Informationssäkerhet – trender 2015

Informationssäkerhet – trender 2015

Informationssäkerhet – trender 2015

Myndigheten för samhällsskydd och beredskap (MSB)

Layout: Advant Produktionsbyrå
Tryck: DanagårdLiTHO

Publ.nr: MSB779 - januari 2015
ISBN: 978-91-7383-509-1

Innehåll

Förord

Förord

Utvecklingen av informationsteknologi skapar nationella och globala utmaningar och nya möjligheter. Utvecklingen utmanar många traditionella idéer och har medfört nya former av interaktion mellan människor. Men förändringarna gör även att samhället blir mer sårbart och skapar därigenom mycket stora säkerhetsutmaningar.

Försvarsberedningen uppger i sin rapport från 2013, *Vägval i en globaliserad värld* (Ds 2013:33), att sårbarheterna som uppstår i dagens globala it-system är, och inom överskådlig tid kommer att vara, en av de mest komplexa frågorna. Försvarsberedningen betonar i sin rapport från 2014 *Försvaret av Sverige* (Ds 2014:20) att det finns ett fortsatt behov av att se på möjligheterna att fortsatt stärka it-robustheten i samhället och analysera behovet av att utveckla cyberförmågor. I den rapport som Riksrevisonen lämnat (RiR 2014:23) blir bilden än tydligare av de utmaningar som samhället står inför.

Den allt mer oförutsägbara och komplexa utvecklingen förstärker behovet av en väl fungerande och allsidig analys av omvärldsutvecklingen. Försvarsmakten, Försvarets radioanstalt, Myndigheten för samhällskydd och beredskap samt Rikskriminalpolisen har därför gemensamt tagit fram denna trendrapport som ett underlag för fortsatt stöd i det säkerhetsarbete som måste bedrivas i alla delar av samhället. Vi hoppas det blir en givande läsning och ett bra stöd för allas arbete med informations- och cybersäkerheten i Sverige.

Stockholm den 10 januari 2015

Mattias Hanson
Chef, MUST:s säkerhetskontor,
Försvarsmakten

Charlotte Lindgren
Chef, Avdelningen för cyberverksamhet,
Försvarets radioanstalt

Tuve Johansson
Sektionen för utredning av IT-brott,
Nationella operativ avdelningen,
Polisen

Richard Oehme
Chef, Verksamheten för samhällets informations- och cybersäkerhet, Myndigheten för samhällsskydd och beredskap

Sammanfattning

Sammanfattning

Rapporten tar upp sju trendområden. Inom vart och ett av dessa identifieras tre huvudpunkter som återges nedan. Sammantaget ger punkterna en övergripande bild av situationen på informationssäkerhetsområdet.

1. **Strategiska beslut om informationssäkerhet tas alltid i en kontext där säkerhet vägs mot andra värden. Följande punkter är viktiga för beslutsfattare att ta till sig:**
   - Informationssäkerhet kommer framöver att allt mera betraktas som en fråga om att skydda hela samhället och dess välstånd snarare än bara teknik.
   - Det blir en allt viktigare utmaning att utforma praxis och lagar så att god informationssäkerhet blir en fördel snarare än en nackdel i den globala konkurrensen.
   - Utveckling av programvara och tjänster ställer höga krav på både beställarkompetens och säkerhetsmedvetande hos beställaren för att uppnå tillräcklig säkerhetsnivå.

2. **It-tjänster i moderna verksamheter är ofta komplexa och utspridda både fysiskt och organisatoriskt. Det får konsekvenser för säkerheten:**
   - Riskerna blir mer svårbedömda och korsberoendena mer svåröverskådliga i takt med att organisationers data passerar många olika rättskipningsområden och tekniska system.
   - Det kommer att ställas allt högre krav på beställarkompetensen hos offentliga aktörer för att kunna leva upp till kraven i exempelvis personuppgiftslagen.
   - Det blir allt vanligare med löpande bevakning och åtföljande åtgärder snarare än preventiva skydd.

3. **Allt mer information om oss själva och om våra tekniska lösningar blir allmänt tillgänglig. Tre nyckelfaktorer för att förstå konsekvenserna är följande:**
   - Frågorna om privatlivet aktualiseras allt mer när större mängd och fler typer av data blir tillgängliga i det moderna samhället.
   - Den ökade delningen av information ger ökad osäkerhet om vem som äger data.
   - Snabb teknikutveckling gör författningar och regler kring elektroniskt informationsutbyte mellan myndigheter föråldrade, vilket försvårar både önskvärda systemintegrationer och skyddet för privatlivet.

4. **Informationssäkerhet har på senare år fått en växande säkerhetspolitisk dimension. Några nyckelobservationer är följande:**
   - Informationsoperationer där internetbaserad propaganda kombineras med diplomati, lögner, medieutspel och traditionell militär verksamhet har blivit vanligt förekommande i väpnade konflikter.
   - Cyberspionage och cybersabotage är en del av ”den säkerhetspolitiska verktygslådan” i allt fler länder.
   - Internets ökade möjligheter till fri och svårkontrollerad kommunikation har medfört motreaktioner i många stater, med försök att isolera sina nationella nät från internet.

5. **I det moderna samhället har så gott som all brottslighet en it-koppling. Följande punkter sammanfattar trenderna på det området:**
   - Dagens it-relaterade organiserade brottslighet har oftast ekonomiska drivkrafter och en internetbaserad kriminell tjänstesektor, *crime-as-a-service*, har vuxit fram på senare år.
   - Samspelet mellan traditionell och elektronisk brottslighet ökar och blir allt mer komplext.
   - Dagens brottslighet ställer nya krav på rättsväsendet, inte minst vad gäller samverkan med utländska polismyndigheter och privata aktörer.

6. **Det sker en ständig kapplöpning mellan angripare och försvarare. Några trender väl värda att uppmärksamma är följande:**
   - Förekomsten av programvara som identifierar sårbarheter samt enkla och billiga tekniska hjälpmedel för angrepp har sänkt tröskeln och satt verktyg i händerna på fler angripare. Samtidigt är de allra mest kvalificerade angreppsverktygen fortfarande hårdvaluta och förbehållna en mindre krets.
   - Trots de tekniska sårbarheterna är människan i systemet ofta den svagaste länken, som kan luras att ladda ner skadlig kod eller uppge känsliga uppgifter.
   - Även om allt fler organisationer inför bestämmelser för informationssäkerhet är steget från bestämmelse till faktisk säkerhet långt.

7. **När samhället blir allt mer beroende av tekniska system måste dessa vara robusta. Viktiga aspekter på detta är följande:**
   - I det moderna samhället blir konsekvenserna av driftavbrott i informationssystem större och mer oöverskådliga.
   - Riskhantering och kontinuitetsplanering blir allt viktigare för att uppnå robusta informationssystem, liksom förståelse för den egna verksamhetens ofta allt mer komplexa it-beroende.
   - Marknaden för cyberförsäkringar är i sin linda, men kommer att växa i framtiden.

Inledning

Inledning

Denna trendrapport är framtagen för att ge en lättillgänglig och samlad bild av situationen på informations- och cybersäkerhetsområdet samt ge en sammantagen bedömning av förhållanden som är särskilt angelägna att uppmärksamma för beslutsfattare i samhället. Bedömningen är främst baserad på utvecklingen under 2013 och 2014.

I arbetet med trendrapporten har Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA), Polisen och Försvarsmakten deltagit, tillsammans med stöd från Totalförsvarets forskningsinstitut (FOI). Trendrapportens innehåll är sammanställt med utgångspunkt från den kunskap och löpande omvärldsanalys som sker vid respektive myndighet.

Rapporten omfattar trender nationellt och internationellt. Med trend avses i denna rapport stabila, långsiktiga förändringar på informationssäkerhetsområdet som bedöms påverka samhället i någon form och som har identifierats av de deltagande myndigheterna. I vissa fall presenteras trendframskrivningar, men eftersom området är relativt nytt saknas ofta statistiska mätetal med långa tidsserier, vilket gör det svårt att förutsäga den framtida utvecklingen.

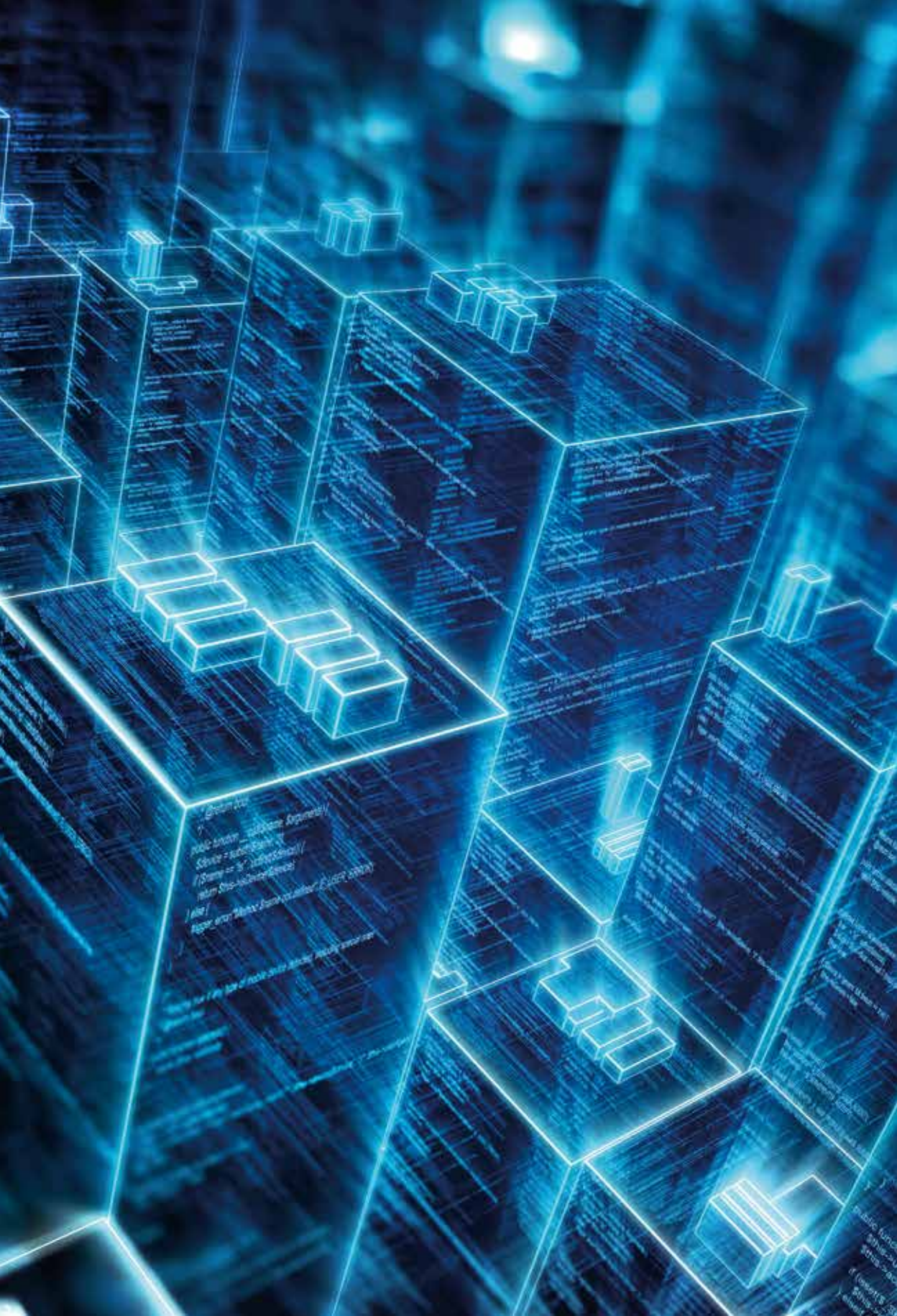
Rapporten har ett brett angreppssätt och täcker många sorters hot och risker. Beroende på sammanhang är de angripare som omnämns allt från ytterst kvalificerade statsaktörer med stora och specialiserade resurser, via organiserad brottslighet som köper och säljer angreppsverktyg på svarta marknader, till mindre kvalificerade så kallade hacktivister eller rentav missnöjda tonåringar som inte riktigt förstår vilka konsekvenser deras handlingar får. Dessutom tar rapporten upp hot och risker som inte uppstår på grund av angrepp, utan snarare på grund av organisationers egna misstag och bristfälliga riskhantering.

De trender som redovisas i rapporten har tagits fram genom ett gemensamt arbete med representanter från de deltagande myndigheterna. Därefter har underlaget kompletterats med andra källor såsom medierapportering, vetenskapliga publikationer,

ett urval av intervjuer och offentligt skriftligt material. Själva texten har bearbetats i flera omgångar där en bredare krets av representanter från myndigheterna har fått möjlighet att lämna kommentarer och synpunkter.

Rapporten har en stor mängd källhänvisninga i syfte att möjliggöra vidare läsning för den intresserade. En stor del av källorna är vetenskapliga publikationer som har genomgått så kallad *peer review*. Metoddiskussionerna i dessa är ovärderliga för att bedöma de resultat som redovisas i dem. Dessa källor är även av intresse eftersom det är av stor vikt att systematiskt utveckla underlag såsom statistik inom informationssäkerhetsområdet.

