Myndigheten för
samhällsskydd
och beredskap

Trendrapport

– samhällets informationssäkerhet 2012

Trendrapport

– samhällets informationssäkerhet 2012

Trendrapport – samhällets informationssäkerhet 2012

Myndigheten för samhällsskydd och beredskap (MSB)

Layout: Advant Produktionsbyrå AB
Tryck: DanagårdLiTHO

Publ.nr MSB505 - december 2012
ISBN 978-91-7383-301-1

Förord

Informationshanteringen i samhället blir alltmer omfattande och komplex. Den snabba utvecklingen inom informationstekniken möjliggör nya och förbättrade former av informationshantering, som på olika sätt ökar kvaliteten och servicegraden för många tjänster i samhället.

Samtidigt medför teknikutvecklingen att samhället blir mer sårbart för avbrott. Det ställs också allt högre krav på att den ökande informationsmängd som rör enskilda individer hanteras på ett säkert sätt. Att på olika sätt upptäcka och hantera de risker som vi ställs inför är en utmaning som kräver gemensamma insatser från alla samhällsaktörer.

MSB har i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet, analysera och bedöma utvecklingen inom området. I detta arbete ingår att lämna råd och stöd. Den här rapporten är en del av det arbetet.

Stockholm 2013-01-10

Richard Oehme
Chef för Enheten för samhällets informationssäkerhet

Sammanfattning

Denna rapport ger en övergripande bild av situationen på informations- och cybersäkerhetsområdet, samt en bedömning av vilka förhållanden som är särskilt angelägna att uppmärksamma. Innehållet är sammanställt med utgångspunkt från den löpande omvärldsanalys som sker vid MSB och baseras främst på utvecklingen under 2011 och 2012.

De utvecklingslinjer som redovisats i denna rapport ger en relativt disparat bild av den rådande situationen på informationssäkerhetsområdet. Några trender är dock tydliga. Dagens informationshantering präglas av hög förändringstakt. Framför allt är det kombinationen av växande informationsmängder, snabb övergång till centraliserade lösningar och den ökade mobiliteten bland användarna som innebär att riskbilden nu förändras, för såväl individer som organisationer och samhället i stort.

Sociala nätverkstjänster är numera en del av vardagen för många människor. Leverantörerna av dessa tjänster lagrar och har tillgång till stora mängder användarinformation och personuppgifter som hanteras enligt avtal mellan leverantör och användare. Risken finns dock att denna information kan användas på sätt som användaren inte tänkt sig.

Skadlig programkod är ett problem som funnits länge men till viss del finner nya former idag till följd av den ökande användarmobiliteten. Skadlig kod kan drabba alla delar av samhället, och har under det senaste decenniet vid upprepade tillfällen slagit ut verksamheten hos olika samhällsaktörer.

En annan utmaning är den mer direkt it-relaterade brottsligheten. Den är ett globalt fenomen som kräver att brottsbekämpande myndigheter idag tar till ny metodik samt samverkar internationellt. Företag inom bland annat finanssektorn drabbas av kännbara kostnader till följd av it-relaterade brott. Samtidigt är mörkertalet sannolikt stort.

Slutligen går det idag att se tydliga risker förknippade med den ökade integrationen och anslutningen av industriella styrsystem till olika kommunikationsnät och olika typer av inbyggda system. Eftersom sådana system används i en lång rad samhällsviktiga verksamheter, till exempel eldistribution och vattenförsörjning, är detta också ett område av säkerhetspolitisk betydelse.

Innehåll

Inledning

1. Inledning

Föreliggande trendrapport är framtagen för att ge en lättillgänglig och samlad bild av situationen på informationssäkerhetsområdet, samt en bedömning av vilka förhållanden som är särskilt angelägna att uppmärksamma och som kan komma att kräva åtgärder från framför allt det allmännas sida. Bedömningen är främst baserad på utvecklingen under 2011 och 2012.

Trendrapporten omfattar såväl nationella som internationella trender inom informations- och cybersäkerhetsområdet. Trendrapportens innehåll är sammanställt med utgångspunkt från den löpande omvärldsanalys som sker vid MSB inom området samhällets informationssäkerhet. Arbetet är baserat på flera olika typer av underlag: basinformation från öppna källor, egen händelsebevakning, händelseinitierade studier, offentligt skriftligt material och intervjuer med olika samhällsaktörer.

It-utvecklingen och dess konsekvenser

2. It-utvecklingen och dess konsekvenser

Sverige är en av världens ledande it-nationer där drygt 90 procent av befolkningen har tillgång till internet.[1] Utvecklingen och användningen av it sedan mitten av 1990-talet har skapat en mängd nya förutsättningar för bland annat kommunikation, lagring och utvinning av data, nya standarer och ekonomisk tillväxt. It-utvecklingen har därmed skapat en rad nya möjligheter, samtidigt som den medfört flera utmaningar.

Informationshanteringen i samhället blir ständigt alltmer omfattande och komplex. Det skapas och lagras mycket stora informationsmängder idag. 2010 var världens skapade eller kopierade datavolym drygt 1 ZB[2] stor. Det motsvarar närmare 150 GB – eller drygt 200 fullmatade CD-skivor - per människa på jorden. Ökningstakten är i storleksordningen 40 till 50 procent per år.[3] Den snabba teknikutvecklingen har gjort det möjligt att lagra hela dokumentsamlingar på en liten minnessticka som går att stoppa i fickan.

De lagringsnät som utgör centrallagren hos dagens it-driftleverantörer kan i sin tur rymma den samlade digitala informationen från ett stort antal företag eller myndigheter. Denna utveckling skapar nya möjligheter. Men den kan också leda till oönskade effekter, hur väl man än försöker skydda sig genom olika förebyggande säkerhetsåtgärder. En minnessticka som kommer på avvägar kan till exempel visa sig innehålla känsliga uppgifter om hundratusentals personer. Vid en mer omfattande it-störning kan det visa sig att stora mängder data från helt olika samhällsområden plötsligt blir otillgängliga.

Kombinationen av växande informationsmängder, ökat beroende av fungerade it-stöd inom snart sagt alla samhällsområden, samt en global koncentrationstendens inom it-drift, har idag skapat en förändrad riskbild som alla samhällets aktörer måste anpassa sig till. I många fall är den information som hanteras inte ens tillgänglig på papper längre. Merparten av informationshanteringen i samhället är idag digital. Så sent som vid millennieskiftet var huvuddelen fortfarande analog.[4]

Till detta kommer att allt större delar av informationen inte hämtas eller bearbetas lokalt. Den kommer utifrån – eller lagras på annan plats. Även kommunikation intar därför en central plats i vår vardag, med internet som främsta kommunikationskanal. Att kommunikation och it-stöd fungerar har idag blivit en förutsättning för att bankomaterna ska fungera och affärerna hålla öppet. Delar av samhällets kommunikation behöver därtill skyddas mot avlyssning eller förvanskning, vilket kräver särskilda åtgärder.

Sist men inte minst är it-utvecklingen tätt sammankopplad med beroendet av el. Skydd mot och planer för hantering av störningar och elavbrott blir, mot bakgrund av ovan, en viktig del i den dagliga hanteringen av it- och informationssäkerhet.

Koncentration och centraliserad it-drift

3. Koncentration och centraliserad it-drift

En påtaglig förändring på informationshanteringsområdet är den successiva centralisering som idag sker av framför allt it-drift och olika typer av standardiserade tjänster för informationshantering.

Inom den offentliga sektorn handlar det om allt från att lägga relativt standardiserade funktioner som personaladministration eller resehantering hos en yttre tjänsteleverantör till att avveckla betydande delar av den egna it-verksamheten och istället placera den hos en extern driftleverantör.

Utvecklingen kan betraktas som en slags återgång till sådan central datadrift som var vanlig under 1970- och 1980-talen. Under de senaste fem till sex åren har den tekniska utvecklingen lett till en betydande intern centralisering genom så kallad serverkonsolidering och virtualisering. Detta följs nu av tilltagande utkontraktering (outsourcing).

Utkontraktering kan ske i många former. En tydlig tendens i samhället är att verksamheter överger den tidigare utveckling och drift som skett av egna system till förmån för hyrda funktioner eller tjänster, något som introducerats med beteckningar som web services, software-as-a-service (SaaS) eller – på senare tid – molntjänster.

Det faktum att allt fler organisationer väljer att utkontraktera sin it-drift eller behandla och lagra sin information med användning av molntjänster, leder oundvikligen till en koncentration av informationsbehandlingen till ett mindre antal aktörer. Tanken är vanligen att den rationaliseringsvinst som uppstår vid stordrift kommer att leda till att den totala kundkostnaden för it-verksamheten minskar.

Det är möjligt att stordrift även kan leda till att informationssäkerheten hos många samhällsaktörer förbättras. Speciellt gäller det små organisationer utan egen specialistkompetens som genom utkontraktering får tillgång till den kompetens större driftleverantörer besitter. Det föreligger emellertid också en risk att informationssäkerheten nedprioriteras i den löpande verksamheten om det inte ställs explicita krav på rutiner, kontroller och åtgärder redan i upphandlingen.

Kraftigt centraliserad it-drift i samhället innebär också en koncentration av risk. Tieto-händelsen i slutet av 2011 illustrerar på ett

tydligt sätt konsekvenserna av denna koncentration vid ett längre driftavbrott. Samhällets sårbarhet ökar när flera kunder på en gång drabbas av ett enskilt driftsavbrott. MSB konstaterade i sin studie av samhällskonsekvenser efter denna händelse att det för offentlig sektor gäller att ställa tydliga krav på informationssäkerhet vid upphandling av it-drift.[5] Hos bland annat Kammarkollegiet pågår idag arbete med att förbättra förutsättningarna för upphandling av bland annat it-drift ur informationssäkerhetssynpunkt.

