Myndigheten för samhällsskydd och beredskap

Samhällets informationssäkerhet

Lägesbedömning 2009

MSB:s kontaktperson:
Helena Andersson, 010-240 41 33

Publikationsnummer MSB 0023-09
ISBN 978-91-7383-009-6

Förord

Myndigheten för samhällsskydd och beredskap (MSB) har i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet, samt analysera och bedöma omvärldsutvecklingen inom området. I samhället sker ett målinriktat arbete med att öka användning av och tillgång till elektroniska tjänster. Förtroende och användarvänlighet är avgörande framgångsfaktorer, men brister i tekniska lösningar, ofullständigt integritetsskydd och otillräckligt säkerhetsmedvetande skapar hinder för ett effektivt utnyttjande av IT.

Denna lägesbedömning är en del av den omvärldsbevakning och analysarbete som MSB bedriver på informationssäkerhetsområdet.

Lägesbedömningen grundar sig primärt på utvecklingen under 2008 och inledningen av 2009 och riktar sig till aktörer i samhället som har att hantera informationssäkerhetsfrågor.

Stockholm i mars 2009

Helena Lindberg

Generaldirektör

Innehållsförteckning

Sammanfattning 7

Del A Lägesbedömning

1 Inledning 13
1.1 Lägesbedömning 13
1.2 Vad är informationssäkerhet och samhällsviktig verksamhet? ... 13
1.3 Utgångspunkter 15
1.3.1 Inledning 15
1.3.2 Helhetssyn 15
1.3.3 Informationssäkerhet och personlig integritet 16
1.3.4 Urvalsmetod 16
1.3.5 Upplägg och källor 17

2 Mål för informations-säkerhetsarbetet 18
2.1 Generella mål 18
2.2 Sektorsspecifika mål 19
2.2.1 Strategi för ökad säkerhet i Internets infrastruktur 19
2.2.2 Nationell IT-strategi för vård och omsorg 20
2.2.3 Handlingsplan för e-förvaltning 20

3 Slutsatser 22
3.1 Inledning 22
3.2 Samhällsviktig verksamhet 22
3.3 Förtroende och integritetsskydd 24
3.4 Effektivt utnyttjande av IT 25
3.5 Nationell säkerhet 26
3.6 Jämförelse med 2008 års lägesbedömning 26

Del B Bakgrund

4 Informationshantering, utveckling och trender under 2008 . 29
4.1 Inledning 29
4.2 Ökad mobilitet 29
4.3 Webb 2.0 29
4.4 Extern tjänstehantering (Outsourcing) 30
4.5 Virtualisering och Service Oriented Architecture 31
4.6 Data Loss Prevention 32
4.7 Radio Frequency Identification 32
4.8 Förändrade beteendemönster på grund av ny lagstiftning 33

5 Antagonistiska hot 34
5.1 Inledning 34
5.2 Samhällsnivå 34
5.2.1 Hot mot samhällsviktiga verksamheter 34

5.2.2 Informationsoperationer 37
5.2.3 Internets militarisering 38
5.3 Organisation och individnivå 41
5.3.1 IT-relaterad brottslighet 41
5.3.2 Nätfiske 42
5.3.3 IT-relaterad utpressning 43
5.3.4 Virus och skadlig kod 43
5.3.5 Spam 44
5.3.6 Social Engineering 44
5.3.7 Botnät 45
6 Sårbarhet och risker 47
6.1 Inledning 47
6.2 Samhällsnivå 47
6.2.1 Elektroniska kommunikationer 47
6.2.2 Digitala kontrollsystem 48
6.2.3 Kryptografiska funktioner 51
6.2.4 Mediesektorn 52
6.2.5 Offentlig verksamhet 53
6.2.6 Finansiella tjänster 54
6.2.7 Hälso- och sjukvård 56
6.2.8 Brottsbekämpning 57
6.3 Organisation och individnivå 62
6.3.1 Mobila enheter 62
6.3.2 Trådlösa nätverk (WLAN) 63
6.3.3 Radio Frequency Identification (RFID) 65
6.3.4 Webbplatser 65
6.3.5 Tid 66
6.3.6 Domain Name System (DNS) och Border Gateway Protocol (BGP) 67
6.3.7 Arkivering 68
6.3.8 Extern tjänstehantering (Outsourcing) 69
7 Insatser för ökad säkerhet 71
7.1 Inledning 71
7.2 Myndighetsinitiativ 71
7.2.1 Handlingsplan för samhällets informationssäkerhet 71
7.2.2 Handlingsplan för E-förvaltning 73
7.2.3 Handlingsplan för internetsäkerhet 74
7.2.4 Grundläggande informationssäkerhet 75
7.2.5 Nationell samverkansfunktion 76
7.2.6 Swedish Government Secure Intranet (SGSI) 76
7.2.7 Kryptografiska funktioner 77
7.2.8 DNSSEC 78
7.3 Reglering 78
7.3.1 Säkrare informationshantering 78
7.3.2 Förebygga och bekämpa brott 80

7.3.3 Skydd av personlig integritet 81
7.4 Standardisering 82
7.4.1 ISO/IEC 27000 Ledningssystem för informationssäkerhet (LIS) 82
7.4.2 Common Criteria 83
7.4.3 Payment Card Industry Standard Data Security Standard (PCI DSS) 84
7.5 Internationella initiativ 84
7.5.1 ENISA 85
7.5.2 Organisation for economic co-operation and development, OECD 85
7.5.3 Internet Governance Forum, IGF 85
7.5.4 European Program for Critical Infrastructure Protection, EPCIP 86
7.5.5 Internationell samverkan 86
7.6 Övning och utbildning 87
7.6.1 Chief Information Assurance Officer (CIAO) 87
7.6.2 SIS Informationssäkerhetsakademi 88
7.6.3 Samverkansövning 2008 (SAMÖ 08) 88
7.6.4 FHS Övning 89

Källor och vidare läsning 90

Sammanfattning

Samhällets funktioner är beroende av fungerande IT och informationshantering varför en tillräcklig nivå av informationssäkerhet är en nödvändighet. Den svaga länken i säkerhetsarbetet är mänskliga beteenden som både kan försvåra skydd av och utgöra direkta hot mot informationshanteringen. Hoten blir alltmer sofistikerade och den IT-relaterade brottsligheten bedrivs affärsmässigt. Brottsbekämpningen begränsas av resursbrist och rättsväsendet lider av kompetensbrist vad gäller IT-relaterad bevisning.

Allt komplexare IT-miljö och alltfler integrerade nätverk gör att fokus ofta riktas mot mer begränsade och hanterbara IT-relaterade problem i den egna organisationen. Det är viktigt att även uppmärksamma och analysera konsekvenser och kopplingar ur ett samhällsperspektiv. Vad händer om det stora flertalet organisationer med samhällsviktig verksamhet outsourcar sin informationshantering till utländska bolag?

Informationssäkerhetsområdet har länge karaktäriserats av brist på helhetssyn och styrning. Idag finns flera handlingsplaner av central betydelse för säkerhetsarbetet och MSB har föreskriftsrätt när det gäller myndigheters informationssäkerhet. Ett ändamålsenligt arbete med informationssäkerhet på nationell och internationell nivå är av central betydelse för samhällsutvecklingen.