Rapporten tar upp sju trendområden. Deras inbördes ordning ger inte uttryck för någon prioritering: rapporten tar inte ställning till om vissa utmaningar, hot eller risker är större än andra. Varje kapitel inleds med tre huvudpunkter som sammanfattar de viktigaste budskapen.



1. Informationssäkerhet – en avvägning mot andra värden

- *Informationssäkerhet kommer framöver att allt mera betraktas som en fråga om att skydda hela samhället och dess välstånd snarare än bara teknik.*
- *Det blir en allt viktigare utmaning att utforma praxis och lagar så att god informationssäkerhet blir en fördel snarare än en nackdel i den globala konkurrensen.*
- *Utveckling av programvara och tjänster ställer höga krav på både beställarkompetens och säkerhetsmedvetande hos beställaren för att uppnå tillräcklig säkerhetsnivå.*

Informationstekniken har förändrat det moderna samhället och blivit en oumbärlig del av det. Idag arbetar vi, betalar räkningar, roar oss och umgås med hjälp av datorer och internet på ett sätt som var svårt att föreställa sig för tio-femton år sedan. Bedömare som EU och OECD (Organisation for Economic Co-operation and Development) är överens om att den nya digitala ekonomin kommer att spela en allt viktigare roll för framtida tillväxt och välstånd [1], [2]. En sådan utveckling ställer tveklöst ökade krav på säkerhet – men gör också innebörden av säkerhet mer komplex.

Informationssäkerhet är inte längre bara ett specialintresse för tekniskt intresserade. Beslutsfattare kommer allt oftare att behöva hantera målkonflikter där informationssäkerhet ställs mot andra värden och där det saknas enkla lösningar. Att styrningsfrågorna är komplexa och kräver såväl engagemang som strategiska beslut på högsta nivå är ett ledmotiv i det här kapitlet.

1.1 Informationssäkerhet för att skydda samhället och dess välstånd

OECD beslutade i december 2013 att revidera sina rekommendationer om informationssäkerhet, vilka legat fast sedan 2002 [2]. I detta decennielånga tidsperspektiv blir de långa utvecklingstrenderna tydliga: it driver innovationer samt ekonomisk och

social utveckling, men utgör också en infrastruktur som är kritisk för det moderna samhällets funktion. Hoten förändras också ständigt. Detta har fått ett stort antal länder – dock än så länge inte Sverige – att anta nationella strategier för cyberområdet och dess säkerhet. Den viktigaste förändringen i OECD:s reviderade riktlinjer är att man avser byta fokus i sin säkerhetssyn: från skydd av de digitala teknikmiljöerna till skydd av de ekonomiska och sociala verksamheter som är beroende av tekniken. Säkerhetsfrågorna anses inte längre endast handla om att hålla nätverk fria från virus eller hemligheter hemliga, utan om samhällets funktion, ekonomins konkurrenskraft och grunderna för vårt välstånd.

EU:s strategi för cybersäkerhet [1] antogs 2013. Som ett led i arbetet med att säkerställa en gemensam hög nivå av nät- och informationssäkerhet i hela unionen påbörjades också arbetet med EU:s direktiv för informationssäkerhet. Förslaget till direktiv ålägger alla medlemsstater att se till att de har en miniminivå av nationell kapacitet samt viss förmåga till internationellt samarbete. Direktivet kommer att påverka offentlig förvaltning och företag inom specifika kritiska sektorer. Direktivet har nu passerat EU-parlamentet, som hade betydande ändringsförslag. EU-kommissionen arbetar nu för att EU ska besluta om direktivet skyndsamt.

1.2 Lagstiftarens utmaningar

Att säkerhetsfrågorna allt mer handlar om att skydda välstånd skapar utmaningar. Lagstiftning som syftar till att stärka säkerheten riskerar nämligen att minska konkurrensen och produktiviteten i ekonomin. Särskilt små och medelstora företag kan drabbas oproportionerligt hårt av säkerhetsregler [3]. Stora bolag kan till och med vända sig till lagstiftarna med förslag på tuffa säkerhetskrav, i syfte att underminera mindre och resurssvagare konkurrenter. Samtidigt kan smarta bestämmelser, som EU:s harmonisering av standarder för elektronik, förenkla för företag och öka handeln [4]. Eftersom varken lagstiftaren eller innovatörerna vet hur tekniken kommer att användas i framtiden kan illa genomtänkta lagar sätta krokben för innovationer och tillväxt.

Forskningen har visat att de stora tillväxteffekterna sällan kommer där man väntar sig – IBM:s pc var exempelvis bara avsedd för kalkylblad när den togs fram [5]. Det blir därför allt viktigare att utforma praxis och lagar så att god informationssäkerhet blir en fördel snarare än en nackdel i den globala konkurrensen [6].

1.3 Krav på beställarkompetens och säkerhetsmedvetande

När man utvecklar programvara står säkerhet sällan i första rummet. Fokus är funktion: att it-tjänsten gör vad den ska. Säkerhet är en så kallad *icke-funktionell* kvalitet och sådana försöker man ofta lägga till i efterhand.

Inom mjukvaruutveckling har det på senare år blivit allt vanligare med så kallade agila metoder. Här försöker man undvika att bara följa en från början fastslagen specifikation, och arbetar med kortare ledtider och fler delleveranser där programvaran löpande anpassas till kundens behov. Detta medför nya utmaningar för säkerheten [7]:

- Det är svårt att göra säkerhetsrevisioner på en dynamisk projektmodell.
- Nya lösningar och designförändringar gör det svårt att säkerställa säkerheten över tiden.
- Ensidigt fokus på funktionella krav leder till att icke-funktionella krav kommer i skymundan.
- Spårbarheten försämras och säkerhetsexpertrollen saknas i projektteamen etc.

Det finns visserligen också gott om förslag på hur säkerhet kan integreras i agil mjukvaruutveckling [8], [9], [10], men någon stor empirisk studie som kan avgöra hur säkerheten påverkas av agil utveckling finns ännu inte.

Hur bör då säkerheten säkras vid mjukvaruutveckling i framtiden? Sannolikt ligger lösningen till stor del i att öka kunskapen och medvetenheten om säkerhetsaspekter på beställarsidan. Agila metoder är ofta effektivare på att leverera den programvara som kunden vill ha. Ansvaret kommer därmed fortsatt att ligga på kunden att efterfråga säkerhet. Detta måste nu ske genom hela utvecklingsprocessen, oavsett om den är agil eller inte. Det räcker inte att skriva om säkerhet i en inledande kravspecifikation. Ett nära samarbete mellan systemutvecklare och informationssäkerhetsexperter blir därmed sannolikt allt viktigare för att uppnå en god säkerhetsnivå.

2. Komplexiteten i moderna it-tjänster

- *Riskerna blir mer svårbedömda och korsberoendena mer svåröverskådliga i takt med att organisationers data passerar många olika rättskipningsområden och tekniska system.*
- *Det kommer att ställas allt högre krav på beställarkompetensen hos offentliga aktörer för att kunna leva upp till kraven i exempelvis personuppgiftslagen.*
- *Det blir allt vanligare med löpande bevakning och åtföljande åtgärder snarare än preventiva skydd.*

Utvecklingen mot en allt mer centraliserad it-hantering fortsätter. Medan varje verksamhet för tio år sedan själv hade hand om sina system för exempelvis löner, lagerhållning och fakturering lägger allt fler nu ut sådana funktioner på externa leverantörer. Ibland är det bara lagrings- och beräkningskapacitet som hyrs, men allt oftare hyrs också själva programvaran, så kallad software-as-a-service eller molntjänster. Drivkraften är kundernas önskan att sänka sina fasta kostnader – det blir mycket billigare om hundra bolag delar på ett datacenter än om var och en ska ha sin egen lösning. Det är denna ekonomiska potential som har fått Riksrevisionen att kritisera statliga myndigheter för att inte pröva frågan om besparingar och effektivisering genom outsourcing tillräckligt, bland annat på grund av starka interna it-avdelningar med låga effektiviseringskrav [11]. Stordriftsfördelarna gör det troligt att molntjänsterna är här för att stanna. Marknaden blir också successivt mognare, med allt fler aktörer och konkurrens dem emellan, vilket driver upp kvaliteten. Outsourcing ställer dock stora krav på beställaren för att inte leda till oönskade risker.

Särskilt för små aktörer kan övergången till externt köpt it innebära att både intrångsskydd och driftsäkerhet ökar, eftersom de får tillgång till både specialistkompetens och bättre teknik. Det gäller inte minst privatpersoner, som lägger allt mer data ”i molnet” och mindre på hemdatorer utan säkerhetskopiering. Det är osannolikt att en småföretagare som sätter upp en egen e-posttjänst får bättre driftsäkerhet än någon av de stora reklamfinansierade ”gratis”

tjänsterna på nätet – däremot behåller denne sina data och får inte sin e-post skannad i annonssyfte. Vad som är bäst beror på omständigheterna. Man får dock aldrig mer än vad man kravställer och betalar för, vare sig med utkontrakterade system eller sådana som man själv handhar.

2.1 Spridd hantering leder till allt mer svårbedömda risker

Samtidigt innebär utvecklingen med outsourcing också ofrånkomligen att allt fler ägg läggs i samma korg och att konsekvenserna av såväl attacker som icke-antagonistiska driftavbrott blir mer svåröverskådliga. En kund i ett moln kan exempelvis drabbas av tillgänglighetsproblem om en annan kunds verksamhet plötsligt växer mycket snabbt. En variant är när en överbelastningsattack på en kund drabbar alla genom att hela plattformen sänks. En relaterad risk är att en enda kunds illegala aktiviteter kan drabba alla andra om en polisutredning plötsligt drabbar molnleverantören. En sofistikerad angripare skulle till och med kunna agera kund i ett visst moln just i detta syfte – eller nyttja sin köpkraft för att förhandla fram villkor som på något sätt missgynnar de andra kunderna [12].

Hela denna skala av både enkla och sofistikerade hot och risker bör vägas in i de riskanalyser som genomförs innan verksamhet kontrakteras ut till underleverantörer eller data läggs i molntjänster. Vidare bör risken för ägarbyte hos leverantören vägas in, särskilt när det gäller möjligheten att värja sekretessen hos känslig information.

Floran av tänkbara angreppsscenarier bör dock inte leda till att man underskattar risken med driftstörningar, oavsett om de är en följd av angrepp eller inte. Tieto-haveriet i slutet av 2011 förblir ett utmärkt exempel på hur centraliserad drift under olyckliga omständigheter plötsligt leder till oväntade och svårförutsägbara problem för stora och till synes orelaterade delar av samhället [13]. Komplexiteten i molnmiljön samt det faktum att ingen idag har en överblick över de beroenden som uppstått gör riskanalyser till en stor utmaning.

Molntjänsterna aktualiserar att ansvar allt oftare är utspritt över flera organisationer, trots att säkerhet förutsätter tydlighet och gott samarbete. Säkerhet kan inte läggas ut på andra – även om den upplevda säkerheten i en molnlösning kan vara hög så ersätter den inte den egna organisationens ansvar eller säkerhetsarbete.

En vetenskaplig studie pekar ut ett antal viktiga problem med det spridda ansvaret [14]: Bland de viktigaste problemen finns svårigheten att utvärdera tjänster, koordinera parterna och att bygga en gemensam och effektiv säkerhetskultur över organisationsgränserna. Det kan också vara problematiskt att få tillgång till data och att bedriva såväl förebyggande arbete som forensiska granskningar.

Standardisering, både av teknik och av kontrakt, samt bättre uppföljning av avtal är en del av lösningen på problemen. Forskningen visar dock att det kan vara svårt att agera rationellt vid kontraktsskrivning rörande exempelvis tillgänglighet [15]. Säkerhet går inte att delegera fullt ut. Sannolikt kommer konsumenter, företag och branschorganisationer att vara centrala spelare i detta arbete, varefter de normer som utvecklats möjligen i efterhand införlivas i lagstiftningen [16]. Förmågan att hantera säkerhet över organisations- och verksamhetgränser blir allt viktigare.

2.2 Offentliga aktörer och beställarkompetensen

Även om molntjänsterna är här för att stanna kan tillväxttakten i svenska kommuners molnanvändning förväntas avstanna efter några uppmärksammade fall av oklarheter avseende hantering av personuppgifter. Datainspektionen har upprepade gånger kritiserat användning av molntjänster där avtalen inte har säkerställt att personuppgiftslagen efterlevs.

I juli 2014 gav Förvaltningsrätten i Stockholm Datainspektionen rätt i ett fall där den aktuella kommunen hade överklagat eftersom avtalet gav leverantören för stort utrymme att behandla personuppgifter för sina egna ändamål och kommunen inte fick tillräcklig information om vilka underleverantörer som leverantören i sin tur anlitade [17]. Här kläms den offentliga sektorn mellan olika krav, där informationssystemen förväntas både vara effektiva och spara pengar, erbjuda medborgarna bättre service och vara säkra. Samtidigt driver offentliga ramavtal på utvecklingen mot en koncentration av it-tjänster till ett fåtal aktörer, eftersom de föreskriver att all offentligt utkontrakterad hantering ska gå till de aktörer som har vunnit ramavtalsupphandlingarna.