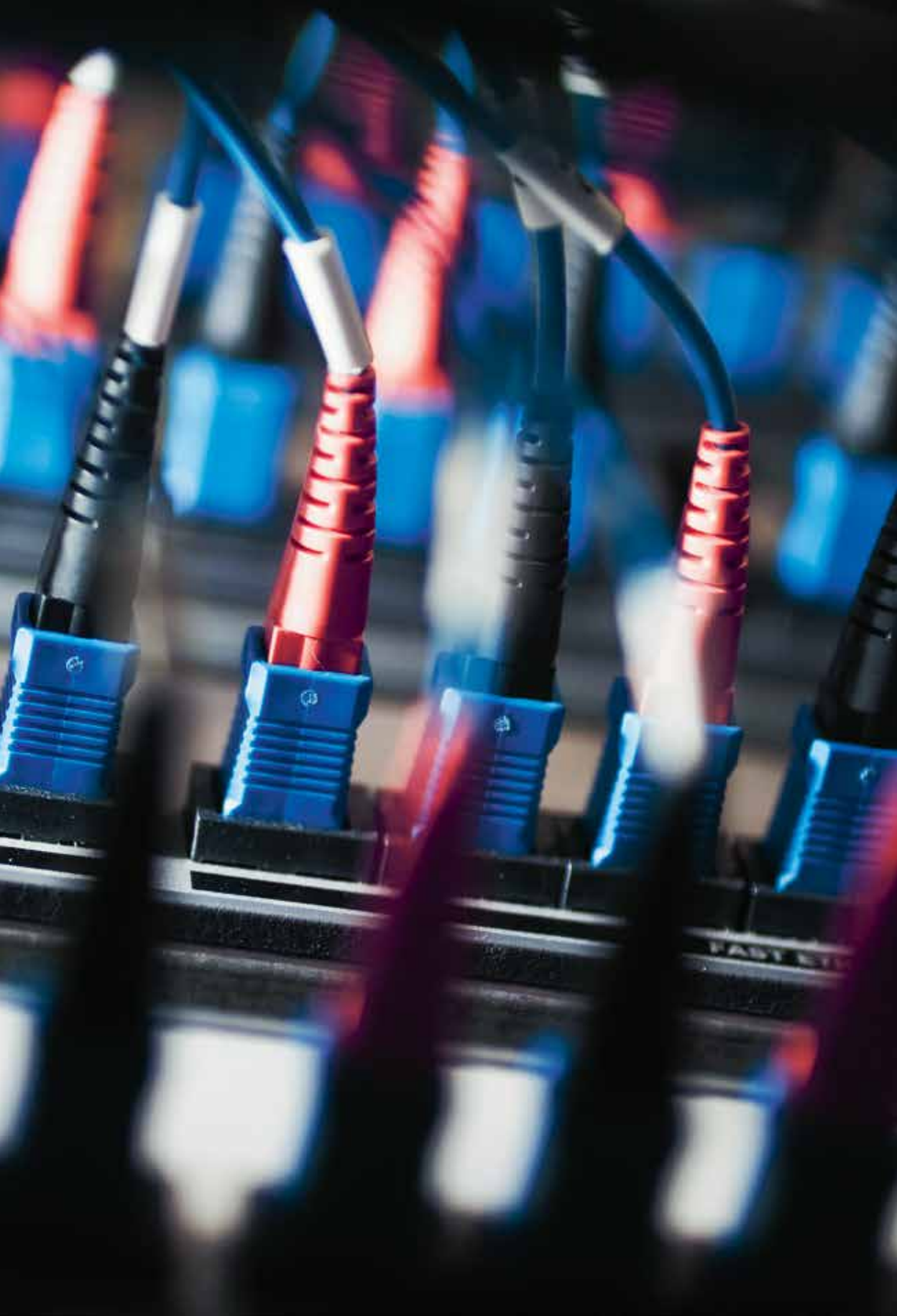
Samtidigt som outsourcingen av it-tjänster pågår i samhället växer också den systematiska datalagringen. Inom det offentliga skannar och lagrar myndigheter, landsting och kommuner stora mängder handlingar som sedan i digital form hamnar i system för ärendehantering eller fakturering. Inom vård och omsorg har det byggts storskaliga journalsystem som snart är tillgängliga för sjukvårdspersonal varhelst en patient behöver hjälp. Allt fler typer av information lagras under lång tid. Det handlar om kreditkortstransaktioner, flyg- och tågbiljetter, vilka varor vi köper i livsmedelsaffären och så vidare.

I vissa fall, till exempel hos myndigheter, styrs hanteringen av tydliga regelverk eller lagstiftning, i andra fall sker hanteringen friare och med avtalsrätten som grund.

I denna samhällsmiljö har begrepp som ”data mining”[6] och ”big data”[7] plötsligt blivit heta områden. Konsten att finna och filtrera fram rätt information blir värdefull, liksom möjligheten att producera relevant information ur annan information (informationsderivat).

Information vi dagligen hanterar kan lagras på andra håll i världen, och innehåller ofta kopplingar till många olika informationskällor. Många av de tjänster vi använder dagligen skulle upphöra att fungera utan sådan fjärråtkomst till information. Samhället har hittills enbart i begränsad omfattning hunnit anpassas till denna transformativa egenskap hos information, alltså möjligheten att på allt mer sofistikerade sätt utnyttja relationer hos information till annan information.

I detta sammanhang kan det europiska PSI-direktivet (Public Sector Information) få stor betydelse.[8] Direktivet behandlar möjligheten att vidareutnyttja allmänna handlingar i elektronisk form. Detta kan ge stora möjligheter att förbättra informationsförsörjningen i samhället, men också innebära risker om stora mängder information sammanställs och analyseras i syfte att kartlägga individer eller hitta sårbarheter i samhällssystem.



Ökande mobilitet och mobila plattformar

4. Ökande mobilitet och mobila plattformar

Den ökade mobila datakommunikationen är en global trend. Under 2011 såldes det fler smarta mobiltelefoner än persondatorer i världen.[9] Enligt en företrädare för Google aktiverades det i början av 2012 dagligen 850 000 Android-baserade smarta mobilterminaler och antalet sådana enheter uppgick vid samma tidpunkt till 300 miljoner.[10]

Utvecklingen i det svenska samhället har under de senaste åren som i resten av världen präglats av tilltagande mobil informationshantering. Den första mobilitetsvågen, som strax före millennieskiftet placerade digitala mobiltelefoner i händerna på en stor del av befolkningen i länder som Sverige, följs nu av en snabb spridning av ”smarta” mobiltelefoner (smartphones) och läsplattor. En betydande del av Sveriges befolkning har under de senaste tre till fyra åren fått tillgång till sådana mobila handenheter för datakommunikation. Det är enheter som vid sidan av röstsamtal och kortmeddelanden även ger tillgång till internet och tjänster som e-post och webbkommunikation. Det ökade antalet smarta mobiltelefoner och läsplattor i världen har inneburit att de numera utgör ett intressant mål för utvecklare av skadlig programkod. Det finns flera tillvägagångssätt för att infektera dessa enheter. Ett är att använda populära sociala nätverkstjänster som kanal för att locka användare till en viss webbplats där användaren luras att installera skadlig kod.[11]

Under de senaste åren har en betydande del av internettrafiken flyttat från fasta nätförbindelser till mobila. En konsekvens av detta har blivit att tillgängligheten i de radioburna segmenten av mobilnäten idag riskerar minska, åtminstone i det korta perspektivet, till följd av omfattande användning av bandbreddskrävande tjänster som strömmande video och tjänster med omfattande signalering.

Det bör emellertid betonas att större delen av den samlade globala datatrafiken fortfarande skickas genom fasta förbindelser (kopparkabel och fiber) och detta förhållande väntas bestå.

Utvecklingen inom området användarmobilitet innebär en ny typ av riskexponering när utrustning som tidigare fanns på arbetsplatsen nu i ökande omfattning följer med användaren och riskerar bli stulen eller tappas bort. De bärbara enheterna, exempelvis smarta mobiltelefoner, läsplattor, Minnesstickor och liknande, innehåller allt

större mängder information men saknar ofta samma typer av åtkomstskydd som utvecklats för de utrustningar som är fysiskt knutna till arbetsplatsen.

Utvecklingen kan på sätt och vis liknas vid förändringen för något decennium sedan då bärbara datorer fick vidare spridning och det började ställas krav på informationsåtkomst även utanför de fasta företagsnäten. Detta är en utmaning, eftersom säkerhetsåtgärder kan visa sig svåra att vidmakthålla i en miljö med utrustning som informationsägaren saknar administrativ kontroll över.

Denna svaghet börjar bli besvärande idag, i takt med att smarta mobiltelefoner och läsplattor i allt större utsträckning används både privat och i arbetet. Fenomenet, som internationellt går under beteckningen BYOD (eng. ”bring your own device”) har nyligen pekats ut som en av de trender som kraftigt kommer att påverka it-området under de närmaste åren. Men när användare ges åtkomst till arbetsrelaterad information via sina privata, mobila enheter kommer skyddet av verksamhetens informationstillgångar enkelt uttryckt att hänga på hur duktiga dessa användare är på att skydda sig själva.

Att tillåta privata smarta mobiltelefoner i tjänsten kan leda till en ny typ av riskexponering för organisationer, bland annat därför att många tillämpningar (”appar” eller motsvarande) idag begär omfattande åtkomst till enhetens interna funktioner. För att kunna installera dem måste användaren i allmänhet tillåta sådan åtkomst.

