren Reveton. I næsten 64 procent af tilfældene var det sårbarheder i Java, som førte til inficering af brugernes computere.

I begge tilfælde var producenterne hurtige til at komme med rettelser uden om den normale opdateringscyklus. Alligevel kan man være skeptisk over for, hvor mange der rettidigt fik opdateret programmerne, da det krævede en aktiv handling fra brugerne.

Et problem med den type sårbarheder er, at de internet-kriminelle hurtigt inkluderer udnyttelse af sårbarheder i de exploit kits, der i dag udgør en stigende risiko. Så snart der kommer et angrebsprogram (exploit) til en endnu ikke rettet sårbarhed, udgør det en væsentlig trussel. Det sætter softwareproducenterne under pres. Når sikkerhedsorganisationer og myndigheder advarer mod brugen af et specifikt stykke software, risikerer producenten, at kunderne bliver så glade for alternativerne, at de mister markedsandele.

I dette afsnit giver vi en status på informationssikkerheden i tredje kvartal 2012. Vi tager udgangspunkt i data opsamlet fra vores egne systemer, suppleret og perspektiveret med data fra internettets åbne kilder.

Vi starter med at sætte fokus på de sikkerhedshændelser, der i løbet af kvartalet blev rapporteret til DK•CERT. Hændelser, der primært tager udgangspunkt i de systemer og netværk, DK•CERT har adgang til. Det vil sige det danske net til forsknings- og uddannelsesinstitutioner, Forskningsnettet, samt de hændelser, der rapporteres til os vedrørende den øvrige del af det danske internet.

Herefter sætter vi spot på udvikling og spredning af malware, der er den største trussel mod borgernes og organisationernes sikkerhed. Da malware ikke kan betragtes som et isoleret fænomen, beskriver vi også udviklingen med hensyn til de afledte hændelser som spam og phishing. De indgår i den samme kriminelle værdikæde.

Vi slutter afsnittet med en beskrivelse af kvartalets væsentligste sårbarheder. Det vil her sige kvartalets nye sårbarheder, de sårbarheder vi så forsøgt udnyttet, samt de sårbarheder vi fandt ved scanning af vores kunders systemer. Det er nemlig ofte sårbarheder, der gør det muligt at kompromittere systemer.

”Alligevel kan man være skeptisk over for, hvor mange der fik opdateret rettidigt, da det krævede en aktiv handling fra brugerne.”

Foreningen af Danske Interaktive Medier (FDIM); “*Browserbarometer*”.
KrebsonSecurity, 2012; “*Inside a ‘reveton’ ransomware operation*”.

2.1. Kvartalets sikkerhedshændelser

Tredje kvartal var præget af, at forårets og sommerens store sportsbegivenheder var overstået. På mange måder var vi tilbage ved normale tilstande. Således modtog vi 4.600 rapporter om sikkerhedshændelser, der førte til registrering af 3.432 unikke sikkerhedshændelser (Figur 1). Det er et fald på 15 procent i forhold til de 4.049 hændelser, vi registrerede i andet kvartal, men en stigning i forhold til årets første kvartal. De registrerede hændelser udsprang af 1.829 forskellige IP-adresser. Det vil sige, at samme IP-adresse i gennemsnit er blevet registreret ved to efterfølgende hændelser.

De fleste sikkerhedshændelser var i tredje kvartal af typen piratkopiering. Dem registrerede vi 680 af (Figur 2). Ved tredje kvartals hændelser om pirat-download af film, musik og software var det 239 forskellige IP-adresser på det danske Forskningsnet, der var årsag til hændelsen. Generelt er antallet af hændelser, hvor repræsentanter for rettighedshaverne gør opmærksom på uretmæssige download af kopibeskyttede værker, faldet i løbet af 2012. Antallet steg dog igen i september måned.

Herefter fulgte hændelser kategoriseret som portscanninger, brute force-angreb og malware hosting. Dem registrerede vi henholdsvis 539, 529 og 510 af. Hvor portscanning og malware hosting er i vækst, har der været et fald i forsøg på at logge på en tjeneste ved systematisk afprøvning af kombinationer af brugernavne og password.

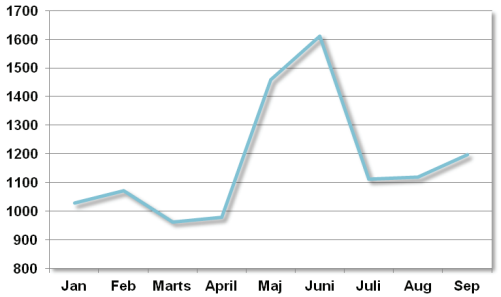
Hvor brute force-angreb set over hele 2012 er ansvarlig for en fjerdedel af de registrerede hændelser, var det i tredje kvartal kun cirka 15 procent. Ved 471 forsøg på brute force-angreb var det udenlandske computere, der forsøgte at logge på SSH-tjenester placeret på danske universiteter. Ved de øvrige hændelser var det danske computere, der forsøgte at logge på tjenester i udlandet. Det drejede sig her primært om SSH- og mailtjenester.

Set over hele året kan vi konstatere, at tilfælde hvor DK•CERT blev gjort opmærksom på danske computere, som deltager i botnet-relateret trafik er stigende. I tredje kvartal registrerede vi 222 hændelser af denne type mod 200 i kvartalet inden og kun 40 tilfælde i årets første tre måneder. Alle henvendelser kom fra udlandet, hvor der i enkelte tilfælde var skaffet adgang til botnettets centrale command & control-servere. Selvom botnet i medierne ikke længere har den store fokus, er de således stadig et problem. Brugen af botnet indgår nemlig i megen internetkriminalitet.

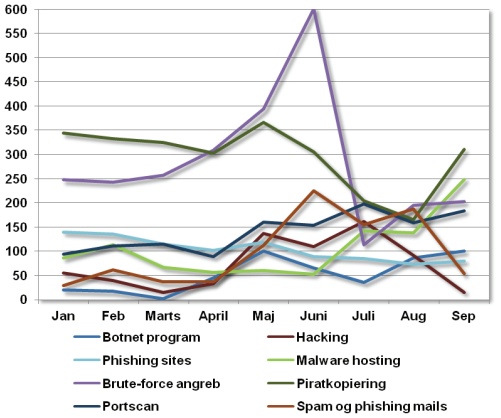
I 269 tilfælde registrerede vi en hændelse som hacking. Det vil sige kompromittering af systemer og/eller informationer. Det kan i nogle tilfælde også dække over defacements eller maskiner inficeret med malware eller phishing, da det ud fra den modtagne information kan være vanskeligt entydigt at kategorisere hændelsen. 162 tilfælde blev i juli måned registreret som hacking, mens antallet siden da har været relativt beskedent. Set over hele kvartalet er antallet af hændelser af denne type faldet i forhold til 400 registreringer i andet kvartal.

2.2. Malware og andre trusler

Offentliggørelser af fortrolige data som angiveligt var fremskaffet ved traditionel hacking, har de seneste år oplevet massiv medieomtale. På trods af det udgør malware den største trussel mod danske organisationer og borgere. I kombination



Figur 1. Sikkerhedshændelser registreret af DK•CERT i 2012.



Figur 2. Væsentligste sikkerhedshændelser registreret af DK•CERT i 2012.

med stadig mere udspekuleret social engineering målrettes malware til at skaffe adgang til data, der i en eller anden grad kan omsættes til penge. På lige fod med avancerede exploit kits handles kreditkortinformationer og adgang til e-mailkonti eller botnet-inficerede maskiner i den kriminelle undergrund. Her har udviklingen ikke stået stille.

Den væsentligste kilde til kompromittering af computere er gennem browseren. Sårbarheder i browseren og de tilknyttede programmer var ifølge Kaspersky Lab ansvarlig for 80 procent af kompromitteringerne i første halvår af 2012. Som middel til at inficere vores computere benyttes en række metoder, der oftest handler om at inficere legale websider. De bliver efterfølgende promoveret ved søgemaskineoptimering, URL-forkortelser i traditionel spam, samt spam på sociale medier som Facebook og Twitter.

Et væsentligt element er her udbredelsen af de såkaldte exploit kits, der har tilføjet et ekstra lag i den internet-kriminelle værdikæde. Et exploit kit er en samling programmer, der afprøver angreb på en række kendte sårbarheder hos de browsere, der besøger det inficerede websted. Exploit kits er professionelle softwareprodukter, der ofte giver brugerne mulighed for versionsopdatering, tilkøb af nye moduler rettet mod specifikke sårbarheder, adgang til botnetinfrastruktur, statistik moduler og lignende.

Udnyttelse af flere sårbarheder samlet i et exploit kit gør det nemt og hurtigt at distribuere malware. Derfor har de gennem det seneste år opnået en stigende udbredelse. Ifølge Sophos der producerer sikkerhedssoftware, var exploit kittet Blackhole i perioden oktober 2011 til maj 2012 således ansvarlig for 28 procent af alle webrelaterede trusler. Det tal forventes at være steget siden.

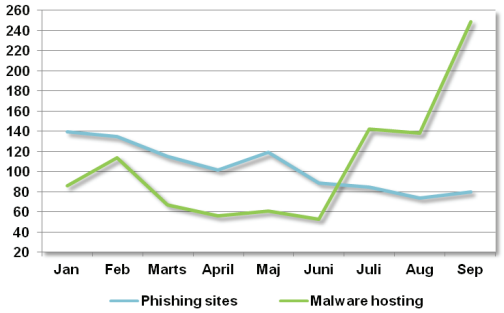
Blackhole udvikles i Rusland og sælges for under 12.000 danske kroner. Exploit kittet placeres på et kompromitteret website, og forsøger herefter at udnytte en række sårbarheder i den besøgendes operativsystem, browser, plug-ins og add-ons. Er maskinen sårbar, bliver den inficeret med malware. Blackhole indeholder også et modul til statistik over benyttede exploits, udnyttede browsere, operativsystemer med mere.