I Kammarkollegiets avtal för it-tjänster finns aspekter av informationssäkerhet inkluderade. Avtalet är dock mer att se som en mall: aktörer kan själv välja vad de tar med i sina slutliga avtal.

En undersökning av hur och om aktörer använt Kammarkollegiets ramavtal genomfördes på uppdrag av MSB 2014. Undersökningen visade att de avtal som ingicks i hög grad saknade relevanta krav på informationssäkerhet. Aktörerna hade många gånger valt att bortse från de möjligheter att ställa krav som gavs. De krav som ingick i avtalet handlade om enstaka aspekter snarare än om ett systematiskt arbete utifrån en riskanalys [18].

Ibland är det inte avtalen som är problemen, utan avsaknaden av avtal. Samverkan mellan offentliga aktörer avseende informationssystem blir allt vanligare, men är ofta inte reglerad i några avtal. Det betyder att det inte går att utkräva ansvar via en rättsprocess om något går fel. MSB har påtalat att man borde utreda hur offentliga aktörer ska kunna sluta fungerande överenskommelser med varandra, med liknande funktion som kommersiella avtal [18]. År 2009 påtalade Riksrevisionen i en granskning av myndigheternas samverkan vid it-investeringar att det fanns brister i de registerlagar som reglerar myndigheternas informationshantering, delvis beroende på föråldrade regler och ofullständiga definitioner [19]. Med den höga utvecklingstakt som finns när det gäller it-investeringar och samverkan kring it, så finns det fortsatt stor risk att Riksrevisionens slutsatser är lika aktuella idag.

2.3 Från preventivt skydd till kontinuerlig monitorering

Blotta antalet uppkopplade enheter skapar också komplexitet: Cisco räknar med att det år 2020 kommer att finnas 50 miljarder saker anslutna till internet [20]. I huvudsak är det en positiv utveckling som effektiviserar gamla verksamheter och möjliggör helt nya: läkare kan övervaka patienter på distans, hushållsapparater kan spara ström och billiga sensorer kan övervaka miljöförändringar. Samtidigt betyder det dock att det tillkommer nya sätt att genomföra angrepp. Det som gäller mobiler och läsplattor gäller allt mer också tvättmaskiner, kylskåp, videokonferenssystem, system för fastighetsautomation och medicinsk teknik.

Alla uppkopplade men dåligt skyddade apparater kan användas för attacker av olika slag [21]. Det kan röra överbelastningsattacker antingen på andra uppkopplade apparater eller på traditionell it-infrastruktur som routrar och webbservrar. Det kan handla om att komma över känslig information. Det kan också handla

om skadegörelse med svårförutsägbara konsekvenser, såsom en attack på frekvensstabiliteten i elnätet genom att slå av och på hackade hushållsapparater.

Industriella informations- och styrsystem, så kallade SCADA-system (*supervisory control and data acquisition*), byggs allt mer upp av standardkomponenter och det blir därför allt vanligare med pc-plattformar och kommunikationslösningar byggda på standardprotokoll (TCP/IP). Följden blir att fler it-komponenter förs in i fler funktioner vilket ökar antalet kommunikations-vägar – och därmed attackvektorer – in till de industriella informations- och styrsystemen [22].

Det är också svårt att installera antivirusprogram: realtidskritiska styrsystem i SCADA-världen kan inte riskera att plötsligt tappa prestanda eller startas om när antivirusprogrammet gör något och en femkronors-sensor i ”sakernas internet” kan inte utrustas med ett skydd för hundratals kronor. Stora företag inom nätverk och datorkommunikation gör nu analysen att tiden när säkerhet kunde hanteras i varje apparat är slut [23]. En sådan utveckling ställer istället ökade krav på löpande bevakning av nätverk och på lägesförståelse i en komplex arkitektur [24].

3. Privatlivet, informationsexplosionen och säkerheten

- *Frågorna om privatlivet aktualiseras allt mer när större mängd och fler typer av data blir tillgängliga i det moderna samhället.*
- *Den ökade delningen av information ger ökad osäkerhet om vem som äger data.*
- *Snabb teknikutveckling gör författningar och regler kring elektroniskt informationsutbyte mellan myndigheter föråldrade, vilket försvårar både önskvärda systemintegrationer och skyddet för privatlivet.*

Mängden elektroniska data växer allt snabbare i det moderna samhället. År 2013 rapporterades det att 90 % av alla data i världen hade tillkommit de senaste två åren [25] och den utvecklingen har bara accelererat. En stor datakälla är användargenererat innehåll i form av bilder, filmklipp, statusuppdateringar och blogginlägg som läggs ut på internet. I takt med att upplösningen i övervakningskameror förbättras och algoritmer blir allt bättre på att identifiera människor och mönster kommer övervakningskameror att generera allt mer information, och mänskliga väktare bli allt sällsyntare. Denna informationsexplosion har satt privatlivet på agendan och lett till mycket diskussion om vem som äger data och hur den får nyttjas.

3.1 Privatlivet på agendan

I juli 2012 gav regeringen Verket för innovationssystem uppdraget att utveckla öppnadata.se, en teknisk plattform för förmedling av öppna data. En bärande idé är att genom e-tjänster förenkla vardagen för medborgare och företagare och effektivisera den offentliga sektorn [26]. I februari 2014 presenterade den så kallade PSI-utredningen sitt slutbetänkande om hur det europeiska PSI-direktivet (*public sector information*), med minimiregler för vidareutnyttjande av handlingar som finns hos offentliga myndigheter, ska omsättas i svensk lag [27]. Bland annat föreslogs åtgärder som kan göra det enklare att använda myndighetsinformation för att utveckla nya tjänster och produkter. Utredningen noterade dock

även att den ökade digitaliseringen och spridningen av information medför en risk för otillbörliga intrång i den personliga integriteten. Speciellt uttryckte man viss oro över möjligheten att begära ut stora mängder offentliga handlingar på papper och sedan skanna in dem till maskinläsbart format. Allt detta tyder på att frågorna om privatlivet kommer att aktualiseras allt mer i takt med att fler typer av data blir tillgängliga.

Den svenska debatten om bruk och missbruk av offentliga handlingar tog fart 2014 i samband med turerna kring Lexbase, en internettjänst där man kan söka efter personer som varit föremål för rättslig prövning i svenska domstolar. Förutom att den vilseledande presentationen av innehållet i Lexbase ledde till stark kritik är tjänsten också ett exempel på hur illa genomtänkta lösningar får oförutsedda konsekvenser. Eftersom vem som helst som var betalande kund kunde fråga databasen om vad som helst publicerades hela databasen med personuppgifter på nätet kort efter starten, med ödesdigra konsekvenser både för folks privatliv och för företagets affärsmodell.

3.2 Osäkerhet kring vem som äger data

Till dataexplosionen hör också en ökad osäkerhet kring vem som äger data. Detta gäller både privatpersoners ägande av uppgifter om dem själva och oklarheter i kontraktsförhållanden mellan företag eller myndigheter. Frågorna om vad som är legitim användning, juridiskt och moraliskt, av de stora datamängderna i dagens samhälle diskuteras allt mer.

Offentlig information från myndigheter görs i många länder tillgänglig på internet, oftast med gränssnitt som är tänkta att underlätta maskinell inläsning och databehandling. Det finns även en marknad där myndigheter säljer data om privatpersoner. Ett sådant exempel är Skatteverkets databas SPAR. En ny marknad har också tillkommit i och med att företag numera köper information om vad privatpersoner gör på sina datorer, surfplattor och smarta telefoner direkt från användaren för en månatlig lön. Därmed blir individen i större omfattning den som kan tjäna pengar på sina egna data. Marknadsvärdet beror på den höga datakvaliteten i professionellt och frivilligt insamlade data, men också på att traditionella webbannonser numera har mindre än 0,01 % chans att bli klickade på. Möjligheten till smartare marknadsföring gör förstklassig information om konsumentbeteende värdefull i nästa led [28].

3.3 Öppenhet och skydd av uppgifter i offentlig förvaltning

I den svenska offentliga förvaltningen är det en stor utmaning för aktörerna att upprätthålla både öppenheten i offentlighetsprincipen och skyddet av privatlivet i personuppgiftslagen. Tyvärr riskerar kompromisslösningar att leda till brister i båda. Den långa livslängden hos både information och tekniska system gör det inte lättare. Lösningar måste hålla många år in i en osäker framtid. Det finns starka tekniska och organisatoriska drivkrafter för att integrera system mellan myndigheter, men styrmedel och regelverk för den offentliga sektorn hänger inte alltid med.

Ett exempel på problem är att patientdatalagens bestämmelser kring sekretess skiljer sig åt beroende på om informationsutbytet sker mellan olika vårdgivare eller inom samma vårdgivare, vilket har lyfts fram av Riksrevisionen [29]. I en granskning av elektroniskt informationsutbyte mellan olika myndigheter konstateras också att reglerna – oftast en kombination av offentlighets- och sekretesslagen, personuppgiftslagen och lagstiftningen för själva sakområdet – har en svåröverskådlig struktur. Sammantaget innebär detta att myndigheterna har svårt att veta vilken information som får utbytas och hur elektroniskt informationsutbyte får ske [30].

I juni 2014 föreslog E-delegationen ett antal ändringar i sekretesslagstiftningen, dels i syfte att underlätta för myndigheter att samverka, dels i syfte att ge förbättrad service och skydd för dem som använder e-tjänster. Om en myndighet ska kunna utkontraktera it-drift till en annan myndighet måste samma sekretess gälla hos leverantören som hos beställaren. För att det inte ska uppkomma luckor i sekretessen föreslogs en bestämmelse om överföring av gällande sekretess [31].

Ur ett säkerhetsperspektiv är det värt att notera att det är väldigt svårt att förutsäga hur den information som tillgängliggörs från olika källor kan kombineras och vilka slutsatser som då kan dras. Forskningsresultat visar exempelvis att amerikanska socialförsäkringsnummer går att utläsa utifrån offentligt tillgängliga data, trots att dessa är avsedda att vara privata [32]. Ny forskning visar också att det är förvånansvärt lätt att peka ut enskilda individer även i databaser där personuppgifter har tagits bort eller modifierats i anonymiseringssyfte [33]. I de stora datamängder som idag finns tillgängliga kan man inte bortse från risken att någon kan hitta och utnyttja en specifik verksamhets viktiga data, eller åtminstone finna en väg in till dem.

4. Den säkerhetspolitiska dimensionen av informationssäkerhet

- *Informationsoperationer där internetbaserad propaganda kombineras med diplomati, lögner, medieutspel och traditionell militär verksamhet har blivit vanligt förekommande i väpnade konflikter.*
- *Cyberspionage och cybersabotage är en del av "den säkerhetspolitiska verktygslådan" i allt fler länder.*
- *Internets ökade möjligheter till fri och svårkontrollerad kommunikation har medfört motreaktioner i många stater, med försök att isolera sina nationella nät från internet.*

Freedom House, en amerikansk icke-statlig organisation som sedan 1941 mäter och verkar för demokrati i världen, konstaterade 2013 att den globala friheten på internet har minskat tre år i rad. Enligt rapporten hade friheten minskat i 34 och ökat i 16 av 60 undersökta länder [34]. Blockering och filtrering av oönskat politiskt och socialt innehåll är på frammarsch, främst i auktoritära länder som Kina, Iran och Saudiarabien, men också i demokratier som Sydkorea.

Den här negativa utvecklingen går delvis på tvärs med den positiva bild av internet som en kraft för frihet som etablerades i samband med den arabiska våren 2011. Medan det då var populärt att tala om ”Twitter-revolutioner” är bilden idag mer nyanserad. En genomgång av forskningslitteraturen visar att flera parallella trender samexisterar [35]: de nya digitala arenorna kan visserligen möjliggöra för människor att utbyta information och avslöja missförhållanden, men de erbjuder också nya möjligheter till censur och desinformation.

4.1 Informationsoperationer i väpnade konflikter

Det är tydligt att användningen av informationsoperationer i konflikter är här för att stanna. Ett antal aspekter på informationskrigföring skildras i en FOI-rapport om Rysslands annektering av

Krim [36]. I februari 2014 publicerades påstått autentiska e-postmeddelanden som antydde att de nya ukrainska ledarna styrdes från väst, läckta av någon som kallade sig Anonymous Ukraine – en historia som blåstes upp i ryskkontrollerad media [37]. Ryska myndigheter beordrade därpå blockering av pro-ukrainska grupper på sociala nätverk i Ryssland [38]. Även framstående oppositionella ryssar som Aleksej Navalnyj och Garri Kasparov fick vid ungefär samma tidpunkt se sina webbplatser officiellt blockeras av de ryska myndigheterna [39]. Hemsidor för ukrainska myndigheter och både pro-ryska och pro-ukrainska nyhetsredaktioner utsattes därefter för överbelastningsattacker där det inte gick att fastställa vem som låg bakom [40]. Den ukrainska säkerhetstjänsten rapporterade om intrång med skadlig kod i parlamentsledamöters mobiltelefoner [41] och teleoperatören *Ukrtelecom* meddelade i inledningen av Krim-operationen att fiberkablar hade kapats och att uniformerad personal hade tagit över deras knutpunkter [42].