Frågan om användning av ”smarta” mobiltelefoner i tjänsten har under de senaste två åren varit en flitigt diskuterad fråga bland såväl myndigheter som företag.[12]

Vissa organisationer skyddar redan idag sina egna mobila utrustningar med såväl tangentlåsning och lösenordsskydd som med kryptering av innehållet och möjlighet till fjärrstyrning och fjärradering av hela enheten. Många större organisationer skaffar sig också färdiga system för smidig administration av de mobila enheterna i stora användarpopulationer.[13]

Identitetshantering

5. Identitetshantering

Möjligheten att säkerställa identitet (autentisering) är ett grundläggande krav i modern informationshantering och elektronisk kommunikation. På detta område börjar tekniken fungera tillfredsställande idag. I många sammanhang används dock fortfarande enkla lösenord eller PIN-koder för att identifiera användaridentitet eller användarroll, till exempel vid inloggning i företagsnät, åtkomst till epostkonton och liknande.

För åtkomst till och hantering av känslig information, till exempel för att genomföra transaktioner på internetbanker, krävs det emellertid bättre identitetskontroll. Här används företrädesvis så kallad tvåfaktorautentisering. Denna autentisering sker med hjälp av exempelvis ett smartkort, en kryptodosa eller genom att ett engångslösenord skickas till användarens mobil.

Utvecklingen på detta område går framåt och allt fler stora organisationer använder tvåfaktorsautentisering för inloggning. På vissa samhällsområden och myndigheter finns det väl utbyggda infrastrukturer. Det gäller inom myndigheter som Polisen, Skatteverket och Försäkringskassan, som hanterar stora mängder integritetskänslig och sekretessbelagd information.

Inom vård- och omsorgssektorn har smarta kort för inloggning, så kallade SITHS-kort, idag utfärdats till uppåt en halv miljon användare inom vård och omsorg. Därmed har ett viktigt steg tagits för att skydda åtkomsten till information i system som Nationell patientöversikt (NPÖ) och Läkemedelsförteckningen.

För medborgare har några aktörer sedan länge utfärdat så kallade e-legitimationer, som används för att få åtkomst till bland annat internetbanker och offentliga e-tjänster. När det gäller medborgarnas möjligheter att identifiera sig på ett säkert sätt genom e-legitimation har utvecklingen under en följd av år drivits framåt av bland andra Skatteverket. Idag har det lett till att en relativt stor andel av landets befolkning använder sig av e-legitimation. Till exempel deklarerade runt 1,5 miljoner personer med hjälp av e-legitimation under 2012.[14] Ett stort antal använder också de självservicefunktioner som finns för att till exempel hantera företagsärenden gentemot Skatteverket och Bolagsverket.

Sveriges kommuner och landsting, SKL, har identifierat 38 typiska e-tjänster som kommuner tillhandahåller.[15] Det rör sig uteslutande om olika typer av anmälningar och ansökningar som en medborgare kan göra via kommunens webbplats. I en enkätundersökning genomförd av SKL, svarade 82 procent av kommunerna att de tillhandahåller minst en av de 38 definierade e-tjänster som använts i enkäten, men många kommuner tillhandahåller sannolikt ett stort antal av dessa tjänster.

Samtidigt är det tydligt att kraven på säkerhet vid autentisering av medborgare skiljer sig markant mellan kommunerna. Lösningar för autentisering genom exempelvis Bank-ID är betydligt vanligare förekommande hos större kommuner än hos små. Användningen minskar proportionellt mot kommunstorleken. Tendensen är densamma när det gäller förekomsten av lösningar för identifiering och autentisering av företag och privata utförare.

Enbart 16 procent av landets kommuner med mindre än 10 000 innevånare har infört eller står i begrepp att införa lösningar för identifiering och autentisering av medborgarna.

Den statliga E-legitimationsnämnden har givits i uppdrag att driva utvecklingen av e-legitimationer vidare. Nämndens uppgift är att stödja och samordna offentliga sektorns behov av säkra metoder för elektronisk identifiering och signering, ett arbete som får betraktas som mycket viktigt för att e-samhället på sikt ska fungera tillfredsställande ur ett informationssäkerhetsperspektiv. Arbetet baseras på en decentraliserad modell för sammanlänkning av olika privata och offentliga infrastrukturer för identifiering, så kallad federation. Under 2013 väntas federationsmodellen även kompletteras med ett valfrihetssystem som redan på kort sikt kommer att öppna marknaden för nya aktörer och tjänstelösningar.


286 711

Sociala nätverkstjänster och personlig integritet

6. Sociala nätverkstjänster och personlig integritet

Sociala nätverkstjänster används i bred utsträckning i samhället. Facebook är för närvarande den dominerande aktören på marknaden med drygt 960 miljoner användare i världen.[16] En stor del av den svenska befolkningen använder idag tjänster av detta eller liknande slag.[17]

Den höga aktiviteten medför att leverantörerna av sociala nätverkstjänster idag lagrar och har tillgång till stora mängder användarinformation och ett brett spektrum av personuppgifter. Informationen hanteras enligt avtal mellan leverantör och användare. Risken finns dock att denna information kan användas på sätt som användaren inte tänkt sig vilket kan få negativa konsekvenser för bland annat den personliga integriteten.

För att komma till rätta med bland annat ovanstående fråga lämnade Europeiska kommissionen i början på 2012 ett förslag på en omfattande reformering av EU:s regler om dataskydd med syftet att stärka integritetsskyddet på internet.[18] Bland annat föreslås en förändring av ansvaret för att efterleva säkerhetskraven vid behandling av personuppgifter.

Användandet av sociala nätverkstjänster kan innebära en utmaning för organisationen om till exempel offentliganställda i egenskap av privatpersoner använt sociala nätverk på sätt som inte bedömts vara lämpligt i förhållande till fastställda regelverk och praxis. Under de senaste åren har det noterats åtskilliga sådana fall, till exempel då sjukvårdspersonal har kommenterat eller publicerat bilder av patienter eller en polis bloggat om en pågående förundersökning. Existerade regelverk som offentlighets- och sekretesslagen, brottsbalkens bestämmelser om förtal samt hälso- och sjukvårdslagen kan tillämpas för vad och hur man kan uttrycka sig i sociala nätverkstjänster. Utöver detta har Datainspektionen både genom rekommendationer och utlåtanden kring särskilda fall givit riktlinjer.

De stora globala leverantörerna av sociala nätverkstjänster kan i vissa situationer spela en mycket viktig roll som förmedlare av information mellan människor och organisationer. Till exempel har flera kommuner under det senaste året använt tjänster som Facebook

och Twitter för att kommunicera med sina medborgare vid tillfällen då den egna webbplatsen eller telefonväxeln inte fungerat. Ett stort antal företag och statliga myndigheter använder dessutom Facebook som en kompletterande kanal till sin webbplats för att nå ut till sina respektive målgrupper med sina budskap.[19]

I de flesta fall är det den enskilde individen som frivilligt använder sociala nätverkstjänster i kontakt med myndigheter. Situationen blir emellertid en annan då ett företag eller en myndighet gör tjänster av detta slag obligatoriska. Det kan handla om kundtjänstfunktioner eller medborgarportaler där man till exempel uppmuntrar till lagring av personuppgifter för förbättrad service inom vård- och omsorgssektorn. I dessa fall krävs särskilda överväganden.

Den personliga integriteten påverkas även i hög grad av den allt större koncentrationen av personuppgifter i myndigheters och företags it-lösningar. Flera länder har redan lagstiftat om obligatorisk, offentlig rapportering av ”informationsläckage” (data breach) och i vissa fall även straffbelagt sådan spridning.[20] Under de senaste åren har det rapporterats om oönskad spridning av stora mängder personuppgifter i bland annat USA[21], Storbritannien[22] , Israel[23] och Grekland[24]. I Sverige har det under 2012 utretts ett dataintrång hos en underleverantör till en myndighet, där man misstänker att en stor mängd känsliga uppgifter ur ett befolkningsregister hamnat i orätta händer.[25]

Det datoriserade informationsutbytets stora omfattning i samhället, inte minst inom och mellan centrala myndigheter samt inom sektorn vård och omsorg, samt den alltmer omfattande utkontrakteringen av it-drift innebär att risken för okontrollerad spridning av information sannolikt kommer vara fortsatt stor under kommande år.

Säkerhet i industriella styrsystem och inbyggda system

7. Säkerhet i industriella styrsystem och inbyggda system

Informationssäkerhet är inte ett område som enbart berör myndigheter, företag och andra organisationer som förvaltar stora datalager, transaktionssystem, affärssystem eller system för ärendehantering. Under det senaste decenniet har ökat intresse riktats mot de informationssäkerhetsrelaterade risker som kan kopplas till teknisk infrastruktur och informationshantering som direkt påverkar exempelvis trafikstyrning, industriproduktion och eldistribution. Detta är ett område som har fått samlingsnamnet industriella informations- och styrsystem[26], eller i vissa sammanhang SCADA-system.[27]

Sådana styrsystem finns numera i de flesta större tekniska infrastrukturer, och styr till exempel överföringen av elkraft i samhället, järnvägssignaleringen och värmeregleringen av våra bostäder.

Att industriella styrsystem är sårbara för elektroniska angrepp och nätangrepp har varit välkänt länge bland dem som arbetar med dessa system. Risken för att sådana oönskade händelser inträffar har dock ökat under senare år och kommer sannolikt att öka ytterligare under det kommande årtiondet. Det sker i takt med att allt fler styrsystem som tidigare utgjort isolerade system eller öar av system nu kopplas ihop med exempelvis administrativa stödsystem och därmed direkt eller indirekt också till internet.