Det sker ett målinriktat arbete med att öka användning av och tillgång till elektroniska tjänster i samhället. Förtroende och användarvänlighet är avgörande framgångsfaktorer men brister i tekniska lösningar, ofullständigt integritetsskydd och otillräckligt säkerhetsmedvetande skapar hinder för ett effektivt utnyttjande av IT. Det är därför viktigt att betona betydelsen av ändamålsenligt informationssäkerhetsarbete som hanterar dessa brister.

Spelreglerna för informationssäkerhetsarbetet har ändrats under 2008 i och med ny teknik, ny reglering och nya användarbeteenden. Outsourcing i form av Cloud Computing kommer att ge organisationer möjlighet att koncentrera sig på sin kärnverksamhet men innebär samtidigt att kontrollen över informationshanteringen minskar. Ökad mobilitet och ökat utnyttjande av interaktiva sociala nätverk medför ökade risker för både organisationer och enskilda eftersom säkerhetsfrågan ännu inte är ett starkt användarkrav. När det gäller utveckling och drift av webbplatser är säkerhetsarbetet eftersatt. I takt med ökat antal besökare och allvarligare hotbild kan detta i förlängningen skada förtroendet för både innehåll och hantering av personuppgifter.

Hotbilden blir allvarligare och IT-relaterad brottslighet är redan nu ett betydande problem. Här ser vi att bedrägerierna blir alltmer sofistikerade och utnyttjar i allt högre grad mänskliga svagheter. Olika former av utpressning är ett område som visat sig svårt att bekämpa och där man befarar ett stort mörkertal. Det finns en hög affärsmässighet i brottsliga kretsar som visas

genom etablerad handel med både attackverktyg, kompetens och uthyrning av kapade datorer. Krisberedskapsmyndigheten visade på denna utveckling redan under 2007 och den har förstärkts ytterligare under 2008.

Brottsbekämpningen möter utmaningar i form av resursbrist och mörkertal rörande IT-relaterad brottslighet. Kompetensbristen inom rättsväsendet när det gäller bland annat IT-relaterad bevisning måste också hanteras. Internationell och nationell samverkan är en förutsättning för att inte bara kunna bedriva ett effektivt arbete mot IT-relaterad brottslighet utan även för att garantera nationell säkerhet.

Det finns idag handlingsplaner för samhällets informationssäkerhet, för säkerhet i Internets infrastruktur och för e-fövaltning samt flera fristående initiativ för att skapa informationssäkerhet. Med hänsyn till det stadigt ökande beroendet av IT samt utvecklingen av hot och sårbarheter ser vi det som avgörande att föreslagna åtgärder, som exempelvis kompetenshöjning och upprättande av grundläggande informationssäkerhet, genomförs. Ytterligare insatser bör ske för att motverka IT-relaterad brottslighet och för att främja internationellt samarbete.

Ord- och förkortningslista

Botnät – Nätverk av datorer som infekterats med skadlig kod som gör det möjligt för en tredje part att kontrollera och fjärrstyra datorer.

Buffer overflow – Överskridande av maximalt tillåten datamängd i minnesbuffert vilket kan resultera i störning eller skada i systemet.

CERT (Computer Emergency Response Team) – Funktion för incidenthantering

CCRA (Common Criteria Recognition Arrangement) – En internationell samarbetsorganisation som erkänner ömsesidigt utfärdade certifikat. Inom CCRA utvecklas såväl standarden Common Criteria som metoder och regelverk för att stödja CCRA avtalet.

Common Criteria – En internationell standard för hur man ställer krav, deklarerar och evaluerar säkerhet i IT-produkter och system.

Communities (nätmötesplatser) – Webbplatser där det ofta krävs ett medlemskap för att ta del av innehållet. Huvudsyftet är oftast att komma i kontakt med likasinnade.

COTS (Commercial off-the-shelf) – Kommersiellt tillgängliga standardprodukter.

Cross-site-scripting – Metod som utnyttjar användarens förtroende för en webbapplikation. Syftet för en angripare är oftast att stjäla känslig information som exempelvis lösenord eller att förstöra utseendet på en webbsida. Även länkar till andra webbsidor kan placeras på sidan.

DDoS-attacker (tillgänglighetsattacker) – Aktiviteter som kan överbelasta eller blockera vissa IT-resurser och på det sättet förhindra behörig åtkomst till resurser i ett IT-system eller fördröja tidskritiska operationer.

Digitala kontrollsystem (SCADA- Supervisory Control And Data Aquisition) – Datorbaserade system för styrning, reglering och övervakning av fysiska processer som exempelvis elektricitet, gas, spårbunden trafik och dricksvattenförsörjning.

DNS (Domain Name System) – Den funktion på Internet som översätter domännamn till IP-adresser. Då det finns ett stort antal domännamn och ingen enskild server kan ha en komplett lista över dessa, finns det i stället ett nät av sammankopplade DNS-servrar som ber varandra om hjälp vid behov.

Drive by downloads – Program som laddas ner till datorn utan användarens vetskap eller vilja vilket kan ske genom att enbart besöka en webbsida. Orsaken till att en dator blir infekterad är ofta dåligt uppdaterade webbläsare.

Exploit – Metod som används för att utnyttja en sårbarhet i ett datorsystem för att komma åt skyddad information eller för sabotage

Hosting – Istället för att köpa, installera och drifta servrar och mjukvara lokalt till varje PC, kan ett företag få tillgång till IT tjänster och applikationer över Internet och då betala för en viss period. En extern hostingleverantör levererar då olika lösningar.

Man-in-the-middle-attack – Utomstående som genom att koppla in sig på en förbindelse mellan två parter simulerar respektive parts identitet mot den andre och på det sättet kan avlyssna eller förändra den överförda informationen.

Metasploit – Hackerverktyg som gör det möjligt för systemadministratörer, men också hackare, som vill utföra ett penetrationstest att kombinera attackkod för en mängd olika säkerhetsluckor med annan skadlig kod

Nätfiske – Metod som går ut på att få en person att lämna ifrån sig konfidentiell information genom att lura personen att antingen svara på ett falskt e-postmeddelande eller besöka en falsk webbsida.

OpenID – Lösning som gör det möjligt att bara behöva logga in en gång med användarnamn och lösenord hos en betrodd OpenID-leverantör. Denne försäkrar sedan användarens identitet till andra webbappliktioner som kräver inloggning.

PGP (Pretty Good Privacy) – PGP bygger på ett system med privata och offentliga nycklar. Alla som vill skicka ett krypterat meddelande till en person använder dennes offentliga nyckel. Mottagaren använder sedan sin privata nyckel för att dekryptera meddelandet.

Rakel – Gemensamt radiokommunikationssystem för organisationer i samhället som arbetar med allmän ordning, säkerhet eller hälsa.

Remote file inclusion – Typ av attack i webbaserade skriftspråk. Attacken innebär att en person kan exekvera sin egna skriptkod på någon annans server. Möjligheten finns sedan för en angripare att få åtkomst till alla filer på webbplatsen och kunna ändra dem om inte rättigheterna är korrekt inställda på webbservern.

SAMFI (Samverkansgruppen för Informationssäkerhet) – I denna grupp som leds av MSB ingår även Försvarets radioanstalt (FRA), Post & Telestyrelsen (PTS), Försvarsmakten (FM), Rikspolisstyrelsen (RPS), Försvarets materielverk (FMV) och Säkerhetspolisen (Säpo).

SGSI (Swedish Government Secure Intranet) – Nättjänst som inte är beroende av Internet och till vilken svenska myndigheter kan ansluta sig och kommunicera med varandra.