Mest slående var kanske ändå vad som kan uppfattas som en samordning mellan olika sätt att bedriva informationskrigföring: det budskap som levererades från den ryska politiska ledningen, dess diplomatiska beskickningar och rysk statskontrollerad internationell media som RT (tidigare Russia Today) fick sannolikt understöd av läckta telefonsamtal med amerikanska [43] och estniska [44] diplomater. De avlyssnade diplomatsamtalen antyder att kvalificerad signalspaning användes för att få mediegenomslag som spred tvivel och osäkerhet i västvärlden. Denna information spriddes på sociala medier och plockades därefter upp av traditionella media.

Informationsoperationer kompletterade den traditionella militära verksamheten och var en viktig faktor för den ryska framgången i Krim-operationen, konstaterar FOI [36]. En likartad bedömning görs av norska Forsvarets forskningsinstitutt: ryska cyberangrepp på viktiga ukrainska kommunikationskanaler syftade till att styra kommunikationsmöjligheterna för utvalda målgrupper, och samtidigt som Krim kommunikationsmässigt skars av från omvärlden genomfördes en massiv informationskampanj riktad mot västvärlden i syfte att få ut ett budskap om legitimiteten i det ryska agerandet [45]. Liknande exempel kan hämtas från andra moderna konflikter. Den Islamska staten (IS), som verkar i Syrien och Irak, använde under hela sin offensiv sommaren

2014 skickligt det moderna medielandskapet för att förmedla sin propaganda och sätta skräck i sina motståndare. Även om det i varje enskilt fall ligger i sakens natur att det är oklart både vilken sida som står bakom vilka handlingar och vad som görs av statsaktörer respektive frivilliga enskilda, så står det klart att moderna krig utspelar sig både i den fysiska miljön och i informationsmiljön. Stridsvagnar och truppförflyttningar är alltjämt pusselbitar, men skadlig kod och propagandistiska ”Twitterbotar” kan också vara det.

Även om det är en tydlig trend att it i allmänhet och olika sorters cyberattacker i synnerhet används mycket i moderna konflikter så betyder det inte att de alltid är effektiva. Forskaren Emilio Iasiello har undersökt några av de mest uppmärksammade fallen på senare år och är skeptisk: Om Ryssland genom cyberattackerna mot Estland 2007 försökte påverka landet så väckte man förvisso mycket uppmärksamhet. Men bronsstatyn flyttades likafullt, Estland förde upp cyberfrågorna i Nato och är fortsatt gediget västorienterat. Om USA eller Israel genom Stuxnet försökte sinka Irans kärnvapenprogram så lyckades man förvisso skapa en del problem på kort sikt. Men i ett längre tidsperspektiv är det inte alls säkert att Irans förmåga eller vilja att bli en kärnvapenmakt påverkades [46]. Det står dock klart att det finns många resursstarka aktörer som försöker nyttja sårbarheter i it-system och rutiner för att skaffa sig fördelar. Det finns också ett mörkertal: de mest kvalificerade cyberattackerna har sannolikt aldrig avslöjats, och deras effekter kan därför inte öppet utvärderas. Det är viktigt att vara medveten om att det finns en kvalificerad hotbild som berör många delar av samhället.

4.2 Cyberspionage och cybersabotage

Frågor om cyberspionage tar också allt mer plats på den diplomatiska arenan. Det amerikanska beslutet att åtala kinesiska cyberspioner våren 2014 är ett exempel på hur en juridisk mekanism som sannolikt aldrig kommer att leda till något straff används för att sända ett diplomatiskt budskap. Skarpare konsekvenser får då de amerikanska importhinder som drabbar exempelvis Huawei och det motsvarande kinesiska förbudet mot Appleprodukter hos myndigheter som offentliggjordes i augusti 2014. Bakgrunden är en rädsla för att företagshemligheter blir stulna och att det egna landets konkurrenskraft därmed undergrävs.

Medan det är lätt att bedöma effekterna av att politiska förhandlingspositioner eller militära planer stjäls – här är skadan skedd så fort de hamnar hos någon annan – är effekterna på konkurrenskraft och ekonomi svåra att bedöma. Här måste man nämligen ta hänsyn både till vilken information som stjäls och till tjuvens förmåga att omsätta det stulna i kommersiellt gångbara produkter.

Ett annat hot som spelar roll för mellanstatliga relationer, men även för enskilda företag, är inplanterade sårbarheter i hård- eller programvara från utländska leverantörer. Detta föder en vilja att istället köpa inhemskt, åtminstone till militära och civila ledningssystem på högsta nivå. Om detta blir vanligt betyder det emellertid att varje land får sämre produkter, eftersom konkurrens från utlandet gör den inhemska industrin mer innovativ och bättre på att använda teknikens möjligheter [47]. Teknisk eftersläpning och dyrare it är priset för ökad säkerhet mot inplanterade sårbarheter, åtminstone så länge de inhemska leverantörerna inte infiltreras. Samma dilemma gäller på tjänstesidan: it- och telekomtjänster köpta från utlandet utgör potentiella säkerhetsrisker, men forskningen har visat att fri handel med tjänster i det långa loppet leder till bättre tillväxt [48].

Den här utvecklingen medför nya utmaningar både för myndigheter, säkerhets- och underrättelsetjänster och för privata företag.

4.3 Hotet mot det öppna internet

Freedom House, vars mätningar ofta används i akademiska studier, noterar i sin analys av friheten på internet 2013 en trend av fler it-angrepp mot oppositionella: i 31 av de undersökta länderna har de styrande angripit sociala nätverk, avlyssnat kommunikationer och slagit ut webbplatser, bland annat genom användning av skadlig kod. Trenden går också mot ökad övervakning: i två tredjedelar av de undersökta länderna ökade statens juridiska eller tekniska förmåga till avlyssning under 2013. En annan juridisk trend är att mer ansvar läggs på mellanhänder som internetleverantörer eller plattformsägare för innehåll. Mest extremt är Kina, där censuren i stor utsträckning är outsourcad till tidningsredaktioner och internetleverantörer som mer eller mindre manuellt går igenom och raderar tiotals miljoner inlägg per år [49].

Internets status har också seglat upp som en het diplomatisk fråga. På ett möte med den Internationella teleunionen, ITU, i Dubai i slutet av 2012 blev konfliktlinjerna mellan å ena sidan USA och EU och å den andra sidan Ryssland och Kina tydliga. De sistnämnda ville se en framtida modell för *internet governance* där FN-organet ITU skulle få en utökad roll – vilket de förstnämnda såg som ett förtäckt sätt att möjliggöra mer censur och statlig styrning. Konflikten var ingen överraskning: Ryssland har under många år försökt bygga internationell acceptans för sin agenda inom vad man kallar ”internationell informationssäkerhet” [50]. I september 2011 skrev Ryssland, Kina, Tadzjikistan och Uzbekistan ett brev till FN:s generalsekreterare där man uppmanade medlemsländerna att samarbeta för att stoppa spridningen av information som underminerar stabiliteten i andra länder [51]. Det ryska budskapet är att alla världens länder möter gemensamma utmaningar som cyberbrottslighet, cyberterrorism och cyberkrig och därför måste samarbeta, helst i FN. Områden som yttrandefriheten på nätet, där det råder påtagliga motsättningar, nämns dock inte.

På den stora NETmundial-konferensen som hölls i Brasilien i april 2014, med deltagare från näringsliv, civilsamhälle och stater från 97 länder, antogs emellertid mänskliga rättigheter inklusive yttrandefrihet som bärande principer för den globala internetpolitiken. Det uppfattades som en framgång för den linje som bland annat Sverige driver. Allt fler länder försöker emellertid att på olika sätt isolera sina nationella nät från resten av internet, ett fenomen som på engelska kallas *splinternet* [52]. Om den trenden fortsätter så går vi mot ett fragmenterat internet, där allt fler lever i informationsbubblor. Det kan komma att påverka inte bara diplomati, opinionsbildning och samhällsdebatt, utan också internationella företag och rentav den gränsöverskridande nätbaserade brottsligheten, *crime-as-a-service*.

5. Brottslighet i informationssamhället

- *Dagens it-relaterade organiserade brottslighet har oftast ekonomiska drivkrafter och en internetbaserad kriminell tjänstesektor, crime-as-a-service, har vuxit fram på senare år.*
- *Samspelet mellan traditionell och elektronisk brottslighet ökar och blir allt mer komplext.*
- *Dagens brottslighet ställer nya krav på rättsväsendet, inte minst vad gäller samverkan med utländska polismyndigheter och privata aktörer.*

Idag har så gott som all brottslighet en it-koppling. Mest uppenbart är det naturligtvis för brott som till sin natur kräver modern teknik, som datorbedrägeri och dataintrång [53]. Men det moderna samhällets kommunikationsvägar är sådana att även brott som häleri, bidragsfusk, kreditkortsbedrägerier och bluffakturor nästan per definition har stora elektroniska inslag idag. Ofta handlar det alltså om gamla brott i ny skepnad.

5.1 En ny internetbaserad kriminell tjänstesektor

Specialisering och arbetsdelning sker även bland kriminella. Teknikutvecklingen har underlättat framväxten av en kriminell internetbaserad tjänstesektor, *crime-as-a-service*. Brottslingen behöver därmed inte göra allt själv, utan kan köpa färdiga komponenter och sätta ihop dem i sitt eget syfte. Ett sådant exempel är webbhotell som ger kriminella säkerhet, driftsäkerhet och anonymitet och som sällan samarbetar med polisen [54]. Genom att sätta upp dessa tjänster i länder med svag eller obefintlig it-lagstiftning blir det extremt svårt att få servrarna nedstängda eller att spåra vem som ligger bakom [55].

Ett annat exempel på ekonomiskt driven brottslighet är *malware-as-a-service*: färdiga lösningar med skadlig kod som kan återanvändas i olika sammanhang. Denna verksamhet blir allt bättre på att tillhandahålla tjänster som liknar kommersiella företag såsom kundsupport, kontinuerliga uppdateringar och

utveckling av produkter. Skadlig kod möjliggör mycket av den brottslighet mot våra informationssystem som vi ser idag. Den tekniska utvecklingen av mobila enheter har gjort dessa mer lukrativa att attackera och hotet har ökat kraftigt de senaste åren. Banksektorn är också mycket utsatt: att kriminella stjäl inloggningsuppgifter eller fångar upp koder vid tvåvägsautentisering blir allt vanligare. Det finns också en trend där man istället för att rikta in sig mot bankkunderna genom massinfektioner riktar in sig mot tjänsteleverantörer som lagrar stora mängder kundinformation. Genom att skapa en bakdörr eller trojan hos en sådan aktör kan stora mängder av personliga data stjälas och säljas.

Så kallad *ransomware* är skadlig kod som installeras på offrets dator som sedan gör det möjligt för gärningsmannen att kryptera datorn alternativt delar av material på datorn. Gärningsmannen kräver sen målsägaren på pengar för att denne ska återfå kontrollen över sin egen dator alternativt det material som krypterats. Ransomware-fallen har ökat kraftigt i Europa de senaste två åren. Metoden är lukrativ eftersom den genererar mycket pengar med liten risk för lagföring. Digitala valutor och förbetalda betalkort har gjort det enklare för de kriminella att komma undan med brottsvinsterna. Ransomware-attacker kan lätt iscensättas av kriminella som saknar särskild teknisk kompetens i och med att tjänsterna lätt går att köpa online. Problemet kring dessa ärenden försvåras också av att aktörer och infrastrukturer inte sällan finns utomlands. Sverige har visserligen inte drabbats lika hårt som många andra delar av Europa men det finns kända fall i Sverige. Ransomware finns både för datorer och mobila enheter [56].

Antivirusföretaget McAfee uppskattade 2014 världens årliga kostnader för cyberbrott till 445 miljarder dollar, där man räknat med både värdet på det som stjäls och offrens kostnader för skydd och återställning [57]. Konkurrenten Symantec uppskattade 2013 samma siffra till mer modesta 113 miljarder dollar, varav de svenska kostnaderna uppges vara 838 miljoner dollar [58]. Precis som med all brottsstatistik finns det dock mörkertal. Alla företag upptäcker inte att de har utsatts för intrång och alla som upptäcker det vill inte berätta om det. Ett skäl att tiga är rykte och börsvärde: forskning visar att it-problem i företag påverkar aktiekursen negativt [59]. Samtidigt har säkerhetsföretagen ett intresse av att överdriva hotet [60].