Upptäckten av Stuxnet sommaren 2010 var en händelse som på allvar fick igång en bred samhällsdiskussion kring sårbarheter i industriella styrsystem. Stuxnet var en skadlig programkod som av allt att döma utgjorde en riktad attack mot styrsystem i en iransk kärnkraftsanläggning. Koden representerade det första publika exemplet på en avancerad och välplanerad attack mot ett styrsystem i samhällsviktig verksamhet. Stuxnet har redan fått efterföljare, och eftersom attackmetodiken studerats på djupet bland it-säkerhetsexperter i hela världen finns det anledning att befara en successiv spridning av liknande angrepp.

Angrepp mot styrsystem kan i vissa fall resultera i betydande samhällskonsekvenser i form av exempelvis längre försörjningsavbrott.

Detta kan ställas mot effekterna av tillgänglighetsattacker mot webbplatser, som ofta är temporära till sin natur och skapar uppmärksamhet snarare än konkreta, bestående skadeeffekter.

Den ökade uppkopplingen av moderna styrsystem, allt från mindre system för reglering av hushållens elförbrukning till stora vattenkraftverk, mot internet ger upphov till sårbarheter som inte fanns tidigare. Vad som kan hända när ett sådant styrsystem blir nåbart utifrån fick vi se i Sverige i slutet av 2010, då någon lyckades ta sig in hos ett svenskt fastighetsbolag och ändrade inomhustemperaturen i ett helt fastighetskomplex.[28] Liknande exempel finns också runt om i världen.

För något år sedan uppmärksammades hur en sökmotor numera gör det möjligt att söka efter kända sårbarheter i industriella styrsystem. Forskare har även påvisat möjligheten att via samma sökmotor identifiera styrsystem, som är länkade till internet och därmed kan vara sårbara för angrepp över internet.

Att allt fler styrsystem numera direkt eller indirekt går att nå från internet har inneburit en riskglidning. Men det finns även andra vägar att nå styrsystemen. Flera tillverkare börjar idag göra det möjligt att nå, konfigurera och felsöka systemen över trådlösa nätverkslänkar (wifi eller motsvarande) vilket ökar möjligheterna att angripa dem. Många styrsystem konstruerades dessutom ursprungligen för att verka i helt isolerad miljö, och har därefter byggts ut successivt med fokus på ökade funktioner snarare än säkerhet. Det har lett till att kommunikationen i många fall fortfarande sker i klartext och via enkla terminaluppkopplingar. Här finns ett stort, hittills inte tillräckligt kartlagt, område av samhällsrisker.

Ett teknikområde som fram till för några år sedan fortfarande befann sig på forskningsstadiet är smarta elnät[29] där nätelement och abonnentutrustningar går att läsa av och styra på distans. En del av denna företeelse har sin upprinnelse i behovet av bättre kontroll över den kraftigt fragmenterade elmarknaden i framför allt Nordamerika, men även i miljöhänseende i Europa. Visionerna har emellertid utvecklats till något betydligt bredare, som innefattar såväl laststyrning i större skala som möjlighet till individuell reglering på såväl abonnentnivå som (på sikt) i enstaka elförbrukande utrustningar.

Idag har teknik lyfts ut från laboratorierna, vilket bland annat lett till storskalig installation av smarta elmätare som går att läsa av på

håll eller centralt hos eldistributören. Sådana finns nu allmänt bland företag och hushållsabonnenter i Sverige. Dessa elmätare väntas framöver att bli allt mer avancerade.

Parallellt med utvecklingen av smarta elnät pågår även forskning kring smarta städer, där man försöker integrera olika typer av informationskällor och sensorer i stadsmiljö. Det handlar exempelvis om att använda fastighetsautomationens möjligheter på nya sätt, att koppla ihop informationssystem i fordon med information i gatunät och trafikstyrning – och naturligtvis länka ihop den teknik som tas fram för en intelligent stadsmiljö med tekniken för smarta elnät.

Båda dessa områden kommer naturligtvis att behöva studeras ur informationssäkerhetsperspektiv. Fortfarande finns det inte standardiserade vägar för att kommunicera, hämta och lämna information, i elnät eller ”stadsmiljö”. Men även om dessa metoder etableras återstår ett mycket komplicerat arbete med att säkerställa stabiliteten hos de infrastrukturer som berörs och på olika sätt förhindra att felaktig information leder till olyckor. Dessa teknikområden befinner sig fortfarande i stora stycken på forsknings- och utvecklingsstadiet, och från samhällets och andra aktörers sida handlar det nu därför främst om att fortsätta stödja den forskning som sker på området med anknytning till säkerhet och stabilitet.

Ett anknutet område är maskin-till-maskinkommunikation (M2M). Det började utvecklas redan före millennieskiftet, men har först under den allra senaste tiden börjat uppmärksammas på allvar. Enkelt uttryckt handlar det om att förse utrustning som redan idag innehåller inbäddad datorkraft med kommunikationsmöjligheter, till exempel för att rapportera användning, försäljning, driftstatus, geografisk position och liknande till användaren, tillverkaren eller en serviceorganisation. Detta område, där tillämpningar kan sjösättas i relativt liten skala, kan få betydligt snabbare genomslag än områdena smarta elnät och smarta städer som snarare är omfattande infrastrukturer.

Säkerhet är viktigt även i maskin-till-maskinkommunikation. Om en bil, en kopiator-skrivare eller en varuautomat förses med en GSM-modul som kan larma ägare eller verkstad vid exempelvis servicebehov så finns det vanligen också en motriktad länk som kan användas för att koppla upp sig mot utrustningen och eventuellt styra eller programmera om den.

Även inom larmkommunikation används liknande teknik redan idag, med till exempel trygghetslarm som vid larmsignal automatiskt kopplar upp en fast eller styrbar kamerabild inifrån den berörda personens hem. I en sådan tillämpning behöver det givetvis finnas en säkerhetsmekanism på plats som förhindrar obehörig uppkoppling.

Maskinkommunikationen förefaller vara en naturlig ny fas i internetutvecklingen. Men den säkerhetsproblematik tekniken för med sig behöver emellertid studeras ytterligare. Ovanstående exempel belyser dessutom behovet av att studera den nya tekniken ur juridiskt perspektiv.

Skadlig kod och skräppost

8. Skadlig kod och skräppost

Skadlig kod (datavirus, maskar, trojaner och liknande) kan drabba alla delar av samhället, och har under det senaste decenniet vid upprepade tillfällen slagit ut verksamheten hos bland annat hela kommunförvaltningar i Sverige. Vid några tillfällen har betydande delar av de drabbade kommunernas it-stöd upphört att fungera i en vecka eller mer.

Under 2011 skapades 403 miljoner varianter av skadlig kod, vilket är en ökning med drygt 40 procent jämfört med 2010.[30] Trojaner fortsätter att bli allt vanligare, till skillnad från maskar och virus där det idag sker en minskning. Vid drygt 60 procent av infektionerna med skadlig kod utgörs koden av trojaner, medan virus och maskar utgör knappt 8 procent vardera.[31]

Skadlig kod görs ofta plattformsoberoende idag och det sker allt fler angrepp mot webbplattformar och publiceringssystem (content management systems). Ransomware (utpressningsprogram) är en trojantyp som blivit vanlig. När sådan kod har infekterat en utrustning hindras användaren att utnyttja utrustningen på vanligt sätt innan det betalats en lösensumma. En kommun i Skåne utsattes för detta våren 2012.[32] Banktrojaner är en annan variant av skadlig kod som blivit vanlig under det senaste året. Här angrips kommunikationen mellan användare och internetbank.

Den stora försäljningsökningen av mobila enheter har medfört att smarta mobiler och läsplattor numera blivit attraktiva för brottslingar att angripa. Antalet kända angrepp har också ökat kraftigt under 2012. Den största andelen av dessa angrepp riktade sig mot Android-plattformen.[33] Till skillnad mot skadlig kod riktad mot datorer, kan den skadliga koden i smarta mobiler även syfta till att spåra användarnas position.

I genomsnitt beräknas drygt en tredjedel av världens datorer med internetuppkoppling vara infekterade av skadlig kod. Det är knappt 10 procentenheter färre än under 2010. Kina fortsätter att vara det land som är mest infekterat. Där är andelen drygt 54 procent. Andelen smittade datorer är generellt lägre i Europa. I Pandalabs undersökning[34] över första kvartalet 2012 är nio av de tio länderna

med lägst andel infekterade datorer från Europa. Japan är det enda landet utanför Europa på listan och Sverige innehar första platsen med mindre än 20 procent infekterade datorer.

I Sverige har den nationella it-incidentfunktionen vid MSB, CERT-SE, utvecklat en tjänst där det går att se var det finns infekterade datorer runt om i landet. Runt 50 000 infekterade IP-adresser per månad är normalt.[35]

Skräppostproblemet håller på att förändras idag. Antalet skräppostmeddelanden minskade under 2011 med 34 procent samtidigt som det skedde en ökning av så kallad social spamning, alltså spamning via sociala medier. Från den hittills högsta noteringen i augusti 2010 på drygt 92 procent av alla epostmeddelanden hade andelen skräppost gått ned till drygt 70 procent i november 2011.[36] Nedgången bedöms bland annat bero på förbättrade filter och att brottsbekämpande myndigheter lyckats ta ned flera stora botnät, i synnerhet världens största botnät för skräppost, Rustock.[37]

Istället har skräpposten i nya former dykt upp i sociala medier som Facebook och Twitter, något som går under benämningen social spamning. Fördelen för de kriminella elementen med att utnyttja sociala media är att de kan sprida sina meddelanden via en kedja av betrodda källor där benägenheten hos mottagarna att agera ökar i linje med vad förövaren vill.