Social Engineering (Social manipulering) – Då en person använder sig av olika sociala knep för att skapa förtroende i syfte att förmå någon att lämna ut känslig eller hemlig information. Nätfiske är en form av social manipulering.

SQL-injektioner – Metod som utnyttjar säkerhetshål i hanteringen av indata i vissa datorprogram som arbetar mot en databas. Problemet uppstår då indata till en sql-sats inte behandlas på rätt sätt av programmeraren, varpå en

attackerare kan använda speciella tecken och kommandon för att manipulera data eller skaffa sig information. Metoden har fått sitt namn av databasfrågespråket SQL.

Trojan – Program som ofta innehåller illasinnad kod och följer med en annan fil eller program. Den kan sedan skaffa sig kontroll och utföra det den är programmerad att göra.

Del A Lägesbedömning

1 Inledning

1.1 Lägesbedömning

MSB har i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området.[1] Arbetet med lägesbedömningen är en del av både omvärldsbevakningen och analysarbetet samt utgör ett stöd i arbetet med den nationella handlingsplanen för informationssäkerhet som MSB förvaltar.[2]

Lägesbedömningen utgör ett stöd till aktörer i samhället som har att hantera informationssäkerhetsfrågor. Bedömningen grundar sig primärt på utvecklingen under 2008 och inledningen av 2009.

1.2 Vad är informationssäkerhet och samhällsviktig verksamhet?

Med informationssäkerhet avses förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet vid hantering av information.[3] Begreppet är omfattande och rör information i alla dess former, både i pappersform och elektroniskt hanterad. *Konfidentialitet* är skyddsmålet att inte obehöriga kan ta del av informationen, *riktighet* att informationen inte förändras eller förstörs på ett obehörigt sätt och *tillgänglighet* att behöriga får tillgång till informationen på det sätt och vid den tidpunkt som önskas. Informationssäkerhet handlar om mer än att säkra informationssystem; även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

Brand, skadlig kod, dataintrång är bara några exempel på hot som kan orsaka förlust av konfidentialitet, riktighet eller tillgänglighet. Förekomsten av *sårbarheter* vid informationshanteringen som exempelvis frånvaro av brandskydd och antivirusprogram gör att *risken* för att hoten orsakar störningar och skada ökar. Avgörande för hur stor risken bedöms vara är inte bara konsekvenserna utan även sannolikheten för att hoten ska realiseras. Riskerna kan minskas genom olika typer av *säkerhetsåtgärder*, exempelvis tekniska, juridiska, ekonomiska eller organisatoriska lösningar.

[1] 6 § Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

[2] http://www.krisberedskapsmyndigheten.se/upload/17005/handlingsplan_samhallets_informationssakerhet_20080401.pdf

[3] SIS Handbok 550:Terminologi för informationssäkerhet

Ytterst handlar arbetet med informationssäkerhet om att slå vakt om en mängd olika värden och målsättningar i samhället, såsom demokrati, personlig integritet, tillväxt samt ekonomisk och politisk stabilitet.

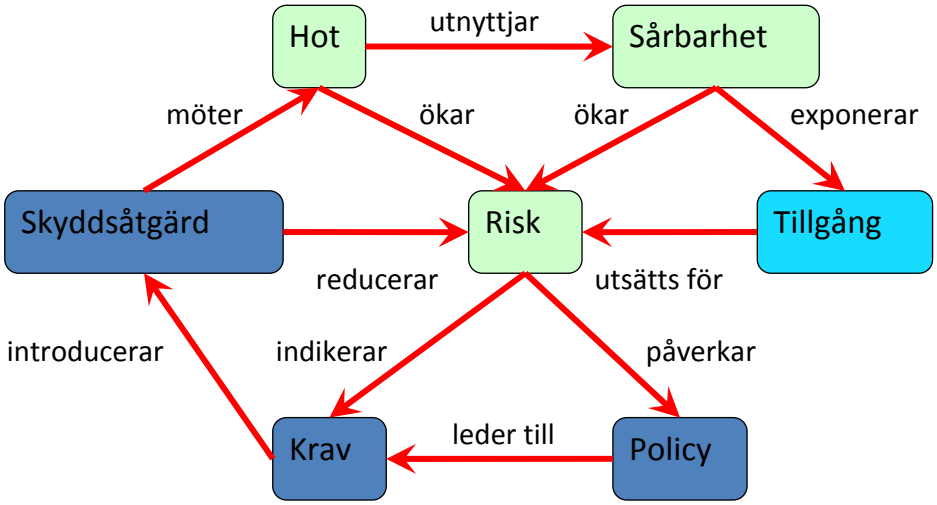


Bild 1 Samband mellan parametrar inom området informationssäkerhet.
SIS Handbok 550: Terminologi för informationssäkerhet

Effektivt informationssäkerhetsarbete kan beskrivas på olika sätt. Den modell som förordas i Vervas föreskrifter[4] rekommenderar ett tydligt ansvar, ett genomtänkt ledningssystem och risk- och sårbarhetsanalys med återkoppling.

De hot och sårbarheter som tas upp i lägesbedömningen rör informationshantering som är av särskild vikt ur ett samhällsperspektiv. Detta inbegriper särskilt informationshanteringen i *samhällsviktig verksamhet* men även annan typ av informationshantering där säkerhetsbrister får konsekvenser för samhällets sätt att fungera.

För att identifiera samhällsviktig verksamhet ur ett krishanteringsperspektiv används här följande kriterier:[5]

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

[4] Verva FS 2007:2 Verket för förvaltningsutveckling (Verva) upphörde vid årsskiftet 2008/2009 men föreskrifterna är fortfarande gällande.

[5] Krisberedskapsmyndigheten, *Samhällsviktigt! Förslag till definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv,* 0253/2005

Effektiv krishantering bygger i hög grad på ett grundligt förebyggande arbete. Hur god informationssäkerheten är i normaltillstånd avgör också till stor del hur väl samhället klarar av att hantera allvarliga störningar och kriser när de inträffar.

1.3 Utgångspunkter

1.3.1 Inledning

För att göra en strukturerad lägesbedömning av *samhällets informationssäkerhet* krävs både en helhetssyn och en urvalsmetod. Den förra för att säkerställa att underlaget för bedömningen är heltäckande och den senare för att säkerställa att de områden som behandlas i rapporten är de mest relevanta med hänsyn till lägesbedömningens syfte.

1.3.2 Helhetssyn

Helhetssyn när det gäller *informationssäkerhet* syftar här på att bedömningen omfattar all information och informationshantering och dess behov av konfidentialitet, riktighet och tillgänglighet. Detta innebär att det inte räcker att studera tekniska lösningar. Användarmönster, ekonomiska förhållanden och rättslig reglering är också av betydelse. En rad aktörer spelar en stor roll för informationssäkerhetens utformning och nivå. Det handlar om allt från myndigheter, teleoperatörer, lagstiftare, antagonister, standardiserings-organisationer, teknikutvecklare och organisationsledning men också den enskilda individen. Utöver detta innefattar en nödvändig helhetssyn även skalan från vardagssäkerhet till säkerhet vid krishantering.

Nästa steg är att klargöra vad vi avser med *samhällets* informationssäkerhet. Begreppet är omfattande och kan ges olika innebörd. I lägesbedömningen har vi utgått från regeringens beskrivning av samhällets säkerhet i propositionen Samverkan vid kris – för ett säkrare samhälle.