Måske på grund af brugen af exploit kits er mængden af de sikkerhedshændelser, vi registrerede som hosting af malware, steget voldsomt siden juni måned. Her registrerede vi 53 hændelser, der blev kategoriseret som malware hosting. I september måned var det tal næsten fem gange så højt, eller i alt 249 (Figur 3). I august måned blokerede Symantec dagligt næsten 1.100 malware-inficerede websites.

Selvom vi i august og september måned havde en oplevelse af, at der var mange dansksprogede phishingmails, der ramte indbakken, afspejler det sig ikke i antallet af hændelser om phishing-sider placeret på danske websites. Det på trods af, at de fleste mails var udført med brug af original grafik og på et forståeligt dansk.

Gennem hele 2012 har vi registreret et faldende antal aktive phishing-sider, som blev hostet på danske webservere. I tredje kvartal registrerede vi således kun 239 hændelser, der blev kategoriseret som phishing-sider mod 310 i andet kvartal. Det kan skyldes, at phishing-sider ofte kun er aktive i ganske få timer, og angrebene i stigende grad er målrettet specifikke organisationer og dens ansatte. Herved mindskes muligheden for at siden opdages og/eller rapporteres til os.

Blandt kvartalets øvrige tendenser er en fortsat stigning i Android-relaterede trusler. Det skyldes, at brugen af mobiltelefoner og mængden af data vi lagrer på dem,



Figur 3: Danske websites inficeret med malware eller phishing-sider registreret af DK•CERT i 2012.

er stigende. Når det hovedsagelig er Android, der er i skudlinjen, skyldes det, at det er lettere at få skadelige applikationer ind på Google Play, end det er på for eksempel Apples App Store, hvor der er mere kontrol.

Tidligere på året blev den trojanske hest Android.Opfake skjult i en kopi af et legitimt spil, der skulle promovere de olympiske lege. Når den trojanske hest var blevet installeret, fik den telefonen til at sende overtakserede SMS'er. På samme vis er malware igennem kvartalet blevet forsøgt skjult i alt fra spil og browsere til falske antivirusprodukter for herefter at blive spredt gennem Google Play.

Som på computeren forsøges mobil malware også spredt ved drive-by-download. Ved besøg på et inficeret websted hentes malware, der efterfølgende skal installeres af brugeren. Ved for eksempel at navngive filen Android System Update 4.0.apk kan bagmændene narre nogle til at installere "opdateringen," selv om det foregår uden om den normale opdateringsprocedure.

I tredje kvartal identificerede antivirusproducenten F-Secure 2.158 malwareinfektioner hos deres danske kunder. Selvom andelen af trojanske heste er faldet fra 45,3 procent i andet kvartal, udgør de stadig den største andel af inficeringerne (Figur 4). Ifølge Kaspersky Lab indeholder 46 procent af de trojanske heste funktioner til at hente og skjule andre programmer, mens 21 procent fungerer som datatyve.

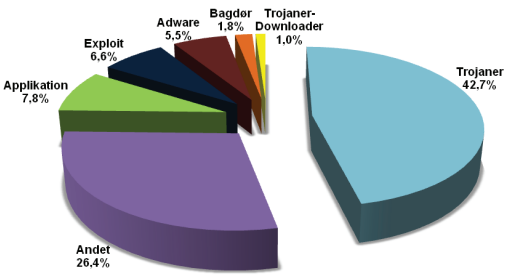
Også for de typer malware, der ikke entydigt kan kategoriseres, er der sket et fald. De udgør nu 26,4 procent mod 28,7 procent i andet kvartal. Derimod er andelen af skadelig kode, der er kategoriseret som exploits, steget fra 2,4 procent i andet kvartal til 6,6 procent i tredje kvartal. Det formodes, at de primært relaterer sig til websites, der har været kompromitteret med exploit kits.

De fleste malware-typer udgør i tredje kvartal en mindre andel end tidligere. Således udgør de syv hyppigst identificerede malware-typer herhjemme i tredje kvartal kun cirka 93 procent af al identificeret malware. Det afspejler en stadig større differentiering og specialisering af funktionaliteten og måske også, at mængden af ny malware er stigende. Som tidligere er det i dag kun en marginal del af den malware, der findes på danskernes computere, som kan sprede sig selv.

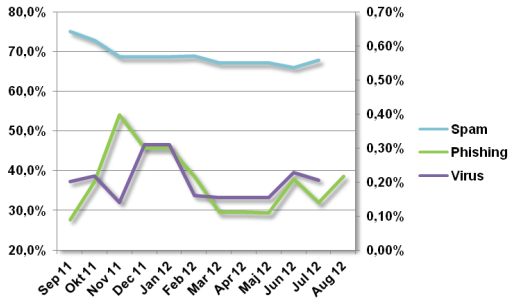
Selvom der stadig er folk, der falder for de samme teknikker som tidligere, er der sket en udvikling. Angrebene er i dag mere kreative og sofistikerede. Et eksempel på det er de mails, der gennem de seneste måneder har ramt vores indbakker med beskeden om, at vores kreditkort har været brugt til køb af børneporno. Modtageren skal derfor verificere sine kort-informationer, hvis ikke kortet skal spærres. I samme boldgade er ransomware, der låser brugerens computer, indtil der er betalt en bøde. Her er det ofte en politimyndighed, der står som afsender. Forseelsen er angiveligt, at computeren har været brugt til download af børneporno og kopibeskyttet materiale. Den type malware blev i juli måned også målrettet danskerne.

Traditionelt set er sommeren præget af stor spam-aktivitet. Den topper i august for herefter at falde i september. Tilsvarende indeholder en større andel af de uønskede mails skadelig kode i august. Forventning til en mere stille september ligger derfor lige for.

Gennem hele 2012 har vi oplevet, at en faldende andel mails sendt til danskerne var spam. Det følger de globale tendenser. 67,7 procent af de mails der blev sendt til danskerne i juli, var spam, hvilket svarer til den globale andel af spam, som i samme måned var 67,6 procent (Figur 5). Over halvdelen af dem var afsendt fra et .com-domæne.



Figur 4. Danske malware-infektioner identificeret af F-Secure i tredje kvartal 2012.



Figur 5. Danske e-mail-trusler registreret af Symantec det seneste år.

Erotiske sider og dating samt medicin udgjorde ifølge Symantec 75 procent af de tjenester og produkter, som august måneds spammail på globalt plan reklamerede for. De udgjorde henholdsvis 42,5 og 32,6 procent af alle spam-mails. 6,9 procent af de uønskede mails omhandlede tilbud om et job. Hvorvidt der var tale om reelle jobs, job som muldyr eller forsøg på phishing er ikke klart.

Generelt ligger Danmark under det globale niveau for mængden af phishing- og virus-mails. Det stemmer overens med data fra Kaspersky Lab, der fortæller, at vi er det land i den vestlige verden, som er mindst udsat for angreb. Således bliver under 20 procent af danskerne udsat fra angreb mod over 40 procent i Italien og Spanien.

Mængden af phishing- og virus-mails, der i juli ramte danskernes indbakke, var ifølge Symantec henholdsvis 0,14 og 0,21 procent. Det er under de globale gennemsnit, som i juli var på henholdsvis 0,32 og 0,43 procent. Andelen af phishing-mails herhjemme steg dog i august til at udgøre 0,22 procent, eller 1 ud af 464 mails (Figur 5).

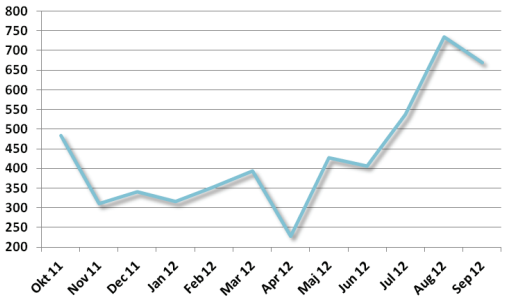
F-secure, 2012; "*F-Secure security lab– virusworld map*".
F-secure, 2012; "*Threat report H1 2012*".
GFI Labs, 2012; "*Fraudsters use legit AV brands to mask Boxer*".
Kaspersky Lab, 2012; "*Spam in August 2012*".
Kaspersky Lab, 2012; "*The geography of cybercrime: Western Europe and North America*".
McAfee, 2012; "*McAfee threats report: Second quarter 2012*".
Privacy PC, 2012; "*Where are we and where are we going 3: Ransom trojans*".
Symantec; "*Intelligence reports*".
SearchSecurity , 2012; "*FireEye warns of steady increase in advanced malware*".
Sophos, 2012; "*Exploring the Blackhole Exploit Kit*".

2.3. Tredje kvartals sårbarheder

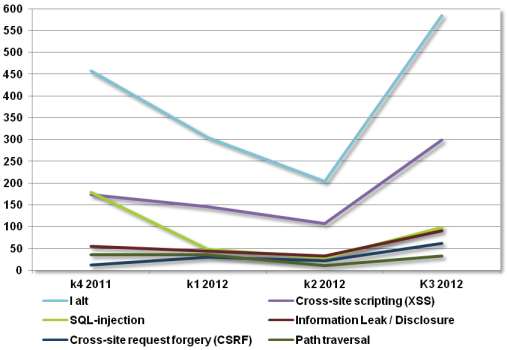
Stigende automatiseret udnyttelse af sårbarheder har sat fokus på organisationernes løbende risikovurderinger og procedurer for opdateringer. Sårbare applikationer er stadig den væsentligste årsag til kompromittering af systemer og data. Blandt andet udbredelse og brug af exploit kits gør, at sårbarhederne i dag udnyttes tidligere. Det illustrerer et par eksempler fra tredje kvartal, hvor sårbarheder blev udnyttet, inden de var offentliggjort og inden der var frigivet en rettelse.