Sårbarheter i programvaror har blivit en strategisk resurs idag. Tidigare okända och icke åtgärdade sårbarheter (sk. zero-day vulnerabilities) kan numera framställas automatiserat och i industriell skala. Därmed ökar möjligheten att tjäna stora pengar på dem, vilket leder till att idealister och ”amatörforskare” på området ersätts av professionella aktörer med större resurser och siktet inställt på att sälja sårbarheterna. Tidigare var det normalt att först underrätta tillverkaren om en sårbarhet och ge denne möjlighet att åtgärda felet innan information publicerades öppet. Nu är trenden istället att sårbarheter i ökad omfattning hemlighålls och säljs till kunder med kriminellt, kommersiellt eller säkerhetspolitiskt motiverat intresse av att förfoga över ”egna” bakdörrar till it-system. Det omfattande informationsutbytet inom it-säkerhetsindustrin har redan börjat minska, till nackdel för dem som arbetar med att bygga skydd, analysera och ta fram hotbilder. Följden av detta är en kapprustning som det blir allt svårare att skydda sig mot. Utvecklingen förväntas fortgå i denna riktning.

It-relaterad brottslighet

9. It-relaterad brottslighet

Den it-relaterade brottsligheten är ett globalt fenomen idag. Den är en utmaning för såväl samhället som för företag inom bland annat finanssektorn som drabbas av kännbara kostnader. Verksamheten hos de traditionella, brottsbekämpande myndigheterna världen över har haft svårt att komma tillrätta med den växande it-relaterade brottsligheten. Detta har flera orsaker, bland annat skillnader i bevisbörda, nationell tillämplig lag och organisationsstrukturer.

En intressant följd av detta är att Microsoft idag skapat en egen ”cyber crime unit” för att stödja brottsbekämpningen inom området. Denna enhet fokuserar primärt på bekämpning av skadlig kod respektive utnyttjande av barn. Microsofts it-brottsenhet har deltagit i några nedtagningar av botnät och de kriminella organisationerna bakom dem. Arbetet har skett i nära samarbete med bland annat FBI och amerikanska domstolar. Vid ett ingripande i slutet av mars 2012, när ett flertal Zeus[38]-botnät togs ned, var Microsoft även fysiskt på plats och deltog vid beslaget.[39]

Även om de flesta aktörer menar att slutresultatet varit positivt kan man fråga sig huruvida det är lämpligt att privata företag agerar som en del av rättsväsendet.

Den it-relaterade brottsligheten fortsätter att skapa rubriker, men det är samtidigt vanskligt att ge några bestämda besked om dess totala omfattning och dess faktiska samhällskostnader. BAE Detica bedömde att kostnaden för it-relaterad kriminalitet i Storbritannien uppgår till 29 miljarder brittiska pund (GBP)[40], Symantec uppskattade den globala kostnaden för immaterialrättsbrott till 250 miljarder dollar (USD) och chefen för den amerikanska säkerhetsmyndigheten NSA, Keith Alexander, hävdade att den globala kostnaden för it-relaterad brottslighet uppgår till 1000 miljarder dollar (USD) årligen.[41]

Det brittiska försvarsdepartementet uttryckte en viss skepsis gentemot kostnadsuppskattningarna och gav en forskningsgrupp från Cambridge i uppdrag att analysera kostnaderna för it-relaterad brottslighet. Den rapport forskningsgruppen publicerade under sommaren 2012 ger inget entydigt svar utan belyser snarare svårigheten att kategorisera och estimera kostnaderna för it-relaterad brottslighet.[42] Det beror

bland annat på att mörkertalet är stort, att kostnaden för immaterialrättsbrott är väldigt svår att uppskatta och att det är oklart i vilken omfattning traditionell brottslighet idag ska kategoriseras som it-brottslighet enbart därför att den ”flyttat ut på nätet”.

Rapporten pekar dock på att en kraftig majoritet av kostnaderna härstammar från vad som går under benämningen traditionell brottslighet och framförallt traditionell brottslighet som numera utförs med hjälp av it. Den första kategorin utgörs bland annat av kostnader för olika former av kortbedrägerier medan kategori två innefattar skattebedrägerier. Genuina it-relaterade brott, som innehåller olika former av internetbankbedrägerier, phishingattacker, utnyttjande av skadlig kod och falska antivirusprogram, utgör enligt rapporten en avsevärt mindre del av kostnaden. Rapporten behandlar inte kostnaden för immaterialrättsbrott.

Antalet anmälda it-brott i Sverige ökar. Preliminära siffror från BRÅ visar att under 2011 anmäldes 3 593 dataintrång och 41 så kallade datasabotage enligt 4 kap 9c§ brottsbalken (1962:700) (BrB). Det är en ökning med 52 procent jämfört med föregående år.

Man kan jämföra med situationen i Norge, där den så kallade mörkertalsundersökningen 2012[43] visade att det 2011 anmäldes endast 361 fall av dataintrång, bedrägerier, missbruk av it-resurser, informationsstöld och spridning av upphovsrättsligt skyddat material medan antalet brott av dessa slag uppskattades till närmare 45 000.

Dataintrången har också ändrat karaktär. Från att tidigare främst rört intrång gjorda av anställda vid sjukhus eller hos polisen i form av olovliga slagningar i register, har det skett en ökning av anmälda intrång hos privatpersoner, t ex i form av kapade mejlkonton och Facebook-konton.[44]

Det står också klart att it-utvecklingen på senare år inneburit en rad nya arbetsuppgifter för polisen såväl i Sverige som i andra länder. Brott som dataintrång, nätbedrägerier och internetförtal kräver ny utredningsmetodik. Dessutom behöver stora mängder it-utrustning innehållsgranskas idag i samband med brottsutredningar. Det är en arbetsbörda som ständigt ökar i takt med att mängden data som ska granskas ökar och genom att vissa kategorier brottslingar utnyttjar allt mer avancerade metoder för att dölja sin verksamhet.

För att upprätthålla förtroendet för rättsväsendets funktion i denna nya miljö är det nödvändigt att hela den brottsutredande delen av rättskedjan har tillgång till den specialistkompetens och de resurser som krävs. Den ofta gränsöverskridande karaktär som dessa brott har innebär dessutom att det krävs en utvidgad internationell samverkan inom brottsbekämpningen. Här har dock viktiga initiativ tagits under 2011 och 2012 på EU-nivå, bland annat genom att ett särskilt, EU-gemensamt organ för it-relaterad brottsbekämpning (EC3) har etablerats vid Europol.

Särskilda händelser

10. Särskilda händelser

10.1 Certifikatproblem för SSL

Säkerhetsmekanismen SSL används för att kryptera kommunikationen mellan användare och exempelvis banktjänster, myndigheter och webbhandelsplatser. SSL utgör därmed en viktig beståndsdel för säkerheten och förtroendet för bland annat internethandeln. Certifikatutfärdare för SSL, men även SSL självt, har blivit utsatt för ett flertal olika angrepp under 2011. Under sommaren 2011 framkom det att den holländska certifikatutfärdaren DigiNotar fått rotcertifikat komprometterade, till följd av dataintrång på grund av bristande rutiner och säkerhetsmedvetande.

Intrånget upptäcktes sedan en datoranvändare i Iran upptäckt en felaktighet vid anslutning till en google-tjänst. Det visade sig sedan att ett stort antal internetdomäner drabbats av att någon utfärdat falska certifikat i Diginotars namn. Det handlade bland annat om välkända domäner som google, yahoo och skype (.com) men även flera underrättelsetjänsters webbdomäner.

Diginotar tillverkade certifikat kommersiellt, men ansvarade också för utfärdandet av myndighetscertifikat i Nederländerna. It-intrånget medförde därmed att det inte längre gick att lita på nederländska myndigheters webbplatser. Den nederländska staten valde att inte återkalla certifikaten, bland annat då det skulle kunna ge upphov till onödiga störningar i vissa tjänster. Incidenten fick följden att DigiNotar gick i konkurs och den nederländska staten tog över företaget. Intrånget hos DigiNotar var måhända den mest uppmärksammade incidenten som berörde certifikatutfärdare och SSL under 2011 men utöver Diginotar angreps även en partner till certifikatutfärdarna Comodo och GlobalSign. Under en säkerhetskonferens i september demonstrerade två forskare hur det var möjligt att via deras ”konceptverktyg” BEAST (”Browser Exploit Against SSL/TLS”) utnyttja sårbarheter i krypteringen som används av SSL/TLS.[45]

Reflektion

Att den teknik som används för att utfärda äkthetscertifikat till webbplatser är känslig har varit känt under en längre tid. Det finns idag drygt 600 olika företag som agerar som centrala certifikatutfärdare, och det finns risker förknippade med en sådan mångfald av äkthetsintyg. Många tekniska bedömare betraktar redan den

PKI-struktur (”public key infrastructure”) som används som otillförlitlig och en återvändsgränd. Skulle det visa sig att ytterligare falska webbplatscertifikat inom kort kommer i omlopp så skulle det på sikt kunna minska tilltron till dataintegriteten hos ett stort antal webbtjänster i världen som förlitar sig på SSL. Det arbetas emellertid på lösningar. En av dem är att transportera certifikat via domänsystemet DNS, en metod som håller på att standardiseras av arbetsgruppen DANE inom internets standardiseringsorganisation IETF.

10.2 RSA, osäkra säkerhetsdosor

I mitten av mars 2011 gick säkerhetsföretaget RSA ut i ett öppet brev till sina kunder och informerade om att de hade blivit utsatta för ett sofistikerat it-angrepp. Det fanns risk att information som potentiellt kunde påverka säkerheten i RSAs säkerhetsprodukt SecurID, som bland annat används i nyckelbricksliknande kryptodosor för säker inloggning, hade läckt ut från företaget.[46] I synnerhet formuleringen om att ”viss information är specifikt relaterad till RSA SecurID två-faktorsautenticeringsprodukter”[47] ledde till spekulationer om intrångets magnitud.