”Med samhällets säkerhet avses händelser och förhållanden som enskilda individer saknar förutsättningar att själva hantera fullt ut och som hotar samhällets funktionalitet och överlevnad. På ett grundläggande plan innebär säkerhet att människor kan känna sig trygga i sin vardag och på ett mer övergripande plan att det finns förmåga att skydda de värden som vi förknippar med att leva i ett modernt demokratiskt samhälle. Samtidigt är mycket av det som är typiskt för det moderna samhället, bland annat i form av vår avancerade teknikanvändning, också det som skapar sårbarheter.”[6]

Vi har överfört detta synsätt på informationssäkerhetsområdet. I handlingsplanen för samhällets informationssäkerhet konstateras att informationssäkerhet är en stödjande verksamhet för att öka kvaliteten hos samhällets funktioner.[7]

[6] Prop 2005/06:133 s 39

[7] Samhällets informationssäkerhet handlingsplan 2008 s 15

Brister i hantering av information leder till ett försämrat förtroende för tjänster och aktörer. Allvarliga och upprepade störningar kan leda till förtroendekriser, som kan sprida sig till fler aktörer och tjänster och även till andra delar av samhället. Exempelvis kan ett försämrat förtroende för Internetbanker smitta av sig till andra som erbjuder Internetbaserade tjänster.

Även fysiska skador på den kritiska infrastrukturen kan få ödesdigra följder. Incidenter som leder till oförmåga eller förstörelse av sådan infrastruktur kan leda till allvarliga kriser som drabbar de finansiella systemen, allmänhetens hälsa, den nationella säkerheten, eller kombinationer av dessa.

Beroendet av fungerande IT ökar kontinuerligt i hela världen i takt med att informationshantering i allt högre utsträckning utförs elektroniskt. Samtidigt sker en entydig ökning av informationssäkerhetsrelaterade hot såsom dataintrång, bedrägerier och spridning av skadlig kod. Bakomliggande aktörer utgörs av såväl enskilda som organiserad brottslighet och terrorister. I vissa sammanhang har även misstankar mot stater framförts.[8]

1.3.3 Informationssäkerhet och personlig integritet

I diskussioner rörande informationssäkerhet aktualiseras inte sällan integritetsfrågan. På motsvarande sätt berörs informationssäkerhet ofta i integritetsdiskussioner. Vi ser informationssäkerhet som ett verktyg för att säkerställa att vald nivå av integritetsskydd kan upprätthållas. Särskilt när det gäller hanteringen av elektronisk information är säkerhet en nödvändighet för att kunna garantera ett skydd för den personliga integriteten såväl som för andra grundläggande fri- och rättigheter som ska fungera i elektronisk såväl som i fysisk miljö. Flertalet av de frågor och områden som behandlas i lägesbedömningen har i större eller mindre utsträckning bäring på integritetsfrågor. För att undvika överlappning har vi därför i del B valt att vid behov behandla integritet under respektive rubrik och lämna övergripande resonemang till slutsatserna i del A.

1.3.4 Urvalsmetod

Med denna helhetssyn på samhällets informationssäkerhet som utgångspunkt har vi valt att behandla sådana områden och frågor som är av särskilt intresse för *informationssäkerhetsarbetet*, särskild betydelse för samhället samt har förändrats, försämrats eller förbättrats *under 2008 och början av 2009*.

Det bör betonas att även om lägesbedömningen behandlar informationssäkerhet ur ett svenskt samhällsperspektiv är det nödvändigt med en internationell utblick. Informationstekniken skapar ett gränslöst samhälle där hot och sårbarheter inte längre är begränsade till vissa geografiska förutsättningar.

[8] Exempelvis hävdade Estland efter attacken 2007 detta, även USA och Georgien har framfört den typen av misstankar mot olika statsmakter.

1.3.5 Upplägg och källor

Även lägesbedömningens upplägg syftar till att spegla helhetssynen på informationssäkerhet och skapa förståelse för de villkor under vilka arbete med informationssäkerhetsarbete bedrivs. Mål, utveckling, hot och sårbarheter styr vilka insatser som görs och bör göras. I avsnittet med slutsatser visar vi på områden och frågor som vi anser är knutna till varandra och behöver ägnas uppmärksamhet.

För att skapa överblick inleds lägesbedömningen med en sammanfattning. Därefter följer två huvuddelar. I ”del A Lägesbedömning” behandlas syfte, utgångspunkter, mål och slutsatser. ”Del B Bakgrund” behandlar på ett mer ingående sätt utveckling och trender, hot, sårbarheter och insatser för att öka informationssäkerhetsnivån i samhället. Indelningen syftar till att öka tillgängligheten till materialet. En genomläsning av de 13 sidorna i del A ger en grundläggande förståelse för informationssäkerhet och vilka frågor som bör ägnas särskild uppmärksamhet. Om ett eller flera områden är av särskilt intresse för läsaren gör kapitelstrukturen det enkelt att finna ytterligare information i del B.

Lägesbedömningen bygger i huvudsak på information från öppna källor, ett flertal fördjupningsstudier, djupintervjuer med aktörer inom såväl offentlig som privat sektor samt en enkätundersökning riktad till statliga myndigheter. Vid arbetet har även funnits tillgång till hemligt material. Det är emellertid en öppen rapport då känslig information har kunnat verifieras med öppna källor eller har lyfts upp till en generell nivå. Huvudparten av källorna redovisas i källförteckningen.

Arbetet med att identifiera och prioritera viktiga frågor har skett i samverkan med bland andra samverkansgruppen för informationssäkerhet (SAMFI) samt KBM:s informationssäkerhetsråd och dess arbetsgrupp för näringslivsfrågor.[9] I dessa råd och grupper finns såväl näringsliv som samtliga myndigheter med central roll inom informationssäkerhetsområdet representerade.

[9] KBM upphörde den 31 december 2008 och verksamheten överfördes vid årsskiftet, tillsammans med verksamheterna i Räddningsverket och Styrelsen för psykologiskt försvar, till MSB.

2 Mål för informations-säkerhetsarbetet

2.1 Generella mål

Målen för informationssäkerhetsarbetet på samhällsnivå framgår av den nationella strategin. Strategin finns idag uttryckt i flera versioner med oklar status och inbördes ordning. För närvarande pågår därför ett arbete att uppdatera och tydliggöra strategin för samhällets informationssäkerhet.[10]

Den första versionen av strategin kom till uttryck i propositionen Samhällets säkerhet och beredskap och innehöll följande målformulering.[11]

”Målet bör vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man ska kunna förhindra eller hantera störningar i samhällsviktig verksamhet.”

Regeringen påpekade att strategin för att uppnå detta mål liksom övrig krishantering i samhället bör utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen. När det gällde ansvarsfördelningen mellan stat och enskild konstaterades principiellt att ”den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet ska fungera tillfredsställande.” Av propositionen framgår även att staten har ett övergripande ansvar för samhällets informationssäkerhet och ska vidta de åtgärder som rimligen inte kan åvila enskilda organisationer.[12]

Tre år senare kompletterade regeringen strategin i propositionen Samverkan vid kris – för ett säkrare samhälle med formuleringen: [13]

”Den av regeringen 2002 fastställda strategin för informationssäkerhet bör utvecklas till att även omfatta att kunna upptäcka, ingripa mot och agera i samband med störningar i samhällsviktiga IT-system. Förtroendet för och tryggheten att använda IT bör öka. En ökad säkerhet och ett förbättrat integritetsskydd bör eftersträvas.”