I tredje kvartal blev der offentliggjort 1.942 nye CVE-nummererede sårbarheder (Figur 6). Det er en stigning på næsten 85 procent i forhold til kvartalet inden. Af dem udgjorde 585 eller næsten en tredjedel sårbarheder i webapplikationer (Figur 7). Det er sårbarheder, der gør det muligt at placere skadelig kode eller phishing-sider på legale websites. Stigningen i antallet af den type sårbarheder skyldes flere offentliggørelser af alle typer websårbarheder. Antallet af nye crosss-site-scripting-sårbarheder er næsten tre gange større end i kvartalet inden.

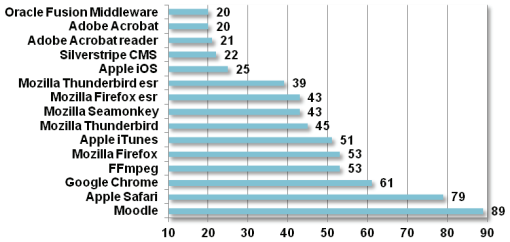
I modsætning til tidligere, udgør nye sårbarheder i open source software i tredje kvartal en væsentlig andel. Således toppes listen over produkter med flest nye CVE sårbarheder af Moodle, der er et gratis system til webbaseret læring (Figur 8). På fjerde pladsen er FFmpeg, der håndterer multimedie data, mens nummer 12 udgøres af Silverstripe CMS (Content Management System). Hvorvidt det er tilfældigt eller et udtryk for professionalisering af open source leverandørerne, der ser sikkerhed som en nødvendighed for at fastholde og erobre markedsandele er uvist.



Figur 6. CVE-nummererede sårbarheder offentliggjort af NIST.



Figur 7. CVE-nummererede websårbarheder offentliggjort af NIST.



Figur 8. CVE-nummererede produktsårbarheder offentliggjort i tredje kvartal 2012.

Derudover er det produkter fra de store softwareleverandører som Apple, Google, Mozilla og Adobe der topper listen. En stor markedsandel giver producenten flere ressourcer, men vil også gøre produktet mere interessant for dem, som ønsker at udnytte det. Derfor er det browsere og programmer der kan fungerer som plugins til dem, der normalt topper listen. De er i dag den væsentligste angrebsvektor. Generelt var der denne gang offentliggjort relativt mange sårbarheder i de mest sårbare programmer.

Man kan ikke umiddelbart udlede en applikations sikkerhedsstatus fra antallet af nye sårbarheder der offentliggøres. Ud over hvilke versioner sårbarhederne offentliggøres i afhænger det af faktorer som blandt andet tilgængeligheden af exploits, der udnytter sårbarhederne og sårbarhedernes potentielle kompromitteringsgrad. Derudover har den lokale implementering af applikationen også en betydning. Generelt kan man dog sige, at risikoen for at en applikation forsøges udnyttet, stiger med dens udbredelse og graden af eksponering mod internettet.

Derudover gælder at sårbarheder i for eksempel Mozillas og Googles produkter går igen på tværs af versioner. Sårbarheder i Mozillas standardversioner er således de samme som i ESR versionerne (Extended Support Release), der er rettet mod organisationer, der kræver support i implementering og drift. Det samme gælder for Google Chrome, der i løbet af tredje kvartal er kommet i to nye versioner. Flere sårbarheder er her knyttet til versioner, som ikke længere er i brug.

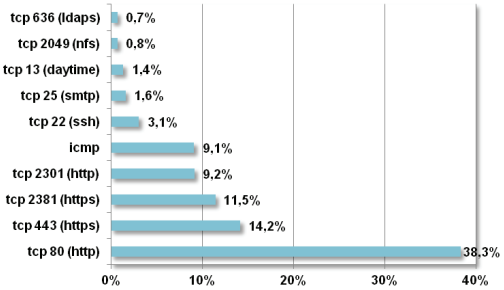
DK•CERT udførte i tredje kvartal 22 sårbarhedsscanninger af i alt 29.111 forskellige IP-adresser på Forskningsnettet, der er det danske net til forskning og uddannelse. 956 IP-adresser var på scanningstidspunktet tilgængelige fra internettet, og 501 af dem havde en eller flere CVE-nummererede sårbarheder. I alt konstaterede vi 4.791 sårbarheder, hvoraf 1.000 blev risikovurderet som værende alvorlige. På 1,7 procent af de scannede maskiner var der således i gennemsnit 9,6 sårbarheder, hvoraf 2 udgjorde en høj risiko.

De fundne sårbarheder var fordelt på 60 forskellige porte og/eller protokoller, hvoraf de fleste var tilknyttet webapplikationer (Figur 9). Således udgjorde sårbarheder i applikationer, der lyttede på TCP-port 80, 433, 2301 og 2381 i alt 73,5 procent af sårbarhederne. TCP-port 2381 og 2301 benyttes til management software fra HP. Forespørgsler på port 2301 sender brugeren videre til port 2381, hvor forbindelsen er krypteret.

De øvrige sårbarheder var i blandt andet mailtjenester (TCP-port 25 og 993), netværksmanagementprotokollen SNMP (TCP-port 161), fjernskrivebord (TCP-port 3389), administration af Apple AirPort (TCP-port 5009) og DNS (UDP-port 53).

Juli-opdateringerne fra Microsoft indeholdt ni rettelser, der fjernede i alt 16 sårbarheder i blandt andet Visual Basic for Applications, Windows, SharePoint og Office for Mac. Mest kritiske var sårbarheder i Microsoft XML Core Services (CVE-2012-1889), Internet Explorer (CVE-2012-1522 og CVE-2012-1524) og Microsoft Data Access Components (CVE-2012-1891). De tillader alle ekstern afvikling af kode.

De kvartalsvise opdateringer fra Oracle den 17. juli rettede i alt 87 sårbarheder i blandt andet Oracle Database, Fusion Middleware, Enterprise Manager og Sun-produkterne. Flere sårbarheder i Fusion Middleware giver mulighed for ekstern afvikling af kode og findes gennem komponenten Outside In. Den benyttes til at konvertere mellem filformater og anvendes også af programmer fra andre producenter, som derfor også er sårbare. Blandt de berørte produkter er Microsofts Exchange og FAST Search Server 2010 for SharePoint.



Figur 9. CVE-nummererede sårbarheder konstateret ved scanning i tredje kvartal 2012.

Mozilla udsendte også deres opdateringer den 17. juli. De indeholdt 15 rettelser til 19 forskellige sårbarheder i Firefox, Thunderbird og Seamonkey. Fem opdateringer blev vurderet som kritiske og rettede i alt ni sårbarheder (CVE-2012-1948, CVE-2012-1949, CVE-2012-1951 - CVE-2012-1954, CVE-2012-1959, CVE-2012-1962 og CVE-2012-1967). Flere af disse giver mulighed for ekstern afvikling af kode.

Apple udsendte den 25. juli version 6 af browseren Safari til Mac OS X. Den lukkede mere end 120 sikkerhedshuller, hvoraf de fleste var i det tilknyttede browserbibliotek WebKit. Der blev ikke samtidig udsendt en ny version af Safari til Windows, som derfor sandsynligvis stadig er sårbar.

Med Googles frigivelse af Chrome 21 den 31. juli blev der rettet i alt 15 sårbarheder. En sårbarhed (CVE-2012-2859), som kun var tilgængelig i Linux-versionen, blev vurderet som kritisk. Seks sårbarheder, hvoraf flere vedrørte visning af PDF-filer, fik Googles næsthøjeste risikovurdering.

Den 14. august udsendte Microsoft deres månedlige opdateringer, der fjernede i alt 26 sårbarheder. Opdateringer til Windows Common Controls (MS12-060), Internet Explorer (MS12-052), Remote Administration Protocol (MS12-054) og Remote Desktop Protocol under Windows XP (MS12-053) blev vurderet som kritiske og rettede i alt ni sårbarheder. Derudover rettede en kritisk opdatering (MS12-058) 13 sårbarheder i Exchange Server 2007 og 2010, der vedrører brugen af Oracles Outside In-produkt.

Adobe udgav den 21. august en opdatering (APSB12-19), der lukkede syv sårbarheder i Flash Player til alle platforme. Sårbarhederne (CVE-2012-4163 – 68 og CVE-2012-4171), hvoraf fem har højeste risikovurdering, kan udnyttes til at få det berørte system til at gå ned og potentielt eksekvering af kode.

Udsendelse af Firefox 15 den 29. august indeholdt 17 opdateringer, som rettede i alt 33 sårbarheder i den tidligere version. Syv rettelser vurderes som kritiske og giver blandt andet mulighed for eksekvering af kode på det sårbare system. Med opdateringen rettes samtidig fejl i Thunderbird og Seamonkey.

I slutningen af august kunne man på flere blogs læse om en endnu ikke offentliggjort sårbarhed i Java, som blev udnyttet i mindre angreb. Den 28. august blev der observeret større angreb og det blev konstateret, at sårbarheden (CVE-2012-4681) nu indgik i exploit kittet BlackHole. Derfor anbefalede blandt andre vi, at man deaktiverede Java. Sårbarheden, der er risikovurderet som kritisk, kan udnyttes til afvikling af kode på det sårbare system. Den 30. august udsendte Oracle ekstraordinært Java version 7 update 7. Den rettede fire sårbarheder, heriblandt CVE-2012-4681. Siden kom det frem, at også den opdaterede version indeholdt en sårbarhed, der dog ikke var set udnyttet.