Tyvärr finns det gott om enkla mål för ekonomiskt driven it-brottslighet, exempelvis i form av datorer som inte har försetts med de senaste säkerhetsuppdateringarna. En studie av 1 424 mjukvaru-sårbarheter som hackare har skrivit skadlig kod för, visade att över 30 % av den skadliga koden hade skrivits *efter* det att säkerhetsuppdateringen hade släppts [61]. Det visar tydligt att långsamma uppdateringsrutiner erbjuder lukrativa mål och understryker vikten av att uppdatera och underhålla sina system.

5.2 Samspelet mellan traditionell och elektronisk brottslighet

Ett exempel på hur traditionell organiserad brottslighet utnyttjar modern teknik kommer från hamnen i Antwerpen, Belgien. I juni 2011 infiltrerades två företagsnätverk i hamnen av holländska hackare. Deras uppdragsgivare var narkotikasmugglare från Sydamerika som gömde kokain och heroin tillsammans med lagligt gods i containrar. Genom datorintrånget kunde de kontrollera containrarnas ankomst, placering och säkerhet så att de kunde hämta godset innan de rättmätiga ägarna hann fram för upphämtning. Efter två år uppmärksammades detta av hamnarbetare som såg containrar förvinna utan förklaring. Det är oklart hur mycket narkotika som hann passera, men över två ton kokain och heroin samt en dryg miljon euro kunde tas i beslag. Värt att notera är också att den första it-attacken, där man försökte komma åt systemen genom att skicka skadlig e-post, misslyckades. Brottslingarna gav sig då istället på den svagaste länken genom att fysiskt bryta sig in på kontoren för att installera utrustning för avlyssning och systempåverkan [62]. Detta samspel mellan traditionell och elektronisk brottslighet ställer nya krav på rättsväsendet och dess förmåga att utreda komplexa brott.

En stor del av internet består av sidor och tjänster som inte indexeras eller är åtkomliga av vanliga sökmotorer. På dessa slutna nätverk finns en stor marknadsplats för kriminella varor och tjänster, så kallade *dark markets*. Handeln har ökat markant, främst när det rör narkotika men också identitetshandlingar, vapen, skadlig kod och dokumenterade sexuella övergrepp mot barn. Silk Road är ett exempel på en sådan marknadsplats som stängdes av amerikansk polis i oktober 2013. Trots att stängningen då beskrevs som ett genombrott i bekämpandet av nätförsäljning av droger finns det uppskattningar som tyder på att försäljningen idag är dubbelt så stor som under Silk Roads storhetstid. På bara

två år fick Silk Road 200 000 registrerade användare och nådde en omsättning på en miljard amerikanska dollar under perioden [63]. Droghandeln på internet har utvecklats och idag går det att beställa bolivianskt fairtrade-kokain eller -opium från icke våldsanvändande producenter.

I syfte att försvåra utredningar och sopa igen spåren efter sig har stora delar av den kriminella ekonomin traditionellt varit kontantbaserad. I takt med att andra betalningsmetoder vuxit fram för helt legala ändamål har den kriminella världen varit snar att haka på. Ett exempel är så kallade förbetalda betalkort, där en summa sätts in på exempelvis ett VISA-kort som sedan kan användas för betalningar utan att det går att ta reda på vare sig vem som genomfört köpet eller varifrån pengarna ursprungligen kom. Idag fyller så kallade kryptovalutor, varav bitcoin är den mest kända, i mångt och mycket samma funktion. Bitcoin är en valuta och ett elektroniskt betalningssystem i ett och är populärt bland kriminella av samma skäl som kontanter är det – transaktioner som gjorts kan inte ångras och är svåra att knyta till specifika individer. Därför är bitcoin eller andra kryptovalutor i princip allenarådande betalningssätt på så kallade *dark markets*. Tyvärr riskerar detta att ge nya tekniska lösningar dåligt rykte och stävja innovationer: bitcoin har också stor potential på helt legitima områden som gräsrotsfinansiering, donationer och säkra transaktioner [64]. Att hitta en välfungerande reglering av digitala valutor som försvårar kriminell användning utan att undergräva de goda effekterna är en viktig framtidsutmaning.

5.3 Dagens brottslighet ställer nya krav

Även om lagen är densamma i den fysiska och den elektroniska världen så påverkas människors beteenden av de skiftande förutsättningarna. Tyvärr tycks tröskeln för att hota och kränka personer anonymt på internet vara lägre jämfört med att säga samma saker öga mot öga. Dessutom blir de tekniska förutsättningarna i utredningen mer komplicerade när förövare kan dölja sig med anonymiseringstjänster och när plattformar och infrastruktur som används för att sprida budskapet inte sällan finns i utlandet. På så sätt har brott som olaga hot och förtal nu fått påtagliga inslag av informationssäkerhet.

Ett annat brott som har vuxit till ett stort samhällsproblem på senare år är identitetstölder. När en identitet har kapats kan förövaren snabbt ta lån och handla varor på internet. Både företag och enskilda drabbas. Det är vanligt att identiteter kapas och används för att starta bolag som sedan begår brott. En reaktion på detta är det förslag om en ny straffbestämmelse för identitetsintrång som lämnades av Egendomsskyddsutredningen (SOU 2013:85) i december 2013 [65]. Brottet föreslås kunna bestraffas med böter eller fängelse i upp till två år.

Den 23 november 2001 signerade Sverige tillsammans med ett antal andra stater Europarådets konvention om it-relaterad brottslighet (ETS nr. 185), även kallad Budapestkonventionen. Konventionen syftade bland annat till att harmonisera konventionsstaternas lagstiftning och underlätta internationellt samarbete. Den rekommenderade därför att staterna borde inrätta brottet grovt dataintrång, vilket Sverige gjorde den 1 juli 2014. Brottet kan ge lägst sex månaders och högst sex års fängelse. I och med den nya lagen är även försök och förberedelse till grovt dataintrång straffbart. Sverige har dock ännu inte ratificerat konventionen, eftersom det pågår en översyn av de författningsändringar som behövs för att Sverige ska kunna leva upp till dess krav [66].

Eftersom den it-relaterade brottsligheten ofta är internationell har det funnits ett behov av harmonisering, samordning och stöd till polisen. Därför bildades EC3 (European Cybercrime centre) den 1 januari 2013 vid den europeiska polissamarbetsmyndigheten Europol. Med detta som grund finns det idag också ett beslut om att inrätta ett liknande nationellt it-brottscentrum i Sverige i samband med att den nya polismyndigheten bildas den 1 januari 2015. Detta för att bättre hantera it-relaterad brottslighet och uppfylla it-brottskonventionens krav.

6. Kapplöpningen mot den svagaste länken

- *Förekomsten av programvara som identifierar sårbarheter samt enkla och billiga tekniska hjälpmedel för angrepp har sänkt tröskeln och satt verktyg i händerna på fler angripare. Samtidigt är de allra mest kvalificerade angreppsverktygen fortfarande hårdvaluta och förbehållna en mindre krets.*
- *Trots de tekniska sårbarheterna är människan i systemet ofta den svagaste länken, som kan luras att ladda ner skadlig kod eller uppge känsliga uppgifter.*
- *Även om allt fler organisationer inför bestämmelser för informationssäkerhet är steget från bestämmelse till faktisk säkerhet långt.*

Angripare är ständigt på jakt efter den svagaste länken. Teknik, användare, organisation och regelverk rymmer alla potentiella svagheter som kan utnyttjas. Vad som ger störst effekt varierar över tiden och mellan olika sammanhang. Ett exempel på ett aktuellt område är appar i mobiltelefoner och läsplattor – apparater som vi alltid bär med oss och som innehåller allt mer känslig information. Även om den största studien av app-säkerhet hittills inte hittade någon skadlig kod eller sårbarheter som direkt gick att utnyttja i de 1 100 mest populära gratis Android-apparna [67] så publiceras ständigt nya exempel på sårbarheter. Exempel på detta är hur kamerafunktionaliteten kan missbrukas [68] eller hur man kan kringgå granskningen i Apples App Store [69]. Det går aldrig att slå sig till ro – kapplöpningen mellan angrepp och försvar pågår ständigt.

6.1 Teknik för angrepp

Programvara för angrepp av olika slag blir allt lättare att få tag på. Att genomföra ett osofistikerat angrepp kräver i och med detta inte längre någon stor kompetens och tröskeln för angrepp sänks. I Sverige har ett antal överbelastningsattacker mot såväl skolor [70] som kommuner [71], [72] uppmärksammats på senare år, även om mörkertalet gör trenden svår att bedöma. Förekomsten av sådana relativt enkla attacker hänger troligen ihop med ökad

tillgänglighet på verktyg. För de mest kvalificerade angreppsverktygen är läget annorlunda. Exklusiv information om sårbarheter i känsliga system betingar ett högt värde. Attacker som utförs med hjälp av sådana hålls väl dolda och når tidningsrubrikerna först långt i efterhand, om någonsin.

Så kallade överbelastningsattacker med *amplifiering* tycks bli allt vanligare och ett flertal uppmärksammade attacker har skett på senare år [73]. Här används bland annat adresseringen i internets domännamnsystem på ett sådant sätt att många tredjepartsdatorer luras att sända trafik till offret i större omfattning än vad dennes system kan hantera. Därmed uppnås en multiplikatoreffekt. För att motarbeta den här trenden måste organisationer mer systematiskt börja se över alla tjänster exponerade mot internet i jakt på sårbarheter. Många fler tjänster än Domain Name System, DNS, har dessa egenskaper, och kan användas för amplifiering.

Information om internetuppkopplade sårbara datorsystem blir allt lättare att hitta på internet, vilket sänker tröskeln för angrepp. År 2013 lyckades forskare kartlägga hela internet (mer precist hela IPv4-adressrymden) på under en timme [74]. En sådan skanning hittar blixtsnabbt miljoner sårbara apparater – och möjliggör för angripare att omedelbart börja utnyttja nyfunna sårbarheter i stor skala. Ett forskningsprojekt vid Cambridge letade efter internetanslutna SCADA-system och hittade tusentals, de flesta utan lösenordsskydd och många med kända sårbarheter [75]. Det säger sig självt att sådan information är värdefull för en angripare. Kvalificerade angripare har naturligtvis länge kunnat samla in sådan information på egen hand, men existensen av samlingssidor på internet sänker trösklarna ytterligare för opportunister som letar efter lätta mål. Andras lagrade skanningsresultat gör det dessutom möjligt att studera sitt mål utan att själv skicka någon trafik till det.

6.2 Användaren är ofta den svagaste länken

Ofta är det emellertid inte tekniska sårbarheter som är den svagaste länken, utan användaren – människan i systemet. Beteendevetenskapliga forskningsresultat visar att vi är mycket benägna att själva dela med oss av våra personuppgifter på nätet [76]. Sådan information kan användas för angrepp på åtminstone två sätt. För det första använder många tjänster fortfarande personliga frågor för

att återställa glömda lösenord. I en värld av öppna data och gott om personuppgifter på nätet kan en angripare enkelt använda sådan information för att gå förbi lösenordsskydd. För det andra underlättas möjligheterna till manipulation (*social engineering)*.

Ett klassiskt exempel på s*ocial engineering* är nätfiske (*phishing*): e-post som under falska förespeglingar lurar offret att göra något skadligt. Även om det är en angreppstyp som har förekommit länge, utvecklas den ständigt och har blivit populärare eftersom klientsäkerheten generellt har förbättrats. Enligt säkerhetsföretaget Symantec skedde det en tydlig förändring i nätfiskarnas modus operandi under 2013, jämfört med tidigare år: medan antalet mottagare och antalet skickade brev per kampanj minskade förlängdes tiden under vilket varje försök pågick, från några dagar till en dryg vecka [77]. Sannolikt rör det sig om en medveten strategi för att minska upptäcksrisken.

När nätfisket förses med en falsk förtroendeingivande avsändare och riktas specifikt mot offret kallas det *spear phishing*. Ett svenskt experiment visar att riktat nätfiske är bättre på att lura användarna än oriktat [78]. Samtidigt ökar upptäcktsrisken: det oriktade meddelandet rapporterades aldrig till någon säkerhetsansvarig, vilket snabbt skedde med det riktade. Forskarna drar slutsatsen att angriparen under vissa omständigheter vill undvika alltför riktat nätfiske, eftersom sådant höjer upptäcktsrisken. Om riktat eller oriktat nätfiske är farligast går inte att säga generellt, det beror på kontexten.

Ett socialt liv på internet är standard för många idag. Många väljer att lämna ut personlig information och klicka på länkar trots medvetenhet om riskerna eftersom fördelarna är stora. Riskbeteendet ser dock olika ut mellan olika generationer, vilket gör det svårt att peka ut *en* trend på området. En holländsk studie har visat att äldre generationer är mer benägna att acceptera okända som kontaktar dem på nätet, medan unga gav ut mer information samtidigt som de oftare använde inbyggda säkerhetsinställningar [79]. Beteendeskillnader mellan användare kommer sannolikt att behöva tas med i beräkningen vid utvecklingen av framtidens säkerhetsutbildningar.