RSA SecurID är en vanlig säkerhetsprodukt med över 30 000 kunder i världen, varav åtskilliga även i Sverige. Företagets kryptodosor används ofta i system där det ställs höga krav på säker inloggning, eller för vissa användare med omfattande rättigheter i ett företagsnät, till exempel nät- och systemadministratörer.

Attacken genomfördes på så vis att angriparen skickade phishing-epost med rubriken “2011 Recruitment Plan.” till två olika grupper av anställda.[48] När sedan en anställd klickade på ett medföljande kalkylblad installerades en bakdörr. Därefter installerade angriparen ett fjärrstyrt administrationsverktyg gjorde det möjligt att fjärrstyra maskiner och nå servrar i RSA:s nätverk.

För att kompromettera en RSA SecurID-enhet behöver angriparen ha tillgång till information om kryptodosa, användarinformation och offrets PIN-koder. Om angriparen inte förfogar över dosan rent fysiskt krävs istället tillgång till sådan information som används för att generera nycklar. En av de många frågorna som florerade i bloggar och artiklar, och som förblev obesvarad, var huruvida angriparen lyckats få tag på dessa under angreppet.

I juni 2011 erbjöd RSA gratis säkerhetsövervakning till alla sina kunder eller utbyte av samtliga dosor.

Reflektion

RSA-intrånget är intressant ur flera aspekter. Det visar inte minst att riktade angrepp och metoden att dupera användare med lockande budskap har förutsättningar att lyckas även i miljöer där man borde vara extra vaksam – som i ett säkerhetsföretag. Angreppet visar också att it-angrepp kan påverka en hel tekniknisch. Många av RSA:s kunder fick i all hast fundera över kompletterande eller alternativa inloggningsmekanismer när det visade sig att ett av säkerhetsbranschens mest väletablerade företag råkat illa ut. De som drabbades visade sig dessutom i många fall vara nyckelfunktioner inom sina respektive organisationer.

10.3 Händelseutvecklingen efter Stuxnet

Den stora it-säkerhetshändelsen under 2010 var Stuxnet, en avancerad skadlig kod som förmodas ha utvecklats med målet att angripa industriella styrsystem i Iran.[49] Stuxnet upptäcktes under sommaren 2010 och gav under det följande halvåret upphov till omfattande teknisk analys och flera rapporter från olika aktörer inom säkerhetsindustrin. Koden beskrivs ofta som en ögonöppnare för vad som praktiskt är möjligt och man började särskilt i relation till angrepp mot samhällsviktig verksamhet prata om it-angrepp och skadlig kod före och efter Stuxnet. Bland it-säkerhetsexperter spekulerades det i vilken typ av efterföljare Stuxnet skulle få.

Drygt ett år senare, i oktober 2011, upptäckte ett ungerskt forskningslaboratorium en ny skadlig kod, som de kallade Duqu. Den innehöll delar som var nästa identiska med Stuxnet vilket medförde att många antog att utvecklarna bakom Duqu haft tillgång till källkoden till Stuxnet. Syftet med Duqu verkade däremot vara ett helt annat. Medan Stuxnet var självreplikerande och innehöll en nyttolast (payload) för att angripa noggrant definierad maskinvara verkade Duqu istället utformat för att samla in underrättelser om vad man förmodar är ett okänt industriellt styrsystem. Upptäckten av Duqu satte ny fart på spekulationerna kring Stuxnets spridningseffekter.

Drygt ett halvår senare, i maj 2012, var det dags igen. Då upptäcktes ytterligare en skadlig kod som verkade byggd för att samla in information och som hade vissa kodsegment gemensamma med Stuxnet. Koden fick beteckningen Flame. Den utmärkte sig bland annat genom att vara betydligt större än såväl Stuxnet som Duqu. Dessutom spred sig Flame på ett nytt sätt, genom att förklä sig som uppdateringsprogrammet för Windows.

En kort tid efter upptäckten av Flame, i juni 2012, dök det upp ytterligare en skadlig kod med likartad karaktäristik. Den fick namnet Gauss. Den mest notabla förändringen bestod i att Gauss innehöll krypterade delar, vilket har försvårat analysen av koden. Detta innebär att man fortfarande inte har kunnat slå fast vilket syfte koden har eller hur den i alla delar är tänkt att fungera. Dessutom stal den bankuppgifter och inloggningsuppgifter till sociala nätverk. Det senare skulle kunna peka på på att tekniken nu spridit sig från säkerhetspolitiskt motiverade aktörer till kriminella aktörer. Samtidigt spred sig Gauss huvudsakligen i Mellanöstern,[50] vilket skulle kunna tolkas som att det fortfarande fanns ett säkerhetspolitiskt syfte bakom koden.

Reflektion

Upptäckten av Stuxnet innebar att it-industrin och världen i stort under hösten 2010 på allvar fick upp ögonen för att riktade hot mot industriella styrsystem inte är en tänkbar utveckling, utan faktiskt utgör en konkret risk. Efterföljarna under de kommande åren bekräftar denna bild. Gemensamt för dessa angrepp är att de varit mer eller mindre riktade mot specifika systemmiljöer eller mot geografiska områden. Från angriparens sida har åtgärder även vidtagits för att de skadliga koderna ska undgå upptäckt och i vissa fall försvåra analys.

Farhågorna om att attackmetoder och distributionsmekanismer kan kopieras och bidra till spridningen av liknande angrepp får anses bekräftade idag. Det finns därför anledning att befara en fortsatt spridning av liknande attackkod. Den storlek och komplexitet som krävs innebär dock en tröskelnivå som kan göra det svårt för mindre aktörer eller enstaka individer att utveckla sådan kod.

Såväl Stuxnet som dess efterföljare detekterades under eller efter spridningsfasen, då koderna varit operativa under en kortare eller längre tid. Med tanke på att kodernas komplexitet även krävt omfattande, bakomliggande programutveckling innebär det att projekten rimligen initierats långt före den tidpunkt då de skadliga koderna upptäcktes.

Det som dessutom kännetecknar it-system som byggts för att styra fysiska processer är att ju närmare själva styrsystemmiljön man kommer, desto färre programverktyg finns tillgängliga för att till exempel detektera attacker och ta bort skadlig kod.

Antivirusföretagen och andra aktörer inom it-säkerhetsindustrin har visserligen uppmärksammat denna nya familj av risker, men utbudet av skyddsmetoder och verktyg släpar fortfarande efter i jämförelse med persondatormiljön.

10.4 Nätaktivism i olika former

Under de senaste åren har det på flera håll i världen tydliggjorts hur internet kan användas för nya typer av opinionsbildning och nätbaserad aktivism. Via internet kan till exempel kunskapen om demonstrationer och protester mot auktoritära regimer kablas ut i samma sekund de genomförs. Människor kan snabbt kommunicera och mobiliseras. Händelserna under den arabiska våren 2011 utgör ett av de bästa exemplen på hur internet möjliggjort snabb nyhetsförmedling under svåra förhållanden, ett friare åsiktsutbyte och på vissa håll underlättat demokratiutvecklingen.

Nätaktivismen tar sig emellertid olika uttryck. Även hacktivism med inslag av dataintrång och rena blockeringsangrepp har blivit ett påtagligt inslag i dagens globala internetmiljö. Vid flera tillfällen har detta drabbat svenska samhällsfunktioner.

Tröskeln för att delta i dessa aktioner har dessutom sänkts markant. Där det tidigare krävdes relativt avancerade kunskaper för att genomföra angrepp tillhandahålls det idag färdigpaketerade angreppsverktyg som i stort sett vem som helst med en internetanslutning kan använda. Ibland levereras verktygen till och med färdiginställda för att angripa namngivna mål.

Under den senaste tvåårsperioden har den löst sammanhållna nätaktiviströrelsen Anonymous återkommande mobiliserat stöd för aktiviteter som bland annat resulterat i blockeringsattacker och oönskad publicering av större mängder information om, eller från, den angripna parten (så kallad ”doxning”). Anonymous, liksom flera andra nätaktiviströrelser, spelade också en viss roll under den arabiska våren 2011, där de genomförde olika typer av nätaktioner mot regimerna i de länder där det uppstått oroligheter.

Ungefär vid den tidpunkten splittrades emellertid Anonymous-rörelsen. Från att ha kunnat mobilisera omfattande stöd för ett fåtal stora kampanjer skapades istället ett otal grenar och aktiviteter. Idag tycks den tidigare relativt samlade ”icke-rörelsen” (vem som helst kan associera sig med Anonymous, själva begreppet representerar en

anonym människomassa i rörelse) inte längre ha samma breda mobiliseringsförmåga som tidigare. I viss mån kan detta ha ett samband med att ett antal identifierade aktivister lagförts i USA, Storbritannien och Nederländerna.

En av de största, mest uthålliga kampanjerna har skett till stöd för Wikileaks och dess ledare Julian Assange. Under senhösten 2010 drabbades delar av den svenska rättsapparaten av sådan aktivism, i samband med att Assange blivit misstänkt i en svensk brottmålsutredning.

Reflektion

Ur samhällsperspektiv får blockeringsattacker mot myndigheter och symbolladdade samhällsaktörer betraktas som ett återkommande fenomen som troligen kommer att öka i omfattning under kommande år. Så sent som i början av september 2012 riktades till exempel flera blockeringsangrepp mot svenska myndigheter, vilket sammanföll i tiden med en nätaktivitet till stöd för Julian Assange. Hittills har nätaktivisternas aktioner oftast haft begränsade skadeverkningar. Följderna har blivit att den drabbade parten fått temporär otillgänglighet på sin webbplats och att det uppstått en trovärdighetsskada för den som drabbats. De senaste åren har också tröskeln för att kunna genomföra en blockeringsattack sjunkit. Det krävs inte längre expertkunskap för att hantera verktygen, och de blir allt mer spridda. Därmed blir det möjligt för allt fler att iscensätta denna typ av missnöjesattacker.