En opdatering af Chrome version 21 rettede den 30. august otte sårbarheder. Tre af sårbarhederne (CVE-2012-2866, CVE-2012-2869 og CVE-2012-2871) fik Googles næsthøjeste risikovurdering. Flere af sårbarhederne gav en kontant dusør på 500 eller 1.000 dollars til de sikkerhedsforskere, der opdagede og rapporterede dem.

Den 6. september udsendte Apple en sikkerhedsrettelse til Mac OS X. Den fjernede en kritisk sårbarhed i Java. Sårbarheden (CVE-2012-4681) var den samme, som en uge tidligere var blevet opdateret til de øvrige platforme af Oracle.

En lille uge senere udsendte Apple den 12. august iTunes 10.7 til Windows 7, Vista, XP SP2 og senere Windows versioner. Den lukker 163 sårbarheder i programmets indbyggede browserkomponent, WebKit. Sårbarhederne kan medføre nedbrud af

iTunes eller afvikling af skadelig kode.

Den 16. september offentliggjorde sikkerhedsforskeren Eric Romang fundet af et angrebsprogram, der udnyttede en hidtil ukendt sårbarhed i Internet Explorer 6, 7, 8 og 9. Programmet blev fundet på en server, der blev benyttet af samme bande, som cirka tre uger tidligere havde udnyttet en sårbarhed i Java. Programmet udnyttede sårbarheden gennem en Flash-fil indlejret på en HTML-side og medførte installation af programmer på den sårbare maskine.

Dagen efter udsendte Microsoft en advarsel om sårbarheden (CVE-2012-4969), der blev vurderet som kritisk. Derfor advarede den tyske regering og en række sikkerhedsorganisationer mod brugen af Internet Explorer, da man forventede angreb, der udnyttede sårbarheden. Senere kom Microsoft den 19. september med en midlertidig løsning på problemet i form af programmet Fix It. Den 21. september udsendte de en endelig opdatering af Internet Explorer, der rettede sårbarheden.

To dage før salget af iPhone 5 startede den 21. september, udsendte Apple telefonens styresystem iOS 6. Den nye version af iOS fjerner mere end 100 sårbarheder, hvoraf hovedparten findes i browserkomponenten WebKit. Samtidig udsendtes en ny version af browseren Safari, samt en række sikkerhedsrettelser til Mac OS X. Safari version 6.01 opdaterer i alt 60 sårbarheder. Også her er de fleste i browserkomponenten WebKit. Sikkerhedsopdateringerne til Mac OS X opdaterer 26 sårbarheder. 15 sårbarheder er i tredjepartssoftware som Apache, BIND og PHP.

Den 21. september udgav ERP-producenten (Enterprise Ressource Planner) SAP en kritisk opdatering, som rettede i alt 27 sårbarheder. De to mest kritiske sårbarheder gav mulighed for afvikling af kode gennem RFC (Remote Function Call), mens ni sårbarheder var af typen cross-site scripting.

Adobe, 2012; "*Security updates available for Adobe Flash Player*".
Apple, 2012; "*About the security content of iTunes 10.7*".
Apple, 2012; "*About the security content of Java for OS X 2012-005 and Java for Mac OS X 10.6 Update 10*".
Apple, 2012; "*About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004*".
Apple, 2012; "*About the security content of Safari 6*".
Apple, 2012; "*APPLE-SA-2012-09-19-1 iOS 6*".
Apple, 2012; "*APPLE-SA-2012-09-19-3 Safari 6.0.1*".
Cnet, 2012; "*German government tells public to stop using Internet Explorer*".
DK•CERT; "*DK•CERT Sårbarhedsdatabase*".
Eric Romang, 2012; "*Zero-Day season is really not over yet*".
Erpscan, 2012; "*SAP critical patch update September 2012*".
FireEye, 2012; "*Java zero-day - first outbreak*".
FireEye, 2012; "*Zero-day season is not over yet*".
Google, 2012; "*Stable channel release*".
Microsoft, 2012; "*Microsoft security advisory (2757760)*".
Microsoft, 2012; "*Microsoft security bulletin summary for August 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for July 2012*".
Microsoft, 2012; "*More information on security advisory 2757760's Fix It*".
Microsoft, 2012; "*MS12-063: Cumulative security update for Internet Explorer: September 21, 2012*".
Mozilla, 2012; "*Mozilla Foundation security advisories*".
Mozilla, 2012; "*Security advisories for Firefox*".
National Institute of Standards and technology (NIST); "*CVE and CCE statistics query page*".
Oracle, 2012; "*Oracle critical patch update advisory - July 2012*".
Oracle, 2012; "*Oracle security alert for CVE-2012-4681*".
Seclists, 2012; "*[SE-2012-01] New security issue affecting Java SE 7 Update 7*".
Websense, 2012; "*New Java 0-day added to Blackhole Exploit Kit*".

3. Overskrifter fra tredje kvartal 2012

"Udbredelse af informationsteknologi har nemlig også en bagside."

I Danmark har vi taget informationsteknologien til os. Tal fra Danmarks Statistik viste, at i juli havde henholdsvis 97 og 92 procent af danskerne mellem 16 og 74 år inden for de seneste tre måneder benyttet mobiltelefon og internet. 55 procent af dem, der havde benyttet mobiltelefon, brugte den til også at gå på internettet.

Den udvikling har øget bankernes, erhvervslivets og det offentliges muligheder for udviklingen af digitale selvbetjeningsplatforme. I dag foretages ansøgninger om lån, indkøb og tilmelding til daginstitutioner eller skole digitalt fra vores eget hjem. Det har øget effektiviteten og fleksibiliteten i vores samfund, men samtidig introduceret nogle problematikker, som for kun 10 år siden var stort set ukendte. Hvor informationsteknologien på mange måder har gjort vores dagligdag mere enkel, er verden nemlig samtidig blevet mere sammenhængende og kompleks.

Hvordan skal man for eksempel som borger forholde sig til ikke at kunne indberette ledighed til sin a-kasse, fordi dens hjemmeside er sat ud af drift af folk, som er uenige med dens måde at agere på? Når østeuropæiske hackere stjæler penge fra ens bankkonto, blot fordi man benyttede netbank? Eller når maskinen låser og en besked på skærmen fortæller, at man skal betale 100 euro for at få den låst op?

Udbredelse af informationsteknologi har nemlig også en bagside. For eksempel er Danmark nummer to på sikkerhedsvirksomheden Incapsulas liste over kilder til angreb på webservere i forhold til antallet af indbyggere. Det betyder ikke, at det er danskere, som står bag angrebene, men sandsynligvis blot, at vi gennemsnitligt har flere internetopkoblede enheder til rådighed, og at vi ikke er bedre til at beskytte dem end folk i andre lande. De fleste af denne type angreb foretages nemlig fra malware-inficerede enheder, som måske er blevet inficeret, fordi man benytter en sårbar browser.

Ovenstående skitserer nogle af de problemstillinger, vi som borgere og samfund står over for. Problemstillinger som ikke er ukendte i erhvervslivet. For eksempel opfatter 17 procent af organisationerne ifølge Danmarks Statistik sikkerhed som en barriere for brug af mobilt internet til arbejdsbrug. Ud over selv at være mål for it-kriminalitet er organisationerne nemlig en del af både problemet og dets løsning. Den stigende digitalisering af vores aktiver øger vores sårbarhed for, at data kommer i de forkerte hænder.

Blandt andet derfor har EU-kommissionen udfærdiget et forslag til revision af databeskyttelsesdirektivet, som ventes til førstebehandling til februar. Ud over at stille større krav til organisationernes behandling af forbrugerdata skal det blandt andet sikre, at forbrugerdata ikke kan kompromitteres, uden at forbrugeren informeres rettidigt.

Tilsammen er dette afsnits fortællinger med til at illustrere, hvordan digitaliseringen af samfundet samtidig medfører nye digitale problemstillinger og risici. Mens nogle kan løses teknisk eller gennem ændret lovgivning og kontrol, vil andre kræve mere åbenhed og stigende information. Det er nemlig i fællesskabet, vi skal forstå og forme vores digitale fremtid. Også når det gælder informationssikkerhed.

Danmarks Statistik, 2012; "*It-anvendelse i befolkningen 2012*".
Danmarks Statistik, 2012; "*It-anvendelse i virksomheder 2012*".
Incapsula, 2012; "*Top security threats and attackers by country*".

3.1. Hacktivisme i skyggen af Restaurant Vejlegården

Efter at fagforeningen 3F i flere måneder havde blokeret Restaurant Vejlegården, blev dens hjemmeside den 19. juli udsat for et Denial of Service-angreb. Angrebet gjorde hjemmesiden utilgængelig og berørte fagforeningens dagpengemodtagere. Det illustrerer en tendens mod større global opbakning til lokale aktioner under signaturen Anonymous.

Baggrunden for angrebet var, at restauranten havde tegnet en overenskomst med Kristelig Fagforening, som 3F mener forringer de ansattes arbejdsforhold. Måneder efter konfliktens begyndelse ramte historien de landsdækkende medier. Herefter tog begivenhederne fart. Politikere valfartede til restauranten for at tilkendegive deres sympatier, og ethvert villigt interviewoffer havde deres egne holdninger og sympatier i forhold til de stridende parter.

Den 19. juli blev 3F's hjemmeside udsat for et Denial of Service-angreb, der gjorde den utilgængelig i flere dage. Angiveligt deltog folk fra blandt andet USA, Mexico, Brasilien, Spanien, Tyskland, Portugal og Australien i angrebet, som i første omgang blev proklameret af Twitter-brugeren Elan0r. Angrebene ramte siden både LO og HK's hjemmesider og berørte cirka 30.000 dagpengemodtageres mulighed for indberetning af ledighed med forsinket udbetaling af dagpenge som følge.