Infosäkutredningen sammanfattade sin syn på den nationella strategin i 10 punkter som delvis byggde på texten i propositionerna.[14]

[10] MSB har fått i uppdrag att lämna förlag på uppdatering av den nationella strategin utifrån den rådande samhällsutvecklingen. Detta arbete kommer även att inkludera formulering av mål. Uppdraget ska redovisas under 2009.

[11] Proposition 2001/02:158 s 103

[12] Proposition 2001/02:158 s 103

[13] Proposition 2005/06:133 s 89

1. Utveckla Sveriges position inom EU och i internationella sammanhang
2. Skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet
3. Främja ökad användning av IT
4. Förebygga och kunna hantera störningar i informations- och kommunikationssystem
5. Förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen
6. Förstärka förmågan inom området nationell säkerhet
7. Utnyttja samhällets samlade kapacitet
8. Fokusera på samhällsviktig verksamhet
9. Öka medvetenheten om säkerhetsrisker och möjligheter till skydd
10. Säkerställa kompetensförsörjningen

Sammanfattningsvis kan konstateras att vid sidan av målet att vi ska ha en hög informationssäkerhet i samhället och särskilt kunna förhindra eller hantera störningar i samhällsviktig verksamhet finns få tydliga mål formulerade på generell nivå. De olika strategiernas utformning indikerar dock att utöver

- *Samhällsviktig verksamhet*

bör även:

- *Förtroende och integritetsskydd*
- *Effektivt utnyttjande av IT*
- *Nationell säkerhet*

ses som prioriterade områden när det gäller informationssäkerhet.

I stort sett samtliga nämnda strategipunkter kan inordnas i nämnda områden. Detta gäller även de nedan behandlade sektorsspecifika målen.

2.2 Sektorsspecifika mål

Inom en rad områden har man valt att ytterligare tydliggöra och konkretisera målen för informationssäkerhetsarbetet och/eller IT-utvecklingen i olika strategidokument. Detta gäller särskilt för Internetsäkerhet, hälso- och sjukvård och e-förvaltning.

2.2.1 Strategi för ökad säkerhet i Internets infrastruktur

Målen för arbetet med infrastruktur och Internet finns bland annat i den strategi för ökad säkerhet i Internets infrastruktur som regeringen beslutade om 2006.[15] Regeringens vision är att Internet om tio år är säkert, snabbt och har hög tillgänglighet för alla i Sverige. Vidare konstateras att det är viktigt att

[14] SOU 2005:42 Säker information, Förslag till informationssäkerhetspolitik s 111

[15] Strategi för ökad säkerhet i Internets infrastruktur N2006/5335/ITFoU

enskilda känner förtroende för att de Internetbaserade tjänsterna och att juridiska, ekonomiska och sociala interaktioner fungerar säkert och snabbt.

För att uppnå detta konstateras att säkerhet bör vara en självklar egenskap i kommunikationsnät, program och utrustning vilket gör användarens miljö och kommunikation säker. Ett viktigt mål i arbetet med att åstadkomma detta är att säkra kritiska funktioner, det vill säga funktioner som, om de inte upprätthålls, ger omfattande störningar eller avbrott och på så sätt försvårar eller förhindrar användning av Internet för stora grupper av enskilda användare eller för samhällsviktiga företag, myndigheter och organisationer. Stora delar av infrastrukturen tillhandahålls av privata aktörer och det offentliga åtagandet bygger på krav som marknaden själv inte kan tillgodose. [16]

2.2.2 Nationell IT-strategi för vård och omsorg

Regeringen beslutade 2006 om en nationell IT-strategi för vård och omsorg och lyfte fram IT som ett av de viktigaste verktygen för att förnya och utveckla vård- och omsorgsverksamheterna.[17] Patientsäkerhet, vårdkvalitet och tillgänglighet konstaterades kraftigt kunna förbättras genom användning av olika former av IT-stöd.

Behovet av informationssäkerhet knyts i strategin särskilt till arbetet att skapa en enhetlig informationsinfrastruktur. *”Om känsliga personliga uppgifter i framtiden ska kunna överföras och tolkas elektroniskt, måste både patienter och vårdgivare lita på att uppgifterna behandlas på ett säkert sätt. För att säkerställa fördelarna med en nationell informationsstruktur och samtidigt värna om andra väsentliga intressen såsom patientens integritet och vårdens effektivitet, krävs en författningsreglerad och för vården anpassad modell för informationssäkerhet. På så sätt får vi en definierad minimistandard som inte bara främjar ett säkert utbyte av individuppgifter utan också datakvalitet och tillgänglighet.”* [18]

I strategin konstateras att en ökad användning av IT kräver förbättringar av de grundläggande förutsättningarna i form av enhetlig informationsstruktur, utbyggd teknisk infrastruktur för IT samt ändringar i lagstiftningen.

2.2.3 Handlingsplan för e-förvaltning

Enligt den av regeringen år 2008 framtagna handlingsplanen för e-förvaltning[19] specificeras som övergripande mål för förvaltningen som helhet att det år 2010 *”ska det vara så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av*

[16] Strategi för ökad säkerhet i Internets infrastruktur N2006/5335/ITFoU s 5f

[17] Nationell IT-strategi för vård och omsorg Regeringens skrivelse 2005/06:139 http://www.regeringen.se/content/1/c6/06/03/73/9959f31e.pdf

[18] Nationell IT-strategi för vård och omsorg Regeringens skrivelse 2005/06:139 http://www.regeringen.se/content/1/c6/06/03/73/9959f31e.pdf s 23

[19] Handlingsplan för e-förvaltning, http://www.regeringen.se/content/1/c6/07/49/95/2c28b30b.pdf

förvaltningens service. Där det är till fördel för medborgare och företagare samt där kvaliteten, säkerheten och produktiviteten kan höjas ska myndigheterna samverka sektorsvis. Därigenom ska Sverige återta en ledande position inom området elektronisk förvaltning".

Denna målsättning ska genomföras genom arbete i fyra insatsområden med olika delmål.

Regelverk för myndighetsövergripande samverkan och informationshantering

- Myndigheterna har regelverk som möjliggör sektorsvis samverkan kring e-förvaltning och en effektiv informationshantering som gör informationen lättillgänglig och användbar, med beaktande av integritets- och säkerhetsaspekter.

Tekniska förutsättningar och IT-standardisering

- Myndigheterna har tekniska förutsättningar som stödjer e-förvaltningsarbetet. En effektiv, robust och framtidssäker infrastruktur för elektronisk kommunikation främjas.
- Myndigheterna har en säkerhetsnivå som skapar ett högt förtroende för e-förvaltningen. Standardisering av begrepps- och informationsstrukturer, gränssnitt för elektroniska tjänster och elektronisk kommunikation m m sker utifrån förvaltningens eller sektorns samlade behov och i överensstämmelse med internationella normer.

Gemensamma verksamhetsstöd, kompetensförsörjning och samlad uppföljning

- Verksamhetsstöd som är gemensamma för myndigheterna harmoniseras och automatiseras i lämplig grad i syfte att undvika onödiga kostnader och höja den samlade produktiviteten. De anställda har nödvändig kompetens för att följa och driva utvecklingen. Statens samlade IT-kostnader följs löpande upp.