Människans begränsade förmåga att hålla många olika lösenord i huvudet är ett annat problem. Många webbsidor bygger på att besökarna skapar ett personligt konto med information som

lagras hos leverantören. För att skydda sådana system mot intrång används allt oftare krav på starkare lösenord och krav på dubbel autentisering (som säkerhetskoder via både sms och en annan e-post). Men långt ifrån alla tjänster använder sådana lösningar, och effekten blir att information om användarna stjäls och ibland publiceras.

6.3 Teknik för försvar och svårigheterna med att skapa säkerhet

Även försvarsmekanismerna automatiseras och produktifieras. Enligt konsultföretaget Gartner uppgick den globala marknaden för brandväggslösningar till 8,7 miljarder dollar 2013, med en tillväxt på 9 % jämfört med 2012 [80]. Det är avsevärt större än marknaden för skydd av enskilda maskiner (*endpoint protection*) som 2012 uppgick till 2,8 miljarder dollar – inte nämnvärt mer än 2011 [81]. Enligt Microsoft hade ungefär 75 % av all världens datorer under 2013 någon form av realtidsövervakande säkerhetsprogramvara som ständigt var påslagen [82].

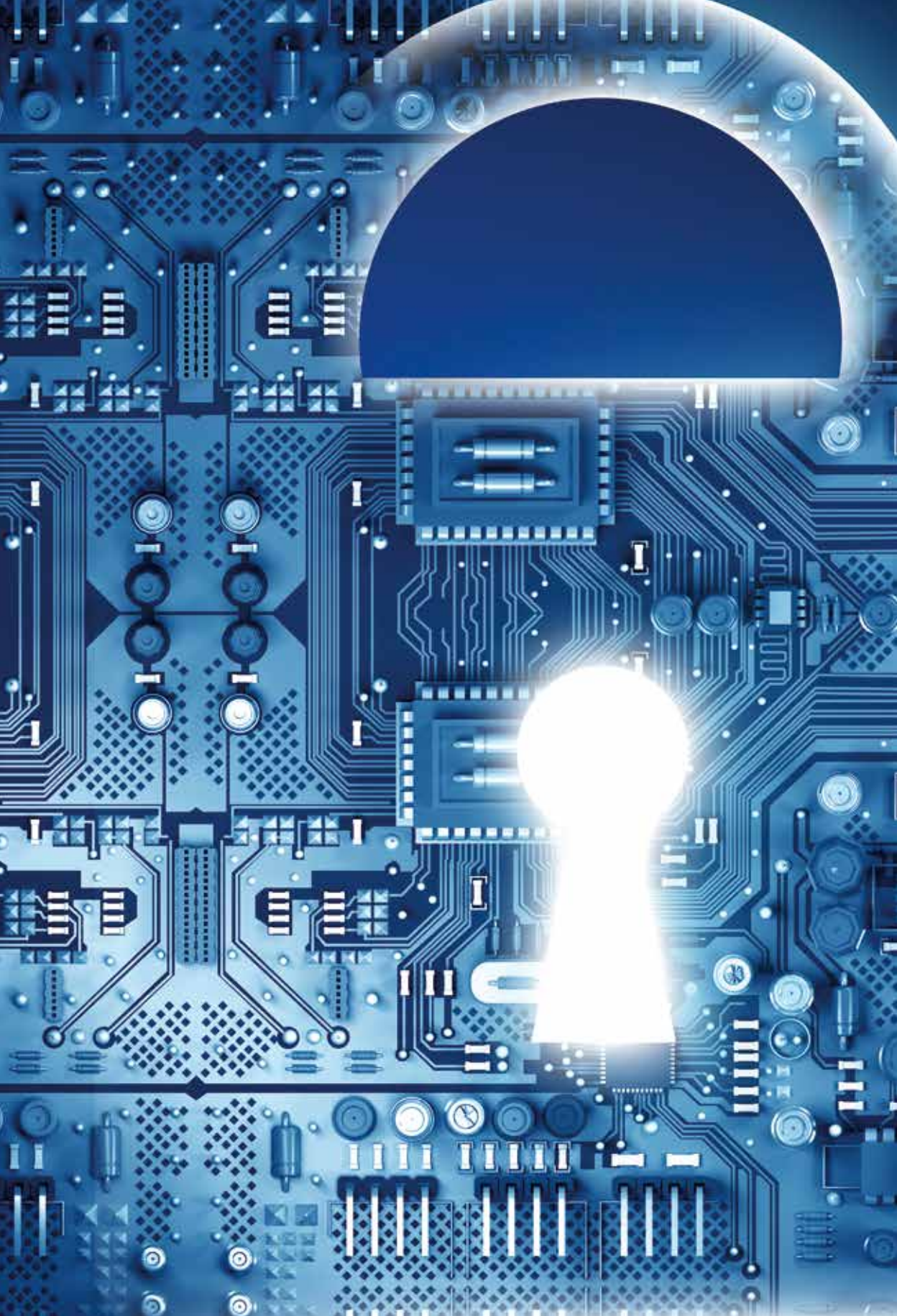
Samtidigt som skyddsverktyg är nyttiga är det också viktigt att inse deras begränsningar. En kvantitativ studie av sårbarhetsskannrar (som används för att hitta kända sårbarheter i operativsystem och annan programvara) visar att skannrar som försetts med relevanta inloggningsuppgifter till systemet hittar i storleksordningen 30–50 % av de kända sårbarheter som faktiskt finns där [83].

Intrångsdetektionssystem (IDS:er) används av många företag och organisationer, men de ger ifrån sig massor av falsklarm om de inte konfigureras rätt och kräver därför omfattande manuellt arbete för att bli användbara [84]. Samtidigt kan IDS:er överraska positivt. Det är lätt att tro att ett system som bygger på kända attackers signaturer inte förmår detektera nya, okända attacker (*zero days*). Ny forskning visar emellertid att det finns intrångsdetektorer som kan detektera även en del attacker som den ännu inte har någon signatur för, låt vara att förmågan är klart sämre än för de kända attackerna [85]. Kapplöpning mellan teknik för attacker och teknik för skydd pågår ständigt.

I Sverige utvecklar Försvarets radioanstalt (FRA) ett tekniskt detekterings- och varningssystem (TDV) som syftar till att upptäcka avancerade it-angrepp mot samhällsviktig verksamhet. Systemet ska förses med så kallade signaturer som erhålls bland

annat via signalspaning och systemet omfattas därför av försvarssekretess. Dessa signaturer ger systemet en förmåga att detektera it-angrepp som inte kan upptäckas med hjälp av kommersiellt tillhandahållna system för upptäckt av skadlig kod. Den information och erfarenhet som ett TDV genererar kan användas för att åstadkomma verkningsfulla skyddsåtgärder.

Många verksamheter försöker öka sin säkerhet genom bestämmelser för informationssäkerhet som användarna ska följa. För att bestämmelser ska ha en positiv påverkan på informationssäkerheten måste de dock efterlevas. Det räcker inte att ha dokumenten. Vetenskapliga studier visar att efterlevnaden av säkerhetsregler är en komplex fråga och att det inte finns några enkla sätt att garantera regelverkets genomslag [86]. Precis som med andra beteenden spelar den enskildes attityd, gruppers normer och det besvär som bestämmelserna medför stor roll. Däremot spelar förekomsten av hårda straff för att bryta mot bestämmelserna väldigt liten roll. En målbild för en informationssäkerhetskultur att sträva mot skulle därför kunna vara flygsäkerhetskulturen inom flygvapnet. Där rapporterar piloter utan att skämmas regelmässigt misstag som de gjort och stärker därmed den framtida säkerheten [87].



7. Robusta informationssystem och kontinuitet

- *I det moderna samhället blir konsekvenserna av driftavbrott i informationssystem större och mer oöverskådliga.*
- *Riskhantering och kontinuitetsplanering blir allt viktigare för att uppnå robusta informationssystem, liksom förståelse för den egna verksamhetens ofta allt mer komplexa it-beroende.*
- *Marknaden för cyberförsäkringar är i sin linda, men kommer att växa i framtiden.*

Tekniken har möjliggjort påtagliga fördelar: automatisering av manuellt arbete, skalfördelar i informationshantering och minskade transaktionskostnader för företag och konsumenter. Samtidigt medför vårt ökade beroende av fungerande teknik att konsekvenserna av driftavbrott – både ekonomiska och icke-ekonomiska – blir allt större och mer oöverskådliga.

7.1 Driftavbrott med oanade konsekvenser

Det är lätt att underskatta icke-antagonistiska hot: hot som inte kommer från någon motståndare utan från våra egna tillkortakommanden, kortsiktighet eller slarv. Encyclopedia of Information Assurance [88] konstaterar träffande att kontinuitet och återställning förmodligen är den del av informationssäkerheten som är lättast att bortse från och skjuta på. Den inställningen kan straffa sig. När en aktör med många kunder drabbas av driftstörningar kan konsekvenserna bli kännbara och oväntade på många olika håll samtidigt. Ett sådant exempel var då it-företaget Evry fick problem på nyår 2013, med följd att flera, vitt skilda, samhällssektorer fick problem med datatillgänglighet.

Även om de antagonistiska hoten är mer spännande ska inte det vardagliga kvalitetsarbetet underskattas. Buggar i program- och hårdvara, kvalitetsbrister i programvaruutveckling och avsaknad av eller slarv i rutiner vid mjukvaruuppdateringar kan skapa stora problem, vilket exempelvis Försäkringskassan fick känna av efter att ett fel i en programvara till en växel orsakade ett haveri i september 2014 [89].

Ett problem med att ägna för lite uppmärksamhet åt vanliga driftavbrott är att det dessutom kan öppna för antagonistiska angrepp. En kvalificerad motståndare som vill angripa ett ledningssystem kan mycket väl tänkas maskera sina angrepp som oregelbundet återkommande driftavbrott. Om den angripne inte har rutiner för att gå till botten med varje driftavbrott utan bara startar om systemet kan angreppet förbli oupptäckt. Motståndaren kan då införa friktioner och störningar upprepade gånger under en längre tidsperiod utan att behöva hitta en ny attackvektor. En studie baserad på data från säkerhetsföretaget Symantec visar att det kan ta åratal innan skadlig kod identifieras [90]. I augusti 2014 väckte en studie från KPMG stor uppmärksamhet, när det visade sig att 13 av 14 undersökta svenska företag och myndigheter hade infiltrerats med skadlig kod som stod i kontakt med en angripares kontrollserver någon annanstans i världen. Från 11 av organisationerna skickades det ut information – företagshemligheter av en eller annan art – till angriparen [91]. Den förhållandevis lilla urvalsgruppen gör studiens resultat svårbedömt, men en liknande studie som KPMG utfört i Finland visar på motsvarande resultat.

7.2 Allt viktigare med riskhantering och kontinuitetsplanering

Alltför få organisationer inser hur deras strategier och avtal påverkar återställningstiden efter oplanerade driftavbrott. Första steget till en mognare risk- och incidenthantering är att lära känna sin verksamhet och dess behov av kontinuitet och tillgänglighet. Ett företag, vars intäkter hänger på tillgängligheten i kortbetalningssystemet, vill hellre ha många korta avbrott än ett enstaka långt. Efter ett kort avbrott kan kunden dra kortet igen och knappt någon skada är skedd – men om ett långt avbrott inträffar i julhandeln kan det äta upp stora delar av årets vinst. För en industriprocess som ett stålverk eller ett pappersbruk vill man hellre ha enstaka långa avbrott än många korta. Varje avbrott där betyder ett stopp i en stor fysisk process, inklusive logistikkedjan, med påtagliga kostnader för återställning och omstart [92].

Tyvärr är mognaden inom incidenthantering fortsatt låg i många verksamheter. En studie gjord av MSB bekräftar den bilden: i en enkät besvarad av 334 svenska myndigheter visade sig 65 % sakna kontinuitetsplan [93]. Av de 35 % som faktiskt hade en plan är det bara 36 % som har övat på hur planen ska sättas i verket [93]. Användandet av standarder som Information Technology

Infrastructure Library, ITIL, eller Internationella standardiseringsorganisationen, ISO:s standard för kontinuitetshantering bidrar till att öka mognaden, men får inte effekt förrän de implementeras – vilket kan ta tid, givet de långa livscyklerna hos många affärssystem.

Kanske har företagsledningar ofta större riskaptit än de kontinuitetsansvariga. Vem har rätt? Detta sätter fokus på en oerhört central punkt: det är svårt att riskhantera rationellt utan överblick över verksamhetens it-beroende. En förändring har skett de senaste åren, från en situation med stuprörslösningar (lönesystemet för sig, säljsystemet för sig) till allt mer integrerade it-landskap, där affärssystemen hänger ihop med varandra, både inom och utom det egna företaget. Att styra och optimera logistikkedjor över flera leverantörsled med hjälp av it-integrationer sker exempelvis regelmässigt i många branscher idag [94]. Även om detta ökar effektiviteten och möjliggör helt nya affärsidéer så har det också lett till att många stora företag idag inte vet hur många it-system de har, hur de är sammankopplade eller exakt hur de stödjer verksamheten. Trenden att outsourca drift eller tjänster till tredjepartsleverantörer i molnet som bara kontrolleras via kontrakt (*service level agreements*, SLA) gör det ännu svårare att på ett effektivt och kvalitetssäkert sätt riskhantera hot. Eftersom det kan vara svårt att agera rationellt vid kontraktsskrivning [15] krävs god beställarkompetens.