Til TV 2 fortalte en anonym hacker, at angrebet var løbet af sporet, fordi mange deltagere ikke var "rigtige" Anonymous. Senere belærte en video på YouTube os om, at det slet ikke var de "rigtige" Anonymous, der stod bag angrebet. Også denne video var signeret Anonymous og kaldte deltagerne i angrebet for forrædere.

Hvordan man i en løstknyttet global bevægelse uden formelle strukturer, regler eller medlemslister kan definere nogle som mere rigtige end andre, skal her stå hen i det uvisse. Flere steder på nettet kan man finde udsagnet om, at alle kan være Anonymous, eller som det kan læses på hjemmesiden anonkbh.dk:

"Anonymous er en idé, et ideal, et catch-all for en kultur, der er opstået på internettet. Anonymous er et navn som selvstændige grupper kan påtage sig, når de handler i hvad de mener er dette ideals ånd."

Uenigheden om hvorvidt angrebene mod 3F var udført af Anonymous eller ej, illustrerer to ting. Dels at der en vilje til at aktionere, hvis man mener, at nogen opfører sig på en måde, der ikke er i overensstemmelse med egne holdninger. Dels at Anonymous ikke er en hackergruppe, men snarere en idé eller bevægelse som man kan tilslutte sig efter forgodtbefindende.

Det er ikke første gang, vi ser hacktivister udføre angreb i Danmark. Imidlertid er det første gang, at en sag, der har så lokal interesse, angiveligt opnår global opbakning. Den udvikling er muliggjort af Anonymous' massive medieomtale, synligheden af deres kommunikationskanaler og en global interesse for at indgå i dette virtuelle fællesskab. Resultatet af ens protester er nemlig her meget synlige.

Ved at forstå og reagere på Anonymous som en global gruppe med et fælles fokus og mål overser man mangfoldigheden af angrebsmotiver fra grupper eller individer, som sætter signaturen Anonymous på deres handlinger. De mere eller mindre politisk motiverede angreb har altid eksisteret. Ved at kalde det Anonymous har man nu fået mulighed for at få global tilslutning til angreb, der primært vedrører lokale forhold.

DK•CERT mener:

Med signaturen Anonymous som den mest fremtrædende har hacktivisme gennem de seneste år været blandt de store nye tendenser. Vi ser en stigning i politisk motiverede angreb som en tendens, der vil fortsætte. Både globalt og lokalt.

Vi mener, at man ikke bør frygte Anonymous, men i stedet overveje, om organisationens forretning, handlinger og data kan give anledning til, at man bliver mål for lokalt betingede angreb, og bruge det aktivt i forhold til den løbende risikovurdering.

Om hacktivisme:

Sammentrækning af hacking og aktivisme, eller på dansk "politisk motiveret hacking". Hacktivister forfølger politiske mål gennem brugen af internettet. De kan overordnet opdeles i tre bevægelser:

Anonymous, der støtter det frie internet er den mest synlige og aktive gruppering. Deres metoder involverer hacking, DDoS-angreb, informationstyveri og offentliggørelse af personlige eller fortrolige informationer.

Cyberoccupiers er de traditionelle aktivister, der primært benytter internettet til propaganda og informationsdeling. Med henvisning til Occupy-bevægelsen er de for et mere transparent demokrati og imod korruption.

Cyberkrigerne er folk, der kæmper for en sag, hvad enten det er religion, nationalstater eller ekstremistiske bevægelser. Benytter sig primært af webgraffiti og DDoS-angreb.

Anonymous København; "*Velkommen til Anonymous København*".
Berlingske, 2012; "*3F-hacker-angreb rammer dagpengene*".
BT, 2012; "*Anonymous: 3F-hackerne er forrædere*".
McAfee, 2012; "*Hacktivism - Cyberspace has become the new medium for political voices*".
TV 2, 2012; "*Anonym hacker: Operationen er kørt af sporet*".
TV 2, 2012; "*3F's hjemmeside lagt ned af hackere*".

3.2. NemID-angreb afværget i Sydbanks netbank

Den 14. august informerede Sydbank sine kunder om, at bankens netbankløsning var under angreb. Som ved årets tidligere netbankindbrud var de uheldige bankkunders computere inficeret med malware, der ved login interagerede med NemID-løsningen.

Ved et realtime man-in-the-middle-angreb lykkedes det i løbet af juli og august måned hackere at logge ind på 13 Sydbank-kunders netbankkonti. Normal login på netbanken ledte ved hjælp af en trojansk hest kunderne til en ny login-side. Den var midlertidig falsk og gav angriberne mulighed for at etablere en ny NemID-session mod netbankløsningen. Pengeoverførslerne blev dog opdaget og afværget af Sydbanks systemer til fraud detection.

Angrebet bliver sandsynligvis ikke det sidste, vi ser på danske netbanker. Det illustrerer truslerne mod NemID's fortsatte succes. Den afhænger af brugernes tillid til løsningen. Her er det væsentligt, at man er i stand til at afværge kommende angreb, hvilket dog også er brugernes eget ansvar. For at angrebene lykkes, kræver det, at man er i stand til forinden at inficere deres computere med malware.

Usikkerhed om Java-platformen er en yderligere problemstilling, som man står over for. Hvordan skal man for eksempel som bruger forholde sig til 0-dags sårbarheder i Java, som den vi i august advarede mod? At man ikke har været i stand til at få et dansk domænenavn til NemID, hvis hjemmeside i dag hedder www.nemid.nu, er tilsvarende med til at skabe uklarhed.

NemID-løsningen har siden den blev introduceret i 2010 været udsat for kritik. Den har blandt andet gået på, at løsningen ikke var brugervenlig nok, var for central og omfattede adgang til både det offentlige og private, blev udviklet og drevet i privat regi og generelt ikke var sikker nok. Særligt har der været kritik af Java, som er valgt som platform for løsningen. Java bliver vurderet som usikker og kan ikke benyttes på alle mobile platforme.

Hvad enten kritikken er berettiget eller ej, er mangfoldigheden af synspunkter med til at sikre, at NemID formes, så den også i fremtiden er både brugervenlig og sikker. I sidste ende handler det om, at vi som brugere har tillid til en løsning, som også er brugervenlig. Også brugeren selv har et medansvar for at login-proceduren ikke kompromitteres af tredjepart. Det vil primært sige at den benyttede computer holdes opdateret og sikker. Belært af det seneste års erfaringer står vi her med en udfordring, som primært er af kommunikativ karakter.

DK•CERT, 2012; "*Alvorligt hul i Java står åbent*".
Sydbank, 2012; "*Angreb på Sydbanks NetBank*".
Version2, 2012; "*Domæne-chok: DanID taber retten til nemid.dk med et brag*".
Version2, 2012; "*Hackere angriber Sydbanks netbank med virus*".
Version2, 2012; "*Hackere snyder NemID igen: Sydbank stopper massivt angreb*".

DK•CERT mener:

Med et par år på bagen er teknologien og brugsmønstrene for NemID efterhånden velkendte. Også i de internet-kriminelle miljøer. Derfor har vi i år set flere netbankangreb, hvor det er lykkedes at omgå sikkerheden i NemID. Vi venter, at disse angreb i fremtiden vil stige i antal.

Vi mener grundlæggende, at NemID er en både sikker og brugervenlig løsning. Det skal dog ikke give anledning til, at vi hviler på laurbærrene, da der er plads til forbedringer. Både i forhold til den benyttede teknologi, hvor og hvordan den benyttes, samt hvorledes løsningen kommunikeres til brugerne. I sidste ende handler det om, at vi har tillid til løsningen.

"Angrebet bliver sandsynligvis ikke det sidste, vi ser på danske netbanker. Det illustrerer truslerne mod NemID's fortsatte succes. Den afhænger af brugernes tillid til løsningen."

3.3. Krav om informationspligt ved tab af data

Sidst i august kritiserede flere personer i sikkerhedsbranchen de danske organisationer for at holde hackerangreb skjult. Ønsket om større åbenhed blev siden taget op af politikere fra både Venstre og Socialdemokratiet, der ikke ville love regulerende lovgivning. Den er dog på vej ind ad bagdøren gennem EU-kommissionens udkast til en revision af databeskyttelsesdirektivet.

Ifølge tal fra Danmarks Statistik svarede syv procent af danske virksomheder med mere end ti ansatte, at de i 2010 var udsat for ødelæggelse af data på grund af virus eller uautoriseret adgang. Seks procent havde oplevet forstyrrelser i it-systemer på grund af denial-of-service-angreb og lignende. Hertil kommer forsøg på angreb, som enten ikke blev opdaget eller ikke gav anledning til forstyrrelser eller tab af data. Det er relativt store tal, som overstiger antallet af politianmeldelser.

Vi har gennem en årrække givet udtryk for et ønske om indberetningspligt ved brud på informationssikkerheden. Dels skylder man sine kunder at orientere dem, og dels betyder den nuværende adfærd, at vi ikke har reel viden om problemernes omfang. Herved blokeres for læring, som i sidste ende også vil komme virksomhederne til gode. Det kommenterede Lars Neupart i en artikel i Berlingske:

"... når der ikke er en åben kommunikation om sikkerhedshændelser, bliver vi ikke klogere som fagfolk."

I dansk lovgivning er virksomhederne ikke forpligtede til at informere om læk af personfølsomme oplysninger, medmindre de selv vurderer, at der er behov for det. Det står i kontrast til blandt andet flere amerikanske delstater, hvor virksomhederne skal informere både offentligheden og personer, hvis data er berørt. Den praksis vil et udkast til revision af EU's databeskyttelsesdirektiv indføre.