10.5 Tieto-incidenten

I slutet av november 2011 inträffade en av de större tekniska it-incidenterna i Sverige under senare år. Då havererade ett lagringssystem hos it-driftleverantören Tieto, vilket drabbade runt 50 kunder, varav flera kommuner och statliga bolag. Det handlade alltså inte om något antagonistiskt angrepp, utan en tekniskt orsakad driftstörning. Konsekvenserna blev emellertid stora. Bland annat slogs recepthanteringen ut i flera dagar vid ett stort antal av landets apotek och Bilprovningen fick totalstopp i sina produktionssystem under närmare en vecka. Två kommuner i Stockholmsregionen fick omfattande störningar i sitt it-stöd som tog veckor att åtgärda och ett antal andra kommuner runt om i landet fick problem med enstaka tjänster.

Reflektion

MSB publicerade i februari 2012 en rapport om händelsen[51], där det bland annat konstateras att den pågående koncentrationen av it-drift till ett fåtal stora driftleverantörer ökar risken för den här typen av händelser i samhället. När ett tekniskt fel inträffar kan det plötsligt drabba olika delar av samhället samtidigt. Förloppet vid en sådan händelse blir snabbt - och det blir allt svårare för samhället att överblicka konsekvenserna.

Ur ett krishanteringsperspektiv visade det sig vid Tieto-incidenten svårt att på kort tid få en tillfredsställande lägesbild och att kunna överblicka de totala konsekvenserna av händelsen. Det berodde bland annat på att informationen om it-driftleverantörernas kunder och deras driftstatus hanterades med sedvanlig affärssekretess samt att några av Tietos kunder tycks ha varit företag som i sin tur levererade nätbaserade tjänster till andra organisationer.

Samlade slutsatser och bedömning

11. Samlade slutsatser och bedömning

De utvecklingslinjer som redovisats ger en relativt disparat bild av den rådande situationen på informations- och cybersäkerhetsområdet. Några trender är dock tydliga. Dagens informationshantering präglas av hög förändringstakt. Framför allt är det kombinationen av växande informationsmängder, snabb övergång till centraliserade lösningar och den ökade mobiliteten bland användarna som innebär att riskbilden nu förändras, för såväl individer som organisationer och samhället i stort.

Samhällets informationshantering är både omfattande och komplex, och omfattningen ökar från år till år. Ett kraftigt beroende av fungerande it-stöd genomsyrar i stort sett alla samhällsområden. Dessutom sker det en snabb koncentration av it-drift och datalagring till helt andra platser än där informationen ursprungligen skapats.

Centraliseringen av it-driften i samhället inbegriper bland annat utkontraktering i stor skala och användning av standardiserade tjänster hos externa driftleverantörer. I Sverige är detta särskilt tydligt inom sjukvården och delar av e-förvaltningsarbetet. Denna stordrift kan bidra till att informationssäkerheten förbättras hos många samhällsaktörer, särskilt bland mindre organisationer. Men samtidigt finns det en risk att bristfälliga lösningar och alltför vaga upphandlingskrav bidrar till att informationssäkerheten försämras istället. Centralisering kan också leda till minskad redundans i samhällssystemet, och ökad risk för att det uppstår kaskadeffekter i samband med störningar.

När utförandet läggs utanför den egna organisationen ställs det större krav än tidigare på väl genomtänkt styrning och uppföljning av it-verksamheten, vilket också kräver särskild kompetens. Avsaknaden av tillräckligt effektiv styrning kan i ackumulerad form innebära en ökad samlad samhällsrisk.

Ett karaktäristiskt drag hos världens it-användning idag är den ständigt ökande graden av mobilitet. Även detta har konsekvenser för informationssäkerheten. Särskilt känsligt är det faktum att många utrustningar ger programvaror av skilda slag alltför omfattande tillgång till den information som finns lagrad. Ofta hanteras både privat och arbetsrelaterad information i samma utrustning, vilket

innebär en utmaning för organisationer. Privatroll och tjänsteroll visar sig ofta svåra att skilja åt, och det finns ett antal existerande regelverk som ställer krav.

När personlig utrustning ges tillträde till arbetsplatsens informationssystem försvinner ofta även den administrativa kontroll som tidigare funnits. Om sådan åtkomst ska tillåtas krävs det tydliga riktlinjer och en medvetenhet bland användarna om säkerhetsproblematiken.

En annan tydlig, global trend är utvecklingen mot allt mer sofistikerad och storskalig datainsamling och dataanalys. Utvinningen av data från de enorma informationsmängder som ständigt skapas och omformas i världen är efterfrågad även av andra än de som samlat in informationen, och ofta i helt andra syften än de ursprungliga. Sociala medier är ett sådant område, där information ofta skapas i ett syfte men därefter utnyttjas i ett annat. Myndighetsdata är ett annat område, där privata aktörer nu bildligen börjar idka gruvdrift på offentlig information.

Ur det allmännas perspektiv är denna dataanalys inte oproblematisk. När det gäller myndigheters verksamhet ska å ena sidan offentlighetsintresset tillgodoses, liksom möjligheten att i kommersiellt syfte vidareutnyttja samhällsförvaltad information. Å andra sidan får den ökade informationslagringen och flödet av information mellan system inte innebära att skyddet av medborgarnas personuppgifter urholkas. Dessutom finns det samhällsskyddsaspekter att anlägga på de möjligheter som skapats att i stor skala inhämta och analysera detaljinformation om till exempel samhällsviktig verksamhet.

På allt fler håll i världen uppmärksammas idag de samhällskonsekvenser som kan uppstå på grund av it-relaterade avbrott i tekniska infrastrukturer. Flera incidenter har på senare år också tydliggjort vad som kan hända. Några anknutna områden är smarta elnät, smarta städer och maskin-till-maskinkommunikation (M2M). Vidare forskning behövs här med avseende på säkerhetsaspekter, liksom studier som ur ett juridiskt perspektiv behandlar behovet av ny lagstiftning.

Skadlig kod och skräppost fortsätter att utmana. Spridningen sker nu i nya, ”smarta” mobila enheter då incitament finns för angrepp även riktade mot dessa. Den traditionella skräpposten minskar,

medan den samtidigt ökar i sociala medier, där meddelanden sprids via betrodda källor. Verksamhetsstörningar och tillgänglighetsattacker orsakade av skadlig kod som direkt eller indirekt tagit sig in i organisationers och privatpersoners informationssystem ser således ut att fortsätta.

Den it-relaterade brottsligheten är, liksom skadlig kod och skräppost, inget nytt fenomen. Kostnaderna för den it-relaterade brottsligheten drabbar såväl privata företag som samhället i stort genom dataintrång, informationsstölder och bedrägerier. Tyvärr har det visat sig svårt att få en bra bild över den it-relaterade brottslighetens omfattning eller vilka samhällskostnader denna brottslighet leder till. Men att it-utvecklingen är en stor utmaning för de brottsbekämpande myndigheterna råder det ingen tvekan om.

En stor utmaning för samhället är också säkerhetsarbetet kring olika typer av industriella styrsystem. Dessa system används bland annat för att styra en rad samhällsviktiga verksamheter, från eldistribution och vattenförsörjning till trafikljus, sjukhusutrustning och logistikcentraler. Antagonistiska angrepp mot sådana system har potential att ställa till mycket stor skada. Området har därmed också en säkerhetspolitisk dimension, vilket inte minst visas av de internationella fall som kunnat studeras, med Stuxnet som främsta exempel.

Ett särskilt fenomen som kunnat iakttas under de senaste åren är en relativt omfattande hacktivism som i flera omgångar väckt stor uppmärksamhet, men knappast orsakat några mer omfattande skadeverkningar ur ett samhällsperspektiv. Det finns dock goda skäl att studera den vidare utvecklingen noggrant, för att skaffa sig kunskap om framför allt de tillvägagångssätt som tillämpas. Liksom när det gäller säkerhetspolitiskt motiverade nätangrepp utgör sådan kunskap en förutsättning för att kunna hantera framtida händelser, där man till exempel kan tänka sig att aktivism och it-brottslighet blandas - och där måltavlorna inte längre är symboliska utan angreppen sker direkt mot samhällsviktig verksamhet.

Referenser

[1] It i människans tjänst – en digital agenda för Sverige. Regeringskansliet, oktober 2011. *http://www.regeringen.se/content/1/c6/17/72/56/-5a2560ce.pdf, 2012-11-01.*

[2] 1 zettabyte = 10^{21} byte

[3] IEEE Industry Connections Ethernet Bandwidth Assessment, IEEE 802.3 Ethernet Working Group, 19 juli 2012, *http://www.ieee802.org/3/ad_hoc/bwa/BWA_Report.pdf, 2012-10-01.*

[4] The World's Technological Capacity to Store, Communicate, and Compute Information, Science 1 april 2011, Vol. 332 no. 6025 pp. 60-65, se även: *http://www.msnbc.msn.com/id/41516959/ns/technology_and_scienceinnovation/t/worlds-shift-analog-digital-nearly-complete/, 2012-10-01.*

[5] Se MSB, Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, 2012, *https://www.msb.se/RibData/Filer/pdf/-26170.pdf, 2012-10-01.*

[6] ”Data mining” används som benämning för den process som söker hitta mönster i stora mängder data. Processen underlättas av specifika mjukvaruprodukter för analys.

[7] ”Big data” eller stordata är benämningen för de enorma datamängder som skapas på internet. Stordata produceras oftast i realtid och kan bland annat härröra från kameror, digitala sensorer och liknande, eller till exempel skapas på Twitter eller Facebook.