Riskhantering uppmärksammas allt mer som en framkomlig väg att stärka informationssäkerheten i organisationer. Alltför många gör dock fortfarande inga riskbedömningar av sitt beroende av information för verksamheten i förväg, utan agerar improviserat när något händer. I en enkätstudie besvarad av 334 svenska myndigheter visade sig 59 % inte använda sig av riskanalyser som stöd vid kontinuitetsplanering [93]. Kring 40 % av myndigheterna visade sig dessutom sakna regler för vad riskanalyserna ska omfatta och för vem som ska initiera dem [93]. Att vända den trenden kommer att ta tid och kräver arbete på flera fronter. Svenskt Näringslivs vägledning ”Säkerhet vid anskaffning och utveckling av system” som slår fast att informationssäkerheten avgörs tidigt i livscykeln, i upphandling och utveckling, är ett exempel [95]. Det är viktigt att redan i upphandlingen specificera vem som bär ansvaret för vad under hela livscykeln. Likartade lärdomar finns i MSB:s ”Vägledning – informationssäkerhet i upphandling” [96].

7.3 Kostnaderna för it-incidenter och vikten av ekonomiska incitament

Det finns ingen tillförlitlig sammanställning av de totala kostnaderna för otillgänglighet hos it-system i Sverige. En undersökning gjord av Inspektionen för socialförsäkringen uppskattar att kostnaderna för spilltid vid fel och driftavbrott var 19 miljoner för Försäkringskassan och 1,7 miljoner för Pensionsmyndigheten år 2012 [97]. I kommersiell verksamhet kan kostnaderna vara mycket större. I samband med Stockholmsbörsens uppmärksammade avbrott i juni 2008 rapporterade Dagens Industri att ”miljardaffärer gick förlorade” [98] och enligt Computer Sweden uppgick Axfoods kostnader under ett fyra timmars långt kabelbrott som förhindrade kortbetalningar till 4,25 miljoner i timmen [99]. Ofta görs dock inga kostnadsuppskattningar ens på medialt uppmärksammade händelser som Tieto-haveriet i november 2011. Svårigheten att göra uppskattningar är också ett symptom på ett djupare problem: de flesta företag och verksamheter vet inte hur sårbara de är, de vet inte vad driftavbrott kan komma att kosta när de gör sin riskhantering och de har till och med i efterhand svårt att beräkna kostnaderna för inträffade driftavbrott.

En viktig faktor för riskhantering är ekonomiska incitament. Aktörer som verkar på en konkurrensutsatt marknad förefaller vara mer proaktiva än exempelvis kommuner. En särskild svårighet är att många offentliga aktörer samverkar avtalslöst med varandra och skulle behöva kunna ingå överenskommelser som svarar mot kommersiella avtal [18]. Utan ansvarsfördelning har de svårt att uppnå någon mogen incidenthantering. Här har alltså många kommersiella företag ett försprång framför offentliga aktörer. Utsattheten borde också spela en roll: aktörer som hanterar skyddsvärda uppgifter och företag med känsliga industriella processer torde vara mognare än många andra när det gäller riskhantering. Sammantaget kommer dessa faktorer förhoppningsvis över tid att leda till en ökad riskmedvetenhet, men faran är om det sker först efter ett antal incidenter med allvarliga konsekvenser. Dessutom leder generell mognad inom riskbedömning, till exempel avseende finansiella risker, inte alltid till mognad inom riskbedömningar av informationssäkerhet.

Ett sätt att åtgärda problemet med avsaknaden av riskbedömningar är genom en starkare koppling mellan it-risk och finansiell risk, exempelvis genom mognare cyberförsäkringar. Cybersäkerhetsmarknaden expanderar. I slutet av 2011 uppskattades den vara värd 750 miljoner dollar [100], medan en uppskattning 2014 pekar på att den vuxit till 2 miljarder dollar [101]. Den svenska marknaden är dock ännu i sin linda. I forskningslitteraturen har man framfört idén att stora aktörer som stater skulle kunna få igång en bättre fungerande cyberförsäkringsmarknad genom att gå först och köpa försäkringar [102]. Försäkringsbolag har en lång historia av att utifrån data ta fram riskprofiler och sätta premier baserat på riskbeteenden, vilket under vissa förutsättningar kan ge incitament för försäkringstagarna att jobba med sin egen säkerhet och därmed också höja säkerheten för alla andra [103]. Försäkringsbolagen skulle på en cyberförsäkringsmarknad kunna ställa krav på att aktörer tvingas betala en högre premie om man saknar vissa grundläggande skyddsmekanismer. I det avseendet kan försäkringar ge ekonomiska incitament för fler att lära sig av andras misstag snarare än av dyrköpta egna.

Samtidigt är det viktigt att inse att en försäkring inte ersätter behovet av internt säkerhetsarbete, lika lite som en brandförsäkring ersätter behovet av brandutbildning, brandvarnare och brandsläckare. En cyberförsäkring är ett avtal, där värdet på det som ska skyddas måste matchas med innehållet i försäkringen och villkoren för när den ska falla ut.

Slutord

Slutord

Det är mycket svårt att spegla den komplexa utveckling som pågår på området informationssäkerhet. Ämnet är, som framgår i denna rapport, oerhört brett. Än svårare är det att sia om framtiden. Teknisk utveckling är bara en av flera faktorer. Därtill kommer människans beteende, vad som händer i omvärlden, nya tjänster och enstaka händelser som uppmärksammas och påverkar vårt beteende. Området är ett komplicerat pussel där bilden hela tiden förändras. Förhoppningsvis bidrar denna rapport till att öka medvetenheten kring informationssäkerhetsområdet och faktorer som kan vara viktiga att ta hänsyn till framöver, särskilt för beslutsfattare inför beslut som påverkar informationssäkerheten.

Referenser

Referenser

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, High representative of the European Union for Foreign affairs and Security policy, 2013. Joint communication to the European parliament, the council, The European economic and social committee and the Committee of the regions, tillgänglig via http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, läst 2014-10-13.

[2] OECD. Review of the 2002 Security Guidelines. http://www.oecd.org/sti/ieconomy/2002-security-guidelines-review.htm, december 2013. Läst 2014-06-30.

[3] Anindya Ghose och Uday Rajan. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. I: *Fifth Workshop on the Economics of Information Security*, 2006.

[4] Alberto Portugal-Perez, José-Daniel Reyes och John S Wilson. Beyond the information technology agreement: Harmonisation of standards and trade in electronics. *The World Economy*, 33(12):1870–1897, 2010.

[5] Ross Anderson och Tyler Moore. Information security economics – and beyond. I: *Advances in Cryptology-CRYPTO 2007*, ss 68–91. Springer, 2007.

[6] Beñat Bilbao-Osorio, Soumitra Dutta och Bruno Lanvin (red.). Global information technology report 2014, 2014. World Economic Forum.

[7] Steffen Bartsch. Practitioners' perspectives on security in agile development. I: *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, ss 479–484. IEEE, 2011.

[8] Konstantin Beznosov och Philippe Kruchten. Towards agile security assurance. I: *Proceedings of the 2004 workshop on New security paradigms*, ss 47–54. ACM, 2004.

[9] Mikko Siponen, Richard Baskerville och Tapio Kuivalainen. Integrating security into agile development methods. I: *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, ss 185a–185a. IEEE, 2005.

[10] Dejan Baca och Bengt Carlsson. Agile development with security engineering activities. I: *Proceedings of the 2011 International Conference on Software and Systems Process*, ss 149–158. ACM, 2011.

[11] Riksrevisionen. IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet? RiR 2011:4, januari 2011.

[12] Henrik Karlzén. Molnet – möjligheter och begränsningar. FOI, Totalförsvarets forskningsinstitut, 2012. FOI-R--3381--SE.

[13] Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter. En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011. Myndigheten för samhällsskydd och beredskap, 2012. Publikationsnummer MSB 367-12.

[14] Stefan Thalmann, Daniel Bachlechner, Lukas Demetz och Ronald Maier. Challenges in cross-organizational security management. I: *System Science (HICSS), 2012 45th Hawaii International Conference on*, ss 5480–5489. IEEE, 2012.

[15] Ulrik Franke, Markus Buschle och Magnus Österlind. An Experiment in SLA Decision-Making. I: *Economics of Grids, Clouds, Systems, and Services*, ss 256–267. Springer International Publishing, 2013.

[16] Nir Kshetri. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4):372–386, 2013.

[17] Kommun måste omförhandla avtal med Google – innebär olaglig behandling av personuppgifter. Dagens Juridik, http://www.dagensjuridik.se/2014/07/kommun-maste-omforhandla-avtal-med-google-innebar-olaglig-behandling-av-personuppgifter, 22 juli 2014. Läst 2014-08-01.

[18] Outsourcing av it-tjänster i kommuner. Myndigheten för samhällsskydd och beredskap, 2014. Publikationsnummer MSB728.

[19] Riksrevisionen. IT-investeringar över gränserna. RiR 2009:18, november 2009.

[20] Cisco. The Internet of Things. http://share.cisco.com/internet-of-things.html, 2011. Läst 2014-08-01.

[21] Rodrigo Roman, Jianying Zhou och Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, 2013.

[22] Vägledning till ökad säkerhet i industriella informations- och styrsystem. Myndigheten för samhällsskydd och beredskap, 2014. Publikationsnummer MSB718.

[23] Cisco 2014 Annual Security Report. Teknisk rapport, Cisco Systems, 2014.

[24] Ulrik Franke och Joel Brynielsson. Cyber situational awareness – a systematic review of the literature. *Computers & Security*, 46:18–31, 2014.

[25] Åse Dragland, SINTEF. Big Data – for better or worse. http://www.sintef.no/home/Press-Room/Research-News/Big-Data–for-better-or-worse/. Läst 2014-10-16.

[26] Näringsdepartementet Regeringen. Uppdrag att utveckla och vidareutveckla den tekniska plattformen öppnadata.se – en portal för innovation. N2012/3599/ITP, juli 2012.

[27] Ett steg vidare – nya regler och åtgärder för att främja vidareutnyttjande av handlingar. SOU 2014:10, februari 2014.

[28] Winston Ross. How Much Is Your Privacy Worth? MIT Technology Review, 2014. Läst 2014-09-17.

[29] Riksrevisionen. Rätt information vid rätt tillfälle inom vård och omsorg – samverkan utan verkan? RiR 2011:19, maj 2011.

[30] Riksrevisionen. Informationsutbyte mellan myndigheter med ansvar för trygghetssystem – Har möjligheter till effektivisering utnyttjats? RiR 2010:18, oktober 2010.

[31] Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service. SOU 2014:39, juni 2014.

[32] Alessandro Acquisti och Ralph Gross. Predicting social security numbers from public data. *Proceedings of the National academy of sciences*, 106(27):10975–10980, 2009.

[33] Magnus Jändel. Decision support for releasing anonymised data. *Computers & Security*, 46:48–61, 2014.

[34] Sanja Kelly, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz och Ashley Greco-Stoner (red.). *Freedom on the net 2013: a global assessment of internet and digital media*. Freedom House, 2013.

[35] Mikael Eriksson, Ulrik Franke, Magdalena Granåsen och David Lindahl. Social media and ICT during the Arab Spring. FOI, Totalförsvarets forskningsinstitut, 2013. FOI-R--3702--SE.

[36] Johan Norberg, Ulrik Franke och Fredrik Westerlund. The Crimea Operation: Implications for Future Russian Military Interventions. I: Niklas Granholm, Johannes Malminen och Gudrun Persson, redaktörer, *A Rude Awakening. Ramifications of Russian Aggression Towards Ukraine.* FOI, Totalförsvarets forskningsinstitut, Stockholm, 2014. FOI-R--3892--SE.

[37] The Voice of Russia. Anonymous Ukraine releases Klitschko e-mails showing treason. http://voiceofrussia.com/news/2014_02_23/Anonymous-Ukraine-releases-Klitschko-e-mails-showing-treason-3581/. Läst 2014-10-14.

[38] The Moscow Times. Russia Blocks Web Pages Linked to Ukraine Protests. http://www.themoscowtimes.com/article/495488.html. Läst 2014-10-14.

[39] Roskomnadzor. Ogranitjen dostup k rjadu internet-resursov, rassprostranjavsjich prizyvy k nesanktsionirovannym massovym meroprijatijam [Begränsad tillgång till en rad internet-resurser som har uppmanat till olagliga massaktioner]. http://rkn.gov.ru/news/rsoc/news24447.htm. Läst 2014-10-14.

[40] Nicole Perlroth. Cyberattacks Rise as Ukraine Crisis Spills to Internet. New York Times, Bits Blog, http://bits.blogs.nytimes.com/2014/03/04/cyberattacks-rise-as-ukraine-crisis-spills-on-the-internet/?_php=true&_type=blogs&_php=true&_type=blogs&hpw&rref=technology&_r=1. Läst 2014-10-14.