Förvaltningens kontakter med medborgare och företagare

- Medborgare och företagare kan på ett enkelt sätt utföra och följa ärenden samt ha tillgång till förvaltningens samlade tjänster och information.

Samtliga delmål ställer krav på informationssäkerhetsarbetet inom förvaltningen.

3 Slutsatser

3.1 Inledning

För att i en lägesbedömning ge en bild av på vilken nivå samhällets säkerhet befinner sig måste man först sätta samman utveckling, hotbild, förekomst av sårbarhet och risker samt vilka insatser som gjorts för att därefter relatera detta till vilka mål vi har. Genom att jämföra var vi står med vart vi vill får vi ett underlag för att resonera om vilka områden som vi behöver ägna särskild uppmärksamhet.

I kapitel 2 redogjorde vi för målen på generell och sektorspecifik nivå. Det kan konstateras att de genomgående är förhållandevis allmänt utformade och endast i begränsad omfattning kan ses som mätbara.[20] De ger dock en hänvisning till vilka områden som ses som särskilt viktiga ur ett samhällsperspektiv. I lägesbedömningens slutsatser har vi därför valt att särskilt studera:

- Samhällsviktig verksamhet
- Förtroende och integritetsskydd
- Effektivt utnyttjande av IT
- Nationell säkerhet

3.2 Samhällsviktig verksamhet

Digitala styr- och kontrollsystem (SCADA) som styr el- och vattenförsörjning och annan grundläggande infrastruktur hör till kärnområdet samhällsviktig verksamhet. Området har fått ökad uppmärksamhet i och med att det skapats en publik, tillgänglig och lättanvänd attackkod som utnyttjar en välkänd sårbarhet i ett relativt väl spritt SCADA-system. Sårbarheter som uppstår när äldre SCADA-system kopplas ihop med moderna administrativa system kvarstår fortfarande och har med tanke på förekomsten av alltmer sofistikerade hot blivit mer akuta att hantera. Det är viktigt att ökade satsningar inom området genomförs under de närmaste åren.

[20] Som ett exempel på ett förhållandevis mätbart mål: Medborgare och företagare kan på ett enkelt sätt utföra och följa ärenden samt ha tillgång till förvaltningens samlade tjänster och information.

IT-relaterade hot riktas mot samhällsviktiga funktioner som finansiella tjänster, medieföretag och hälso- och sjukvården.

- Hälso- och sjukvården har under året drabbats av flera incidenter som medfört att patientjournaler blivit otillgängliga och medicinsk utrustning påverkats. Både tekniska och administrativa brister i den elektroniska informationshanteringen har påvisats vilket, när de ses sammantagna med hot som skadlig kod, skapar ett stort behov av ökade insatser när det gäller informationssäkerhet.
- Uppgifter tyder på att medieföretag i vissa fall underlåtit att rapportera om dataintrång på grund av rädsla för repressalier. Detta skulle kunna leda till allvarliga konsekvenser ur ett samhällsperspektiv då kriminella kan påverka medias rapportering och öka mörkertalet.
- När det gäller den finansiella sektorn ligger sårbarheten främst hos kunderna och attackerna riktas mot svagheter i deras säkerhetssystem eller brister i deras säkerhetsmedvetande.

IT-relaterad brottslighet är ett komplext hot mot samhällsviktig verksamhet. Brottsbekämpningen försvåras dels av resursbrist, mörkertal och gränsöverskridande problematik. Verksamheter hanterar händelser internt som tekniska problem medan de i själva verket blivit utsatta för IT-relaterad brottslighet. Säkerhetsarbete och brottsbekämpning inom IT-området är ett område där privata företag tar ett ovanligt stort utrymme och ansvar. En problematik med denna rollfördelning är att gränserna mellan brott och incident blir otydlig och att de brottsbekämpande myndigheterna förlorar överblicken av den IT-relaterade kriminaliteten. Till skillnad från brottsbekämpande myndigheter, är de som begår IT-relaterad brottslighet inte bundna av juridiska och geografiska gränser. För att skapa funktionella och effektiva internationella regelverk och konventioner krävs harmonisering av nationella regelverk. Vi ser därför ett stort behov av ökad samverkan på internationell nivå när det gäller både lagstiftning och brottsbekämpning. Ett viktigt steg är EU-kommissionens allmänpolitiska initiativ från 2007 för att förbättra samordningen på europeisk och internationell nivå när det gäller kampen mot IT-relaterad brottslighet.

Internet utgör en grundläggande del i samhällets elektroniska infrastruktur. Robusthet är en förutsättning för tillgänglighet och förtroende för de tjänster som tillhandahålls elektroniskt. I detta sammanhang vill vi uppmärksamma att användningen av säkerhetsprotokollet DNSSEC fortfarande är begränsad, även om en långsam ökning sker. När det gäller tid bör både beroendet av störningskänsliga tidskällor och bristen på signerade tidskällor i form av signerade NTP-servrar (Network Time Protocol) beaktas av de aktörer som bedriver samhällsviktig verksamhet. Att signera centrala svenska NTP servrar är en förhållandevis enkel åtgärd, som vid sidan av det arbete som PTS bedriver med att minska samhällets beroende av störningskänsliga tidskällor, kan bidra till ökat förtroende för Internets funktioner. Arbetet med att minska antalet oskyddade trådlösa nätverk är mer komplext och bör bedrivas både genom insatser mot användare och återförsäljare. Även tillgång till säkra produkter är

en viktig del i en infrastruktur, arbetet med standarden Common Criteria ser vi som betydelsefullt.

3.3 Förtroende och integritetsskydd

Ett ändamålsenligt skydd av personlig integritet och andra grundläggande fri- och rättigheter är en förutsättning för att skapa ett välgrundat förtroende för olika e-tjänster i samhället. Utvecklingen på IT-området går fort och personlig information hanteras på ett allt mer sofistikerat sätt. Inom en rad samhällssektorer görs omfattande satsningar på en ökad användning av elektronisk informationshantering, inte minst när det gäller e-förvaltning och hälso- och sjukvård. Ny teknik och förändrade användarbeteenden/nya tjänster har också underlättat tillgången till personlig information. På tekniksidan bör RFID uppmärksammas och utvecklingen av webb 2.0 har genom användarvänlighet och användarstyrt innehåll inte sällan lett till en ökad tillgång till personlig information, exempelvis genom sociala nätverk. Spridning av skadlig kod genom sociala nätverk är ett växande hot som kan få direkt påverkan på förtroendet för tjänsterna.

Även lagstiftning har förändrat tillgången till personlig information då lagstiftaren på grund av brottsbekämpningsskäl givit upphovsrättsinnehavare tillgång till information som tidigare inte var nåbar. Angående brottsförebyggande verksamhet bör även signalspaningslagen nämnas då man för att eftersträva teknikneutralitet har skapat förutsättningar för signalspaning i både eter och kabel. Reglering har även bidragit till att förtydliga integritetsskyddet inom vissa områden, som exempel kan nämnas patientdatalagen och återigen signalspaningslagen.

Effektiv brottsbekämpning kan både till viss del inkräkta på integritetsskyddet samt främja det. För att skapa förtroende för informationshantering i elektronisk miljö är det av betydelse att brottsbekämpningen av IT-relaterad brottslighet upplevs som effektiv. Samtidigt måste avvägningen mellan integritetsskydd och brottsbekämpning vara ändamålsenlig.