EU-kommissionens udkast blev offentliggjort den 25. januar. Det styrker borgernes retsstilling og giver i højere grad ejerskab af egne data. Blandt andet betyder det, at borgeren har krav på at blive orienteret, hvis dennes data kompromitteres af tredjepart, ligesom virksomhederne har pligt til at orientere en lokal tilsynsførende myndighed. Ansvaret for overholdelse af lovgivning påhviler herhjemme Datatilsynet, hvis direktør Janni Christoffersen blandt andet udtalte:

"For virksomheder og organisationer er der større krav om at tage ansvar for databeskyttelse. Der strammes op med nye forpligtelser for at øge fokus på databeskyttelse."

Hvis lovændringen indføres, vil det betyde et større økonomisk incitament for organisationerne til at tage ansvar for informationssikkerheden. Ud over indirekte omkostninger som prestigetab kan kompromittering af virksomhedernes data betyde bøder eller erstatning, som håndhæves i stil med markedsføringslovens §6 vedrørende spam. Derudover pålægges det organisationer med over 250 ansatte at udpege en databeskyttelsesansvarlige, der skal medvirke til organisationens overholdelse af forordningen.

Berlingske, 2012; "*IT-indbrud holdes skjult for dig*".
Berlingske, 2012; "*Politikere ønsker mere åbenhed om hackerangreb*".
Danmarks Statistik, 2011; "*Danske virksomheders brug af it - 2011*".
Datatilsynet, 2012; "*EU-Kommissionens reformpakke om databeskyttelse*".
Datatilsynet, 2012; "*Udtalelse om EU-Kommissionens forslag til forordning om databeskyttelse*".

DK•CERT mener:

De seneste år har sat fokus på offentliggørelse af kompromitterede data. Data flyder og lagres på tværs af landegrænser. Derfor hilser vi en europæisk harmonisering af reglerne om databeskyttelse velkommen.

Vi mener, at en skærpet informationspligt ikke blot vil sikre borgernes rettigheder, men også øge organisationernes fokus på informationssikkerhed. I et bredere perspektiv giver informationspligten muligheder for videnindsamling og -deling omkring aktuelle trusler, som ikke er mulig i dag. Alt sammen til borgernes, organisationernes og samfundets bedste.

"... når der ikke er en åben kommunikation om sikkerhedshændelser, bliver vi ikke klogere som fagfolk."

Europa-kommissionen, 2012; "*Commission proposes a comprehensive reform of the data protection rules*".
Europa-kommissionen, 2012; "*Opinion 01/2012 on the data protection reform proposals*".
Version2, 2012; "*Opråb til danske virksomheder: Skjul ikke hackerangreb*".
Version2, 2012; "*Pas på nye privacy-regler: Datatilsynet får kæmpe bødehammer*".

3.4. Når malware tager data som gidsel

Din computer er låst, indtil du har betalt en bøde for at se børneporno, med venlig hilsen politiet. Det er den korte version af en type malware, der gennem de seneste år er steget i antal. Politi-ransomware er blevet en god forretning, der i juli måned også blev målrettet danskerne.

Politi-ransomware er blandt de hurtigst voksende trusler på internettet. Derfor har både FBI og Europol i år advaret specifikt mod den. At det også er en god forretning, viser bagmændenes egne statistikker. En enkelt variant blev den 17. maj spredt til 2.116 computere alene i Frankrig. I 79 tilfælde (3,7 procent) valgte brugerne at betale "bøden". I alt betalte 322 personer fra hele verden denne dag, hvilket indbragte 28.000 euro. Dagen efter var indtjeningen 44.000 euro.

Ved hjælp af exploit kits som for eksempel BlackHole spredes malwaren fra kompromitterede hjemmesider ved drive-by-download til de besøgendes computere. Ofte efterprøves flere sårbarheder i for eksempel Java, Flash eller Adobe Reader. Lykkes det at inficere computeren, hentes koden, der ved for eksempel kryptering låser computeren. Herefter præsenteres brugeren for kravet om at betale en bøde for at få låst maskinen op. Den mest kendte variant, Reveton, installerer samtidig en trojansk hest og indeholder funktionalitet til indsamling af brugernavne og kodeord fra computeren.

I juli måned kom det første tilfælde af den type malware målrettet danskere. Et vindue med overskriften "Computeren er blevet blokeret for at overtræde lovgivningen i Danmark" fortalte, at man havde set børnepornografisk materiale og piratkopieret ophavsretsbeskyttet materiale. Derfor var maskinen blevet låst, indtil man via betalingstjenesten Ukash havde betalt en bøde på 100 euro. Beskeden var udført på dårligt dansk og uden en egentlig afsender, hvorfor de fleste gennemskuede, at der var tale om malware.

Som falske telefonopkald fra Microsoft er politi-ransomware delvist et skridt i evolutionen af falske antivirusprodukter. De præsenterer de inficerede for et vindue, der fortæller, at maskinen er inficeret med malware, som kun kan fjernes ved køb af et specifikt "antivirusprodukt". For at øge incitamentet til at købe det falske antivirusprodukt har malwaren i stigende grad "låst" den inficerede computer.

Med en kombination af en ubrugelig maskine, brugerens skyldfølelse og pres fra "myndighederne" har politi-ransomware skruet op for brugen af social engineering. Det skal i sidste ende få brugeren til at betale uden at konsultere andre. De færreste har lyst til at fortælle naboen eller kollegaen, at man har fået en bøde for at kigge på børneporno. Det hvad enten det er tilfældet eller ej. Mens inficeringer med falske antivirusprodukter ifølge McAfee falder, er ransomware derfor i vækst.

Vi har endnu ikke set troværdige eksempler på ransomware, der udgiver sig for at komme fra de danske myndigheder. Om det skyldes, at vi rent sprogligt udgør et relativt lille "marked", manglende udbredelse af anonyme betalingsmidler eller at vores computere er mere sikre end i de andre europæiske lande, ved vi ikke. Det seneste eksempel fra juli måned giver dog en forventning om, at det er et pro-

DK•CERT mener:

Ransomware er den hurtigste og nemmeste måde at omsætte sin kode til rede penge på. Når malwaren er distribueret til download, er det blot at vente på, at pengene ruller ind på kontoen. I modsætning til andre typer malware er der ingen data, der efterfølgende skal bearbejdes eller forsøges omsat til penge.

Derfor venter vi, at væksten af denne type malware vil fortsætte – også målrettet danskere. Så længe der er computere, som ikke er beskyttet, er der brugere, der er villige til at betale for igen at få adgang til deres computer og data. Det hvad enten det er "politiet" eller andre, der har låst den.

Ransomware:

Malware, der tager brugernes data som gidsel, indtil der er betalt løsepenge (ransom) med anonyme betalingssystemer som for eksempel Ukash, Paysafe og MoneyPak. Oftest sker gidseltagningen ved at kryptere indhold på den inficerede computer, hvorfor malwaren blandt andet også benævnes kryptovirus. Malwaretypen er ikke ny og har i flere år floreret særligt i Rusland. En af de første trojanske heste, AIDS- eller PC Cyborg-trojaneren fra 1989, havde samme funktionalitet.

Politi-ransomware er det seneste skud på stammen. Den spredes ved drive-by-download. Brugeren præsenteres for en besked fra den lokale politimyndighed, der fortæller, at maskinen er låst på grund af download af børneporno, kopibeskyttet materiale og tilsvarende. Maskinen låses op ved betaling af en bøde på typisk 100 euro, pund eller dollars.

"De færreste har lyst til at fortælle naboen eller kollegaen, at man har fået en bøde for at kigge på børneporno. Det hvad enten det er tilfældet eller ej."

blem, som også herhjemme vil vokse i både troværdighed og mængde. Der er trods alt tale om en god forretning.

Computerworld, 2012; "*Her er den første afpresnings-software på dansk*".
McAfee, 2012; "'*Police ransomware' preys on guilty consciences*".
McAfee, 2012; "*McAfee threats report: Second quarter 2012*".
KrebsonSecurity, 2012; "*Inside a 'reveton' ransomware operation*".
Wikipedia; "*Ransomware (malware)*".
Wikipedia; "*Rogue security software*".

3.5. Angreb udnyttede hul i Internet Explorer

Et hidtil ukendt sikkerhedshul i Internet Explorer blev brugt i begrænsede, målrettede angreb. Programmet benyttes til halvdelen af danskernes internetsurf, så truslen var potentielt alvorlig. I medierne blev den præsenteret som meget alvorlig.

Den 16. september skrev sikkerhedsforsker Eric Romang på sin blog, at han havde fundet et angrebsprogram på en server. En analyse viste, at angrebet udnyttede et hidtil ukendt sikkerhedshul i Internet Explorer. Dagen efter bekræftede Microsoft, at sårbarheden findes i Internet Explorer 6, 7, 8 og 9. Den 19. september udsendte de en midlertidig rettelse af typen Fix It. Den 21. september kom en rettelse, der fjernede denne og fire andre sårbarheder i Internet Explorer.

Sårbarheden lå i browserens behandling af objekter, der bliver slettet. Angribere kunne udnytte den til at afvikle programkode. Kort tid efter offentliggørelsen blev der udsendt et modul til Metasploit, der udnyttede sårbarheden i praksis. Der er kun observeret få angreb, der udnytter sårbarheden.

Medierne skruede op for sensationen i dækningen af sårbarheden. Flere talte om en kommende virus, skønt der kun var tale om en sårbarhed. Det gav øget opmærksomhed hos borgerne, hvilket er en god ting. Men det medførte også, at nogle borgere blev mere bekymrede, end der var grund til.