[41] RBK Ukraina. SBU podtverdila fakty telefonnych atak na mobilnye nardepov [SBU bekräftar fakta om telefonattacker mot parlamentsledamöter]. http://www.rbc.ua/rus/news/accidents/sbu-podtverdilo-fakty-telefonnyh-atak-na-mobilnye-nardepov-04032014120700. Läst 2014-10-14.

[42] Ukrtelekom. V AR Krim nevidomimi u vijs'kovij formi povtorno zablokovano dekil'ka vuzliv zv'jazku [I den autonoma republiken Krim har okända uniformerade män upprepade gånger blockerat flera kommunikationsknutpunkter]. http://www.ukrtelecom.ua/presscenter/news/official?id=120389. Läst 2014-10-14.

[43] BBC. Ukraine crisis: Transcript of leaked Nuland-Pyatt call. http://www.bbc.com/news/world-europe-26079957. Läst 2014-10-14.

[44] Reuters. Estonia denies leaked call implicates Ukraine protesters in killings. http://www.reuters.com/article/2014/03/05/us-estonia-eu-ukraine-idUSBREA2423O20140305. Läst 2014-10-14.

[45] Henning André Søgard och Janne Merete Hagen. *FFI-fokus: Kampen om sannheten*. Forsvarets forskningsinstitutt, 2014.

[46] Emilio Iasiello. Cyber attack: A dull tool to shape foreign policy. I: *Cyber Conflict (CyCon), 2013 5th International Conference on*, ss 451–468. IEEE, 2013.

[47] Roberto Alvarez och Raymond Robertson. Exposure to foreign markets and plant-level innovation: evidence from Chile and Mexico. *The Journal of International Trade & Economic Development*, 13(1):57–87, 2004.

[48] Aaditya Mattoo, Randeep Rathindran och Arvind Subramanian. Measuring services trade liberalization and its impact on economic growth: An illustration. *Journal of Economic Integration*, 21(1):64–98, 2006.

[49] Gary King, Jennifer Pan och Molly Roberts. How censorship in China allows government criticism but silences collective expression. I: *APSA 2012 Annual Meeting Paper*, 2012. Tillgängligt på SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2104894.

[50] Ryska utrikesministeriet. Convention on International Information Security (Concept). http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument. Läst 2014-09-25.

[51] Li Baodong, Vitaly Churkin, Sirodjidin Aslov och Murad Askarov. Brev daterat den 12 september 2011 från de permanenta representanterna för Kina, Ryska federationen, Tadzjikistan och Uzbekistan till Förenta nationerna, ställt till generalsekreteraren. Generalförsamlingens diarienummer A/66/359.

[52] Anil Ananthaswamy. Age of the splinternet. *New Scientist*, 211(2821):42–45, 2011.

[53] Brottsförebyggande rådet. Anmälda brott. Slutlig statistik för 2013. www.bra.se/statistik, mars 2014.

[54] European Cybercrime Centre (EC3) vid Europol. Internet Organised Crime Threat Assessment (IOCTA), september 2014.

[55] Aditya K Sood och Richard J Enbody. Crimeware-as-a-service – a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 6(1):28–38, 2013.

[56] European Cybercrime Centre (EC3) vid Europol. Police Ransomware Threat Assessment, februari 2014.

[57] Net Losses: Estimating the Global Cost of Cybercrime. Teknisk rapport, McAfee & Center for Strategic and International Studies, juni 2014.

[58] 2013 Norton Report. Teknisk rapport, Symantec Corporation, oktober 2013.

[59] Anandhi Bharadwaj, Mark Keil och Magnus Mähring. Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, 18(2):66–79, 2009.

[60] Paul Hyman. Cybercrime: it's serious, but exactly how serious? *Communications of the ACM*, 56(3):18–20, 2013.

[61] Muhammad Shahzad, Muhammad Zubair Shafiq och Alex X Liu. A large scale exploratory analysis of software vulnerability life cycles. I: *Proceedings of the 2012 International Conference on Software Engineering*, ss 771–781. IEEE Press, 2012.

[62] Hackers deployed to facilitate drugs smuggling, 2013. Intelligence Notification 004-2013, European Cybercrime Centre (EC3) vid Europol.

[63] The Crypto Crimson. UNODC: Online Drug Trade On The Rise Since Silk Road Demise. http://cryptocrimson.com/2014/07/unodc-online-drug-trade-thriving-since-silk-road-demise/.

[64] Wired World in 2014, 2013. Wired Magazine.

[65] Stärkt straffrättsligt skydd för egendom. SOU 2013:85, december 2013.

[66] Europarådets konvention om it-relaterad brottslighet. SOU 2013:39, juni 2013.

[67] William Enck, Damien Octeau, Patrick McDaniel och Swarat Chaudhuri. A study of Android application security. I: *Proceedings of the 20th USENIX Security Symposium*, 2011.

[68] Longfei Wu, Xiaojiang Du och Xinwen Fu. Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *Communications Magazine, IEEE*, 52(3):80–87, 2014.

[69] Tielei Wang, Kangjie Lu, Long Lu, Simon Chung och Wenke Lee. Jekyll on iOS: When Benign Apps Become Evil. I: *Proceedings of the 22nd USENIX Security Symposium*, ss 559–572, 2013.

[70] TT. 18-åring åtalas för dataintrång. VLT, 23 augusti 2014. s. 25.

[71] Annsofie Wieland. Hackers stör Bjuvs datatrafik. Landskronaposten, 16 januari 2014. s. A27.

[72] Ola Thelberg. Nätattack mot Härnösand. Tidningen Ångermanland, 26 februari 2013. s. 4.

[73] FuiFui Wong och Cheng Xiang Tan. A Survey of Trends in Massive DDOS Attacks and Cloud-Based Mitigations. *International Journal of Network Security & Its Applications (IJNSA)*, 6(3):57–71, 2014.

[74] Zakir Durumeric, Eric Wustrow och J Alex Halderman. Zmap: Fast internet-wide scanning and its security applications. I: *Proceedings of the 22nd USENIX Security Symposium*, ss 605–620, 2013.

[75] Éireann P Leverett. Quantitatively assessing and visualising industrial system attack surfaces, 2011. M.Phil.-avhandling, University of Cambridge, Darwin College.

[76] Jayant Venkatanathan, Vassilis Kostakos, Evangelos Karapanos och Jorge Gonçalves. Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing. *Interacting with Computers*, 2013. 10.1093/iwc/iwt058. I kommande nummer.

[77] 2014 Internet Security Threat Report, Volume 19. Teknisk rapport, Symantec Corporation, april 2014.

[78] Hannes Holm, Waldo Rocha Flores och Göran Ericsson. Cyber security for a Smart Grid – What about phishing? I: *Innovative Smart Grid Technologies Europe (ISGT Europe), 2013 4th IEEE/PES*, ss 1–5. IEEE, 2013.

[79] Wouter Martinus Petrus Steijn. A developmental perspective regarding the behaviour of adolescents, young adults, and adults on social network sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8(2), 2014.

[80] Greg Young, Adam Hils och Jeremy D'Hoinne. Magic Quadrant for Enterprise Network Firewalls. Teknisk rapport, Gartner, Inc., april 2014.

[81] Peter Firstbrook, John Girard och Neil MacDonald. Magic Quadrant for Endpoint Protection Platforms. Teknisk rapport, Gartner, Inc., januari 2014.

[82] Security Intelligence Report volume 16. Teknisk rapport, Microsoft Corporation, 2014.

[83] Hannes Holm, Teodor Sommestad, Jonas Almroth och Mats Persson. A quantitative evaluation of vulnerability scanning. *Information Management & Computer Security*, 19(4):231–247, 2011.

[84] John R Goodall, Wayne G Lutters och Anita Komlodi. Developing expertise for network intrusion detection. *Information Technology & People*, 22(2):92–108, 2009.

[85] Hannes Holm. Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter? I: *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, ss 4895–4904. IEEE, 2014.

[86] Teodor Sommestad, Johan Bengtsson och Jonas Hallberg. Varför följer inte användarna bestämmelser? – En meta-analys avseende informationssäkerhetsbestämmelser. FOI, Totalförsvarets forskningsinstitut, 2012. FOI-R--3524--SE.

[87] Säkerheten i första hand. *Försvarets Forum*, (4):21–22, 2014.

[88] Kevin Henry. Business continuity planning: Case study. I: *Encyclopedia of Information Assurance*, kapitel 42, ss 344–350. Taylor & Francis.

[89] Computer Sweden. Försäkringskassans cio om buggen bakom it-kraschen. http://computersweden.idg.se/2.2683/1.588563/forsakringskassans-cio-om-buggen-bakom-it-kraschen. Läst 2014-10-14.

[90] Leyla Bilge och Tudor Dumitras. Before we knew it: an empirical study of zero-day attacks in the real world. I: *Proceedings of the 2012 ACM conference on Computer and communications security*, ss 833–844. ACM, 2012.

[91] Unknown threats in Sweden. KPMG, 2014. Läst 2014-09-17.

[92] Ulrik Franke. Optimal IT Service Availability: Shorter Outages, or Fewer? *IEEE Transactions on Network and Service Management*, 9(1):22–33, mars 2012.

[93] En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter. Myndigheten för samhällsskydd och beredskap, 2014. Publikationsnummer MSB740.

[94] Taco van der Vaart och Dirk Pieter van Donk. A critical review of survey-based research in supply chain integration. *International Journal of Production Economics*, 111(1):42–55, 2008.

[95] Tommy Svensson. Säkerhet vid anskaffning och utveckling av system. vägledning för informationssäkerhetsdeklarationen. Svenskt Näringsliv/Näringslivets Säkerhetsdelegation, oktober 2011.

[96] Vägledning – informationssäkerhet i upphandling. Myndigheten för samhällsskydd och beredskap, 2013. Publikationsnummer MSB555.

[97] Inger Sohlberg och Susanne Jansson. Dolda it-kostnader i verksamheten. Försäkringskassan och Pensionsmyndigheten. Inspektionen för socialförsäkringen, mars 2012. Rapport 2012:5.

[98] Jenny Askåker och Mikael Kulle. Miljardaffärer gick förlorade. Dagens Industri, ss 6–7, 4 juni 2008.

[99] Jörgen Lindqvist. It-säkerhet är alltid för dyrt – tills något händer. Computer Sweden, 4 maj 2012.

[100] John A. Wheeler och Paul E. Proctor. Understanding When and How to Use Cyberinsurance Effectively. Teknisk rapport, Gartner, Inc., april 2012.

[101] Defending the digital frontier. Special report: Cyber security. The Economist, 12 juli 2014. s. 9.

[102] Eli Dourado och Andrea Castillo. Why the Cybersecurity Framework Will Make Us Less Secure. Teknisk rapport, Mercatus Center at George Mason University, april 2014.

[103] Marc Lelarge och Jean Bolot. Economic incentives to increase security in the internet: The case for insurance. I: *INFOCOM 2009, IEEE*, ss 1494–1502. IEEE, 2009.

Om myndigheterna

Om myndigheterna

Försvarsmaktens uppdrag är att ansvara för Sveriges militära försvar. **Försvarsmakten** har lång erfarenhet av att utveckla och driftövervaka landsomfattande säkra och robusta lednings- och informationssystem. Verksamheten kräver att Militära underrättelse- och säkerhetstjänsten (MUST), drifts- och säkerhetsorganisationen upprätthåller hög och aktuell kompetens inom både teknik och säkerhetskultur. **Försvarsmakten** ger även stöd till andra myndigheter och totalförsvaret.

Försvarets radioanstalt, **FRA**, är en civil underrättelsemyndighet vars verksamhet bidrar till att skydda Sverige och svenska intressen. Ett av myndighetens uppdrag är att bidra till att stärka informationssäkerheten inom samhällsviktig verksamhet i Sverige. **FRA** bidrar till att stärka skyddet genom att bland annat testa sårbarheten i it-system eller genom att ge konkreta råd om hur informationssäkerheten kan förbättras i de berörda verksamheterna.

Myndigheten för samhällsskydd och beredskap, **MSB**, är en statlig myndighet med uppgift att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser. Verksamheten för samhällets informations- och cybersäkerhet ansvarar för att stödja och samordna arbetet med samhällets informationssäkerhet samt att analysera och bedöma omvärldsutvecklingen på området. Verksamheten ska även lämna råd och stöd i det förebyggande arbetet samt svara för föreskrifter på informationssäkerhetsområdet. Vidare ansvarar verksamheten för arbetet med Sveriges nationella funktion för stöd till samhället i arbetet med att hantera och förebygga it-incidenter.

Polisens uppdrag är att minska brottsligheten och öka tryggheten i samhället. Nationella operativa avdelningen (NOA) har ett nationellt ansvar för **Polisens** kärnverksamhet, inklusive att bekämpa den komplexa it-brottsligheten.

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB779 - januari 2015 ISBN 978-91-7383-509-1