Det finns en medvetenhet om betydelsen av skydd för personlig integritet vilket avspeglas i flera av de insatser för ökad säkerhet som genomförts under 2008. Exempelvis innehåller samtliga redovisade handlingsplaner ett flertal åtgärder som verkar i en integritetsfrämjande riktning. Enligt regeringens handlingsplan för e-förvaltning är elektronisk identifiering en viktig faktor för tilliten och dialogen mellan myndigheter, medborgare och företag. I många ärenden finns ett behov av säker identifiering, krav på underskrift och skydd för den personliga integriteten.

Målen som är relaterade till förtroende och personlig integritet uttrycker en strävan mot att i ökad utsträckning kunna utnyttja och skapa effektiva e-tjänster samtidigt som behovet av skydd för den personliga integriteten betonas. Brister i brottsbekämpning, sårbarheter i e-förvaltning, hög frekvens av identitetsstölder och stölder av kortinformation indikerar att vi ännu inte har nått våra mål. För att uppnå och upprätthålla ett adekvat skydd finns det enligt vår bedömning ett behov av helhetssyn när det gäller skyddet av personlig integritet, vilket kan uppnås genom att sätta samman teknik, juridik,

användarmönster. Det är av särskild vikt att bevaka teknikutvecklingen och se till att reglering ger tydligt stöd och klara ramar för skyddet. Det är i denna diskussion viktigt att framhäva att integritetsskyddets omfattning ibland måste begränsas på grund av brottsbekämpning. Som ett första steg bedömer vi det vara av stor betydelse att genomföra de insatser som handlingsplanerna förespråkar, samtidigt bör den rättsliga reglering som rör integritetsskyddet regelbundet ses över för att säkerställa att den är utformad på ett adekvat och ändamålsenligt sätt i förhållande till sitt syfte.

3.4 Effektivt utnyttjande av IT

Effektiv IT-användning förutsätter såväl administrativ som teknisk säkerhet. Detta aktualiserar en rad olika områden och vi vill rikta särskild uppmärksamhet mot outsourcing (extern tjänstehantering), nya användarmönster och kontinuitetsplanering.

Externa tjänsteleverantörer hanterar allt mer av samhällets informationsmängd och säkerhetsfrågorna som följer med det. Nivån på kundernas kravställning är mycket varierande vilket kan bero på okunnighet angående säkerhetsbehov, aningslöshet rörande hot men också återhållsamhet gällande kostnader. Den offentliga sektorn styrs av lagen om offentlig upphandling och många myndigheter använder priset som enda kriterium vid utvärdering av inkomna offerter. I många fall har både offentliga och privata kunder en övertro på den säkerhet som ingår i bastjänsten och formar sina avtal därefter. Bristen på medvetenhet om problematiken ser vi allvarligt på och bedömer att det finns behov av kompetenshöjande insatser och eventuell regleringsöversyn.

Nya användarmönster i samband med ökad mobilitet och tillgång till webb 2.0-tjänster medför nya risker för organisationer. Detta bör föranleda mer omfattande säkerhetsarbete men viljan att utnyttja snabb teknikutveckling och strävan efter användarvänlighet gör ofta att säkerhetsöverväganden kommer i andra hand.

Kontinuitetsplanering är en grundläggande del av det interna säkerhetsarbetet för att säkra organisationens verksamhet. Brister har identifierats i flera sammanhang, bland annat har undersökningar under 2008 visat på att det finns brister hos kommuner i deras arbete med att motverka och dokumentera avbrott i sin verksamhet samt skydda kritiska rutiner från effekter av oförutsedda allvarligare avbrott eller katastrofer. Detta tyder på behov av åtgärder för att främja systematiskt informationssäkerhetsarbete.

Användare måste kunna lita på webbinnehåll och skydd av känslig information på webbplatser. Under 2008 noterades ett stort antal attacker mot databaser eller databasservrar knutna till webbplatser. Det bakomliggande problemet vad gäller webbplatsers säkerhet bottnar många gånger i en brist på processer och styrning, att det inte görs säkerhetstester och analyser etc. Många webbplatser är från början inte byggda för ett stort antal användare och vikten har lagts på användarvänlighet och funktion framför ett fungerande informationssäkerhetsarbete. Antalet personer som bygger och förvaltar

webbplatserna är också ofta få i förhållande till antalet användare. Angripare utnyttjar detta och använder olika angreppssätt för att nå sina syften.

Allt komplexare IT-miljö och alltfler integrerade nätverk gör att fokus ofta riktas mot mer begränsade och hanterbara IT-relaterade problem i den egna organisationen. Det är viktigt att även uppmärksamma och analysera konsekvenser och kopplingar ur ett samhällsperspektiv. För att kunna utnyttja informationsteknikens potential och bygga upp nödvändigt förtroende är det avgörande att bygga upp grundläggande informationssäkerhet och kompetens på informationssäkerhetsområdet. Båda punkter är åtgärdsförslag i handlingsplanen för samhällets informationssäkerhet.

3.5 Nationell säkerhet

Händelserna i Georgien och senare Israel/Gaza visar på en utveckling mot konflikter där traditionella väpnade strider pågår parallellt med informationsoperationer. Informationsoperationernas potentiellt asymmetriska karaktär gör det svårt för den drabbade nationen att veta vilken respons som är lämplig eftersom stor osäkerhet kan råda avseende vem som är angripare. Farhågan är att det så småningom kommer att finnas aktörer med tillräcklig mängd information och med kompetens och vilja att utföra cyberattacker som kan störa och slå ut samhällsviktig verksamhet.

Det hot som informationsoperationer utgör mot stater idag kräver ett nytt sätt att se på säkerhet. Vi har hittills sett exempel på cyberattacker ämnade att destabilisera ett land, störa informationskanalerna i samband med väpnad strid, påverka beslutsfattande och rekrytera sympatisörer. Det parallella användandet av informationsoperationer och väpnad strid i samband med konflikter bedömer vi kommer att fortsätta och vidareutvecklas. Ur ett svenskt perspektiv förefaller fortfarande hotet om att samhällsviktiga infrastrukturer ska bli drabbade vid en framtida attack som det mest troliga scenariot men det är även av vikt att vara medveten om riskerna för informationsmanipulation.

Vi bedömer att ett fortsatt fokus på internationell samverkan är nödvändig för att kunna möta den form av asymmetriska hot som informationsoperationer utgör och för att stå bättre rustade inför storskaliga nätverksattacker av den typ som har drabbat flera nationer under senare tid.

3.6 Jämförelse med 2008 års lägesbedömning

2008 års lägesbedömning fokuserade främst på hot och sårbarheter/risker. Detta avsnitt är en kort sammanfattning av ett flertal av de slutsatser som presenterades i föregående års lägesbedömning. För att skapa överblickbarhet har de strukturerats enligt samma huvudmål som används vid behandlingen av mål i lägesbedömningen för 2009.

Samhällsviktig verksamhet: Hotbilden med angrepp mot digitala kontrollsystem uppmärksammades. Här konstaterades att många länder rustade sig för att kunna motstå befarade attacker mot kritisk infrastruktur som elförsörjning, vattenrening och liknande. Amerikanska rapporter pekade på lyckade angrepp mot elnät.