[8] Europaparlamentets och rådets direktiv 2003/98/EG om vidareutnyttjande av information från den offentliga sektorn, PSI-direktivet (från Public Sector Information), antogs den 17 november 2003. Direktivet genomfördes i svensk rätt den 1 juli 2010 genom lag (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen.

[9] Canalys: 62,7% och IDC: 61,3% *http://mobithinking.com/blog/2011-handset-and-smartphone-sales-big-picture, 2012-10-01.*

[10] Se Andy Rubin, Google+, 27 februari 2012, *https://plus.google.com/u/0/112599748506977857728/posts/Btey7rJBaLF#112599748506977857728/posts/Btey7rJBaLF, 2012-10-01.*

[11] Se AVG Community Powered Threat Report, Q1 2012, *http://aa-download.avg.com/filedir/news/AVG_Community_Powered_Threat_Report_Q1_2012.pdf, 2012-10-01.*

[12] Se MSB, Vägledning för säkrare hantering av mobila enheter, 2012, *https://www.msb.se/en/Products--services/Publications/Publications-from-the-MSB/Vagledning-for-sakrare-hantering-av-mobila-enheter/, 2012-11-01*

[13] På detta område har ett särskilt produktsegment vuxit fram: Mobile Device Management (MDM). Se även Forbes magazine, Mobile Device Management Hits Center Stage, but Concerns Remain, *http://www.forbes.com/sites/tomkemp/2012/02/15/mobile-device-management-hits-center-stage-but-concerns-remain/, 2012-11-22*

[14] Rekordmånga e-deklarerade – smartphone växer snabbast, pressmeddelande från Skatteverket, 2012-05-08, *http://www.skatteverket.se/omskatteverket/press/pressmeddelanden/riks/2012/2012/rekordmangaedeklareradesmartphonevaxersnabbast.5.71004e4c133e23bf6db800078980.html*

[15] Sveriges kommuner och landsting, E-förvaltning och e-tjänster i Sveriges kommuner 2011. *http://brs.skl.se/brsbibl/kata_documents/doc40082_1.pdf, 2012-11-01.*

[16] *http://www.checkfacebook.com/, 2012-11-01.*

[17] Se .SE, Svenskarna och internet 2012, Olle Findahl, *http://www.iis.se/docs/SOI2012.pdf, 2012-11-23*

[18] Europeiska kommissionen, Förslag till europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning). KOM(2012) 11 slutlig. 25 januari 2012. *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, 2012-10-01.*

[19] Enligt en undersökning av E-delegationen från 2010, använde sig 30 procent av myndigheterna under regeringen av Facebook. *http://www.edelegationen.se/sites/default/files/imce/filer/publikationer/Enkatsvar_utdrag_ur_betankande.pdf, 2012-10-01.*

[20] Se till exempel Information Commissioner's Office (UK), 2012-10-16, Police force pays £120,000 penalty for data breach, *http://www.ico.gov.uk/news/latest_news/2012/police-force-pays-120000-penalty-for-data-breach-16102012.aspx, 2012-11-30*

[21] The Huffington Post, 2012-09-19, 94 Million Exposed: The Government's Epic Fail on Privacy, *http://www.huffingtonpost.com/adamlevin/government-data-security_b_1897229.html, 2012-11-30*, se även Rapid7 Report: Data Breaches in the Government Sector, 2012-09-06, *http://www.rapid7.com/news-events/press-releases/2012/2012-federal-data-breach-report.jsp, 2012-11-30*, samt Privacy Rights Clearinghouse, 2011-12-16, The Top Half Dozen Most Significant Data Breaches in 2011, *https://www.privacyrights.org/top-data-breach-list-2011, 2012-11-30*

[22] Help Net Security, 2012-09-30, UK data breaches up 1000% in five years, *http://www.net-security.org/secworld.php?id=13504, 2012-11-30*

[23] Jerusalem Post, 2012-05-13, Six indicted over Population Registry data theft, *http://www.jpost.com/NationalNews/Article.aspx?id=269728, 2012-11-30*

[24] Washington Post, 2012-11-20, Greek police arrest man on suspicion of theft of 9 million personal data files on Greeks, *http://www.washingtonpost.com/world/europe/greek-police-arrest-man-on-suspicion-of-theft-of-9-million-personal-data-files-on-greeks/2012/11/20/72dc5c64-331a-11e2-92f0-496af208bf23_story.html, 2012-11-30*

[25] Computer Sweden, 2012-03-29, Skatteverket hackat, *http://www. idg.se/2.1085/1.440750/skatteverket-hackat, 2012-11-30,* se även Computer Sweden, 2012-09-19, Logica-intrång kan ha pågått i flera år, *http://computersweden.idg.se/2.2683/1.466890, 2012-11-30*

[26] ICS står för Industrial Control System.

[27] SCADA står för Supervisory Control and Data Acquisition (styrning och datainsamling). Benämningen används ofta för att beskriva styrningen i distribuerad miljö, där man samlar ihop övervakning och styrning av ett större antal industriella styrsystem.

[28] Sveriges Radio, Nyheter/Ekot, 700 hushåll utan värme efter hacker-attack, *http://sverigesradio.se/sida/artikel.aspx?programid=160&artikel=4239787, 2012-11-01.*

[29] Den engelska beteckningen är Smart Grid.

[30] Symantec, Internet Security Threat Report, 2011 Trends, Volume 17, April 2012. *http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf, 2012-11-01.*

[31] PandaLabs Quarterly Report, January – March 2012, *http://press.pandasecurity.com/wp-content/uploads/2012/05/Quarterly-Report-PandaLabs-January-March-2012.pdf, 2012-10-01.*

[32] IDG.se, Nya hackartrenden: kidnappning, *http://www.idg.se/2.1085/1.443228/nya-hackartrenden-kidnappning, 2012-04-13.*

[33] McAfee Threats Report: Third Quarter 2012, *http://www.mynewsdesk.com/se/pressroom/mcafee/document/view/mcafee-threats-report-q3-2012-23141, 2012-11-01.*

[34] PandaLabs Quarterly Report, January – March 2012, *http://press.pandasecurity.com/wp-content/uploads/2012/05/Quarterly-Report-PandaLabs-January-March-2012.pdf, 2012-10-01.*

[35] Se vidare *https://www.cert.se/megamap, 2012-11-22.*

[36] The Wall Street Journal, Spam Finds New Target, 4 January 2012, *http://online.wsj.com/article/SB10001424052970203686204577112942734977800.html, 2012-11-01.*

[37] Under 2010 bedömdes botnät stå för 88.2 procent av spamtrafiken mot 81.2 procent under 2011.

[38] Zeus är ett botnät som enligt uppgift kontrollerade 13 miljoner datorer världen över. Datorerna i Zeus-botnätet användes dels för att skicka stora mängder skärppost, men även för att stjäla pengar.

[39] Säkerhetsbloggen: CSI Redmond – Microsoft tar lagen i egna händer, *http://blog.eset.se/csi-redmond-microsoft-tar-lagen-i-egna-hander/, 2012-10-01;* F-Secure, Microsoft's Digital Crimes Unit Targets ZeuS. *http://www.f-secure.com/weblog/archives/00002337.html, 2012-11-22;* Here's How Microsoft's Digital Crime Unit Is Taking Down Evil Spammers, *http://articles.businessinsider.com/2012-03-29/news/31253437_1_botnet-zeus-microsoft, 2012-11-22.*

[40] Bae Systems and Detica, Office of Cyber Security and Detica report estimates that the overall cost to the UK economy from cyber crime is £27 billion annually, 17 February 2011, *http://www.baesystemsdetica.com/news/office-of-cyber-security-and-detica-report-estimates-that-the-overall-cost/, 2012-11-01.*

[41] Does Cybercrime Really Cost $1 Trillion?, *http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion, 2012-09-26*

[42] R. Anderson et al., Measuring the Cost of Cybercrime, 2012. *http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf, 2012-10-01.*

[43] Næringslivets sikkerhetsråd, Mørketallsundersøkelsen – Informasjonssikkerhet og datakriminalitet, 2012, *http://www.nsr-org.no/moerketall/, 2012-11-22*

[44] SVT.se, 12 december 2011, *http://svt.se/2.22620/1.2640303/dataintrangen_okar_kraftigt_i_landet, 2012-10-01.*

[45] Ekoparty Security Conference 8th edition. *http://ekoparty.org/eng/index.php, 2012-10-01.*

[46] CERT-SE, RSA drabbat av dataintrång, *http://www.cert.se/publikationer/namnvart/rsa-drabbat-av-dataintraang, 2012-10-01.*

[47] RSA, Open Letter to RSA Customers, *http://www.rsa.com/node.aspx?id=3872, 2012-10-01.*

[48] RSA, Anatomy of an Attack, 1 April 2011, *http://blogs.rsa.com/rivner/anatomy-of-an-attack/, 2012-10-01.*

[49] Den skadliga koden tycks ha varit konstruerad för att söka upp och förstöra delar av en processanläggning för anrikning av uran, belägen i Natanz i Iran. Se vidare Symantec, W32.Stuxnet Dossier, februari 2011, *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2012-11-22;* New York Times, 2012-08-09, Times Topics: Cyberattacks on Iran – Stuxnet and Flame, *http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html, 2012-11-22;* samt de resonemang som förs i Sanger, David E. Confront and Conceal, 2012.

[50] Kaspersky Labs, Gauss: Abnormal distribution, (2012) *http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf, 2012-11-22*

[51] Se MSB, Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, 2012, *https://www.msb.se/RibData/Filer/pdf/26170.pdf, 2012-10-01.*

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB505 - december 2012 ISBN 978-91-7383-301-1