Når medierne taler om virus, skyldes det nok, at begrebet sårbarhed eller sikkerhedshul ikke er kendt. Her har sikkerhedsbranchen en informationsopgave, så befolkningen lærer at forstå begreberne sårbarhed, virus og angrebsprogram.

I dette tilfælde er der tale om en potentielt alvorlig sårbarhed, der dog endnu ikke har været brugt til særlig mange angreb. Det korrekte budskab burde derfor være, at brugerne så vidt muligt skulle undlade at bruge Internet Explorer, indtil Microsoft kom med en rettelse. Kunne det ikke lade sig gøre, kunne man følge de råd, som Microsoft giver i sin sikkerhedsadvarsel: Installer EMET (Enhanced Mitigation Experience Toolkit) eller sæt sikkerheden for zonen Internet til Høj. Det sidste råd er umiddelbart nemmest at følge, men i praksis medfører det, at mange websteder ikke fungerer. Derfor risikerer man, at brugerne hurtigt dropper indstillingen og dermed bliver sårbare igen.

Nogle organisationer kan med et tryk på en knap ændre sikkerhedsindstillingen i Internet Explorer for alle brugere. For andre kræver det, at hver enkelt medarbejder modtager en mail og følger anvisningerne i den. Naturligvis er den første metode mest effektiv.

DK•CERT mener:

Når der opdages en sårbarhed i et så udbredt program som Internet Explorer, er det afgørende at kommunikere korrekt om den. Informationen skal på den ene side fortælle, hvor alvorlig sårbarheden er, på den anden side skal den ikke skræmme ved at overdrive konsekvenserne. Organisationer skal derfor nøje overveje, hvordan de informerer deres brugere om truslen, og hvad de bør gøre.

Vi mener, at denne type sårbarhed viser, hvor vigtigt det er at have centrale værktøjer til administration. Derfor bør organisationer lette deres sikkerhedsarbejde ved at indføre central administration af sikkerhedspolitikker.

"Medierne skruede op for sensationen i dækningen af sårbarheden. Flere talte om en kommende virus, skønt der kun var tale om en sårbarhed."

DK•CERT, 2012; "*Microsoft lukker huller i IE og Flash*".
Foreningen af Danske Interaktive Medier (FDIM); "*Browserbarometer*".
Microsoft, 2012; "*Microsoft security advisory (2757760)*".
Erik Romang, 2012; "*Zero-Day Season Is Really Not Over Yet*".

3.6. Hackere lækkede data fra universiteter

Ved at udnytte SQL-injection-sårbarheder fik hackere fat i data fra en række universiteters databaser. De lagde oplysninger om godt 40.000 brugerkonti ud på nettet. Årsagen er angiveligt, at man er utilfreds med udviklingen af uddannelsessystemerne.

Den 1. oktober lagde en hackergruppe ved navn Teamghostshell data fra universiteter ud på forskellige websteder. Ifølge gruppen selv er der tale om data fra verdens top 100 universiteter, der ikke før har været lækket. Tidligere har Anonymous-bevægelsen fremsat trusler mod uddannelsesinstitutioner i Europa, og selvom der ingen danske universiteter er blandt de hackede institutioner, illustrerer det, at også de kan blive mål for angreb.

De lækkede data er for eksempel mail-adresser og brugernavne på ansatte og studerende. I nogle tilfælde optræder også passwords, ofte dog kun som hashværdier. Det ser således ud til, at der ikke var kritiske data i lækagen. Danskere der har været tilknyttet udenlandske institutioner, bør dog tjekke, om deres data optræder på listerne.

Hackergruppen skriver, at den fandt langt flere data, men at den har valgt at begrænse offentliggørelsen af dataposter. På mange af de kompromitterede servere fandt de efter eget udsagn også skadelige programmer (malware).

Stikprøver viser, at data typisk er hentet ved at udnytte SQL-injection-sårbarheder i web-applikationer. Den slags sårbarheder er ofte relativt nemme at fjerne. Med tanke på at webgrænsefladen er blandt de mest angrebne, kan man derfor undre sig over, at så store organisationer overhovedet havde den slags sårbarheder.

Angrebet er et eksempel på hacktivisme i stil med den, vi også kender fra Anonymous-bevægelsen. Teamghostshell begrunder lækagen med, at gruppen er kritisk over for udviklingen af uddannelsessystemerne og hvordan de interagerer med den øvrige verden. Eller som de blandt andet selv skriver på webstedet Pastebin:

"… we have ventured from learning valuable skills that would normally help us be prepared in life, to just, simply memorizing large chunks of text in exchange for good grades."

Angrebet viser, at selvom man ikke har profit som mål og i egen selvopfattelse arbejder til samfundets bedste, kan der være nogle, der har en anden holdning til, hvordan man udfører sine gerninger. Som med angrebet på 3F's hjemmeside i juli bør det medføre et større fokus på databeskyttelse. Også i organisationer der ikke traditionelt opfattes som oplagte mål.

Identityfinder, 2012; "*Large-Scale Coordinated SQLi Attack on Higher Education*".
Threatpost, 2012; "*Team Ghost Shell claims to publish records from thousands of universities*".
Teamghostshell, 2012; "*#ProjectWestWind - Today's education!*".

DK•CERT mener:

Globaliseringen har medført en stigende mangfoldighed i motiver og muligheder for digitale angreb. Således viser det aktuelle angreb, at det i dag er de færreste organisationer, der kan afskrives som mål. Mange af de sårbarheder der blev udnyttet, er nemme at fjerne og burde ikke have været der.

Det er en god anledning til at tjekke, om ens egen it-sikkerhed er på plads. Her mener vi, at angrebet bør medføre, at man også i den akademiske verden sætter større fokus på sårbarheder i sine web-applikationer. Det er oftest dem, der udnyttes, hvad enten det handler om at stjæle data eller kompromittere sidens besøgende.

4. Ordliste

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

Anonymous-bevægelsen: En løst defineret internetbaseret gruppe, som i 2003 opstod via hjemmesiden 4chan.org. Gruppen benytter sig blandt andet af DDoS angreb i deres kamp for ytringsfrihed og mod hvad de anser som censur og misbrug af nettet. Er særlig kendt for dens modstand mod Scientology Kirken og for sin støtte til Wikileaks og The Pirate Bay. Gruppen stod også bag operation AntiSec i foråret 2011.

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.

Cross-site request forgery (CSRF): En metode, der muliggør at uautoriserede parametre og kommandoer eksekveres på serveren gennem henvendelser fra en bruger, som websitet har tillid til. Metoden kan for eksempel medføre overtagelse af brugerens session til det enkelte site.

Cross-site scripting (XSS): En sårbarhed på et websted, der gør det muligt at afvikle scriptkode i browseren hos en bruger, der besøger det. Der er forskellige former for cross-site scripting, som gør det muligt at udføre komplekse angreb. Metoden kan for eksempel anvendes til phishing, hvor brugeren bliver omdirigeret til et forfalsket website. En angriber kan udnytte et website, som en bruger har tillid til, til at få adgang til fortrolig information.

CVE, CVE-nummer: Common Vulnerabilities and Exposures, forkortet CVE, er en liste over offentligt kendte sårbarheder i software. Listen dækker sårbarheder i de fleste kendte og alment udbredte programmer, men ikke i skræddersyet eller internt udviklet software, der ikke er i distribution, såsom de fleste webapplikationer.

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 samtidig. Det kaldes distributed denial of service (DDoS).

Drive-by attacks, drive-by download: Angreb hvor tilfældige besøgende på en kompromitteret hjemmeside forsøges inficeret med skadelige programmer. Den inficerede hjemmeside vil ofte være en sårbar legal side, som brugeren har tillid til,

og infektionen foregår uden dennes vidende. Infektionen udnytter som regel sårbarheder i programmer på brugerens pc, ofte browseren eller udvidelser som Flash og Java.

Exploit: Et program som forsøger at udnytte sårbarheder i software med det formål at kompromittere systemet.

Exploit kit: Software der placeres på et website og afsøger de besøgendes computer for sårbarheder i browseren og tilhørende programmer. Er computeren sårbar, kompromitteres den med et af programmets exploits. Indeholder ofte også funktioner til opdatering, statistik med mere.

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

Hacker: På dansk betyder hacker en person, der uden foregående tilladelse forsøger at kompromittere computersystemers sikkerhed. På engelsk kan man skelne mellem en hacker og en cracker eller whitehat hacker og blackhat hackere, afhængigt af om aktivitetens formål er at forbedre kode og/eller sikkerhed, eller det er at udføre it-kriminalitet.

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

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

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

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

Ransomware: Sammentrækning af ordene ransom (løsesum) og malware. Skadelig kode, der tager data som gidsel, ofte ved kryptering.

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

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

eller installere malware.

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.

Sårbarhed: En fejl i et it-system, som en angriber kan udnytte til at få adgang til systemet, forhindre det i at fungere eller på anden måde misbruge det.

Sårbarhedsscanning: Kortlægning af kendte sårbarheder knyttet til services på et systems åbne porte. Benyttes ofte efter foregående scanning.

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

Virus: Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres virussen, og den inficerer andre programfiler. Oprindelig kunne kun egentlige programmer indeholde virus, men dokumenter med makroer kan også gøre det. Virus spredes ofte som mail vedlagt en trojansk hest, der indeholder virussen selv.

Warez, piratsoftware: Begrebet dækker over computerprogrammer, musik, film og lignende, der distribueres illegalt og i strid med rettigheder og licensbetingelser. Warez er en sproglig forvanskning af flertalsformen af software.

5. Figuroversigt

6. Referencer

Adobe, 2012; "*Security updates available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb12-19.html

Anonymous København; "*Velkommen til Anonymous København*"; anonkbh.dk/info/

Apple, 2012; "*About the security content of iTunes 10.7*"; support.apple.com/kb/HT5485

Apple, 2012; "*About the security content of Java for OS X 2012-005 and Java for Mac OS X 10.6 Update 10*"; support.apple.com/kb/HT5473

Apple, 2012; "*About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004*"; support.apple.com/kb/HT5501

Apple, 2012; "*About the security content of Safari 6*"; support.apple.com/kb/HT5400

Apple, 2012; "*APPLE-SA-2012-09-19-1 iOS 6*"; prod.lists.apple.com/archives/security-announce/2012/Sep/msg00003.html

Apple, 2012; "*APPLE-SA-2012-09-19-3 Safari 6.0.1*"; prod.lists.apple.com/archives/security-announce/2012/Sep/msg00005.html

Berlingske, 2012; "*3F-hacker-angreb rammer dagpengene*"; www.b.dk/nationalt/3f-hacker-angreb-rammer-dagpengene

Berlingske, 2012; "*IT-indbrud holdes skjult for dig*"; www.b.dk/nationalt/it-indbrud-holdes-skjult-for-dig

Berlingske, 2012; "*Politikere ønsker mere åbenhed om hackerangreb*"; www.b.dk/politiko/politikere-oensker-mere-aabenhed-om-hackerangreb

BT, 2012; "*Anonymous: 3F-hackerne er forrædere*"; www.bt.dk/politik/anonymous-3f-hackerne-er-forraedere

Cnet, 2012; "*German government tells public to stop using Internet Explorer*"; news.cnet.com/8301-10805_3-57515312-75/german-government-tells-public-to-stop-using-internet-explorer/

Computerworld, 2012; "*Her er den første afpresnings-software på dansk*"; www.computerworld.dk/art/220175/her-er-den-foerste-afpresnings-software-paa-dansk

Danmarks Statistik, 2011; "*Danske virksomheders brug af it - 2011*"; www.dst.dk/pukora/epub/upload/15242/dkit.pdf

Danmarks Statistik, 2012; "*It-anvendelse i befolkningen 2012*"; www.dst.dk/pukora/epub/Nyt/2012/NR376.pdf

Danmarks Statistik, 2012; "*It-anvendelse i virksomheder 2012*"; www.dst.dk/pukora/epub/Nyt/2012/NR465.pdf

Datatilsynet, 2012; "*EU-Kommissionens reformpakke om databeskyttelse*"; www.datatilsynet.dk/nyheder/nyhedsarkiv/artikel/eu-kommissionens-reformpakke-om-databeskyttelse/

Datatilsynet, 2012; "*Udtalelse om EU-Kommissionens forslag til forordning om databeskyttelse*"; www.datatilsynet.dk/nyheder/nyhedsarkiv/artikel/udtalelse-om-eu-kommissionens-forslag-til-forordning-om-databeskyttelse-1/

DK•CERT, 2012; "*Alvorligt hul i Java står åbent*"; https://www.cert.dk/nyheder/nyheder.shtml?12-08-27-13-02-46

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

DK•CERT, 2012; "*Microsoft lukker huller i IE og Flash*"; https://www.cert.dk/nyheder/nyheder.shtml?12-09-24-08-56-11

Eric Romang, 2012; "*Zero-Day season is really not over yet*"; eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/

Erpscan, 2012; "*SAP critical patch update September 2012*"; erpscan.com/press-center/news/sap-critical-patch-update-september-2012/

Europa-kommissionen, 2012; "*Commission proposes a comprehensive reform of the data protection rules*"; ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Europa-kommissionen, 2012; "*Opinion 01/2012 on the data protection reform proposals*"; ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

FireEye, 2012; "*Java zero-day - first outbreak*"; blog.fireeye.com/research/2012/08/java-zero-day-first-outbreak.html

FireEye, 2012; "*Zero-day season is not over yet*"; blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

F-Secure, 2012; "*F-Secure security lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

F-secure, 2012; "*Threat report H1 2012*"; www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2012.pdf

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

GFI Labs, 2012; "*Fraudsters use legit AV brands to mask Boxer*"; www.gfi.com/blog/fraudsters-use-legit-av-brands-to-mask-boxer/

Google, 2012; "*Stable channel release*"; googlechromereleases.blogspot.ca/2012/07/stable-channel-release.html

Identityfinder, 2012; "*Large-Scale Coordinated SQLi Attack on Higher Education*"; www.identityfinder.com/blog/post/Large-Scale-Coordinated-SQLi-Attack-on-Higher-Education.aspx

Incapsula , 2012; "*Top security threats and attackers by country*"; www.incapsula.

com/the-incapsula-blog/item/397-top-security-threats-and-attackers-by-country

Kaspersky Lab, 2012; "*Spam in August 2012*"; www.securelist.com/en/analysis/204792246/Spam_in_August_2012

Kaspersky Lab, 2012; "*The geography of cybercrime: Western Europe and North America*"; www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America

KrebsonSecurity, 2012; "*Inside a 'Reveton' ransomware operation*"; krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

McAfee, 2012; "*Hacktivism - Cyberspace has become the new medium for political voices*"; www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf

McAfee, 2012; "*'Police ransomware' preys on guilty consciences*"; blogs.mcafee.com/mcafee-labs/police-ransomware-preys-on-guilty-consciences

McAfee, 2012; "*'McAfee threats report: Second quarter 2012*"; www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf

Microsoft, 2012; "*Microsoft security advisory (2757760)*"; technet.microsoft.com/en-us/security/advisory/2757760

Microsoft, 2012; "*Microsoft security bulletin summary for August 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-aug

Microsoft, 2012; "*Microsoft security bulletin summary for July 2012*";technet.microsoft.com/en-us/security/bulletin/ms12-jul

Microsoft, 2012; "*More information on security advisory 2757760's Fix It*"; blogs.technet.com/b/srd/archive/2012/09/19/more-information-on-security-advisory-2757760-s-fix-it.aspx

Microsoft, 2012; "*MS12-063: Cumulative security update for Internet Explorer: September 21, 2012*"; support.microsoft.com/kb/2744842

Mozilla, 2012; "*Mozilla Foundation security advisories*"; www.mozilla.org/security/announce/

Mozilla, 2012; "*Security advisories for Firefox*"; www.mozilla.org/security/known-vulnerabilities/firefox.html

National Institute of Standards and technology (NIST); "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Oracle, 2012; "*Oracle critical patch update advisory - July 2012*"; www.oracle.com/technetwork/topics/security/cpujul2012-392727.html

Oracle, 2012; "*Oracle security alert for CVE-2012-4681*"; www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html

Privacy PC, 2012; "*Where are we and where are we going 3: Ransom trojans*"; privacy-pc.com/articles/where-are-we-and-where-are-we-going-3-ransom-trojans.html

SearchSecurity , 2012; "*FireEye warns of steady increase in advanced malware*";

searchsecurity.techtarget.com/news/2240162628/FireEye-warns-of-steady-increase-in-advanced-malware

Seclists, 2012; "*[SE-2012-01] New security issue affecting Java SE 7 Update 7*"; seclists.org/bugtraq/2012/Aug/225

Sophos, 2012; "*Exploring the Blackhole Exploit Kit*"; sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf

Sydbank, 2012; "*Angreb på Sydbanks NetBank*"; http://www.sydbank.dk/privat/artikler/netbankindbrud

Symantec; "*Intelligence reports*"; www.symanteccloud.com/da/dk/globalthreats/overview/r_mli_reports

Teamghostshell, 2012; "*#ProjectWestWind - Today's education!*"; pastebin.com/AQWhu8Ek

Threatpost, 2012; "*Team Ghost Shell claims to publish records from thousands of universities*"; threatpost.com/en_us/blogs/team-ghost-shell-claims-publishe-records-thousands-univerisities-100212

TV 2, 2012; "*Anonym hacker: Operationen er kørt af sporet*"; nyhederne.tv2.dk/article.php/id-52040255:anonym-hacker-operationen-er-k%C3%B8rt-af-sporet.html

TV 2, 2012; "*3F's hjemmeside lagt ned af hackere*"; nyhederne.tv2.dk/article.php/id-51969246:3fs-hjemmeside-lagt-ned-af-hackere.html

Version2, 2012; "*Domæne-chok: DanID taber retten til nemid.dk med et brag*"; version2.dk/artikel/domaene-chok-danid-taber-retten-til-nemiddk-med-et-brag-47523

Version2, 2012; "*Hackere angriber Sydbanks netbank med virus*"; www.version2.dk/artikel/hackere-angriber-sydbanks-netbank-med-virus-46985

Version2, 2012; "*Hackere snyder NemID igen: Sydbank stopper massivt angreb*"; www.version2.dk/artikel/sydbank-stopper-13-netbank-indbrud-efter-nemid-hacking-46990

Version2, 2012; "*Opråb til danske virksomheder: Skjul ikke hackerangreb*"; www.version2.dk/artikel/opraab-til-danske-virksomheder-skjul-ikke-hackerangreb-47137

Version2, 2012; "*Pas på nye privacy-regler: Datatilsynet får kæmpe bødehammer*"; www.version2.dk/artikel/nye-eu-krav-oeger-alvor-i-datatab-men-mindsker-bureaukrati-43148

Websense, 2012; "*New Java 0-day added to Blackhole Exploit Kit*"; community.websense.com/blogs/securitylabs/archive/2012/08/28/new-java-0-day-added-to-blackhole-exploit-kit.aspx

Wikipedia; "*Ransomware (malware)*"; en.wikipedia.org/wiki/Ransomware_(malware)

Wikipedia; "*Rogue security software*"; en.wikipedia.org/wiki/Rogue_security_software

Kontakt:

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

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