Förtroende och personlig integritet: Problemet med att känsliga persondata sprids till obehöriga lyftes särskilt. Det gäller bl a illegal handel med bankkonton, inloggningsuppgifter, personnummer och kreditkortsuppgifter. Det förekom utpressning baserat på hot att sprida känsliga uppgifter om enskilda personer och företag. Nätbedrägerier var det vanligaste IT-relaterade brottet mot enskilda svenskar och nätfiskekampanjer mot bankkunder förekom såväl 2006 som 2007. Legitima webbplatser manipulerades för att komma åt individers datorer och information.

Effektivt utnyttjande av IT: I rapporten konstaterades att beroendet av IT ökar, speciellt inom verksamheter som sjukvården och finanssektorn, vilket samtidigt innebär ökad sårbarhet. Ett exempel är införandet av e-tjänster men även outsourcing nämndes. Majoriteten av de IT-relaterade incidenterna hos svenska myndigheter orsakas fortfarande av administrativa brister, det gäller bland annat avsaknad av policy och kontinuitetsplaner. Drygt hälften av myndigheterna råkade ut för incidenter under 2007. Driftstörningar förekom inom IP-telefoni, regeringens webbplats, och i Teracoms verksamhet.

Nationell säkerhet: Storskaliga informationsoperationer av den typ som drabbade Estland är en etablerad risk. USA, Storbritannien och Tyskland utsattes för ett ökande antal attacker mot myndigheter 2007. Cyberkrigföring och statsmakters IT-baserade underrättelseverksamhet spåddes växa i omfattning. Terrorhotet mot Sverige bedömdes dock inte som särskilt stort under 2008. Kriminella grupper skapade omfattande nätverk med olika roller uppdelade på olika länder. Två trender lyftes särskilt upp:

- Allt fler små och riktade angrepp,
- stora nät av kapade datorer som kan hyras kommersiellt för att genomföra angrepp

Incidentrapporteringen karakteriserades av ett stort mörkertal, både gällande organisationer och enskilda.

Del B Bakgrund

4 Informationshantering, utveckling och trender under 2008

4.1 Inledning

Teknisk utveckling och förändrade användarmönster påverkar informationssäkerhetsarbetet. En rättvisande analys av behov och brister när det gäller säkerhetsåtgärder måste därför förankras i den faktiska miljö i vilken informationssäkerhetsarbetet skall bedrivas. I föreliggande kapitel har vi valt att välja ut ett antal utvecklingstrender som vi bedömer har stor betydelse för informationssäkerhetsarbetets utformning. Även om teknikutveckling är en förutsättning för flera av trenderna är det ofta först förändrade beteendemönster hos användarna som föranleder mer omfattande säkerhetsöverväganden. Samtliga avsnitt innehåller en kort beskrivning, redogörelse för trendens betydelse ur både ett informationssäkerhets- och samhällsperspektiv, bedömning av utveckling under 2008 samt resonemang om utvecklingens konsekvenser och möjligheter. Vi bedömer att utvecklingen av cloud computing är av särskilt intresse eftersom användningen av tjänstekonceptet spås öka kraftigt framöver. En förståelse för tjänstens struktur är av stor vikt för att kunna hantera hot och sårbarheter på ett säkert och ändamålsenligt sätt. Även webb 2.0 tjänster är av intresse ur ett säkerhetsperspektiv eftersom de både förändrar kommunikationsmönstren hos användarna och gör gränserna mellan privatliv och yrkesliv svårare att urskilja – båda företeelserna kan ha en avgörande påverkan på valet av informationssäkerhetslösningar.

4.2 Ökad mobilitet

På längre sikt ser vi en utveckling med allt högre integration med den mobila världen. Trots att det förekommer säkerhetsincidenter är säkerhet ännu inte ett starkt användarkrav varför problemen inte sällan skjuts på framtiden. Fokus riktas istället mer mot ökad funktionalitet och användarvänlighet. Sårbarheter behandlas närmare i avsnitt 6.3.1 Mobila enheter.

4.3 Webb 2.0

Utvecklingen på Internet går mot en mer användarstyrd miljö med hög interaktivitet. Detta sätt att använda Internet kallas Webb 2.0 och omfattar bland annat Facebook, bilddagboken.se, Wikipedia, bloggning med mera. Det som skiljer den här typen av tillämpningar mot de mer traditionella är att användarna betydligt mer än tidigare själva styr över informationen. Utvecklingen styrs i hög grad av användarnytta och inte i första hand genom nya tekniska lösningar. I dagsläget används dessa tillämpningar såväl privat som inom näringsliv och offentlig verksamhet. Gränsen mellan arbete och privatliv suddas ut och sårbarheter i de tekniska lösningarna kan på det sättet

utnyttjas för att få tillgång till organisationers interna nät. Vad gäller den tekniska säkerheten finns brister hos både sociala nätverk och bloggar.

Den stora ökningen av direktmeddelandetjänster (AOL, Yahoo, MSN Messenger m.fl.) har medfört nya problem för företagen som äldre säkerhetslösningar inte rår på. Eftersom det är lätt att överföra filer via direktmeddelanden har metoden på många ställen blivit allt mer förekommande.

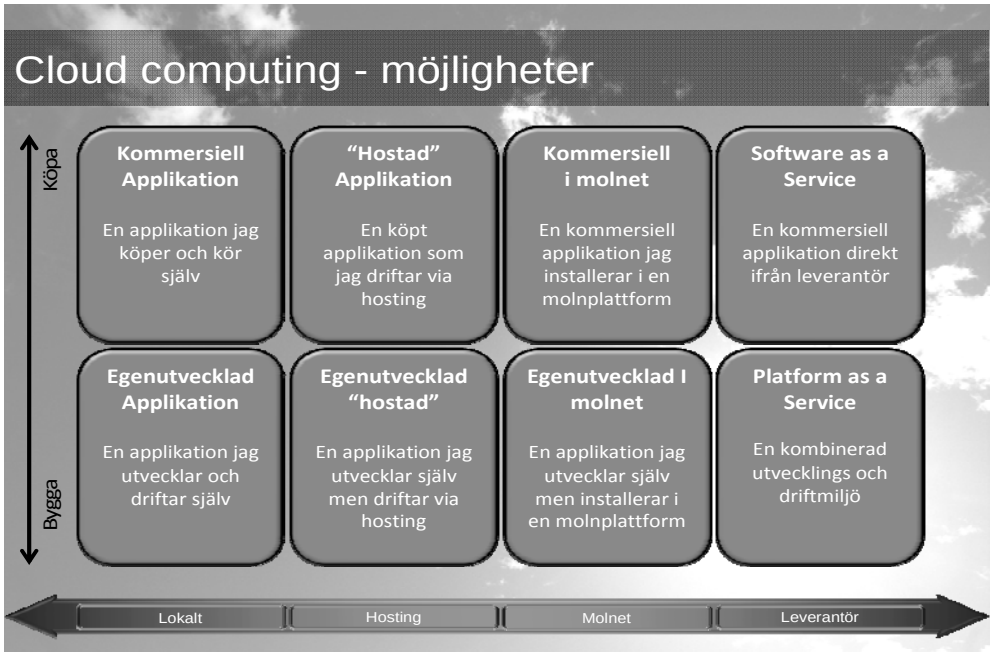
4.4 Extern tjänstehantering (Outsourcing)

Utvecklingen går mot att externa tjänsteleverantörer hanterar allt mer av samhällets informationsmängd och säkerhetsfrågorna som följer med det. Det finns många *fördelar* som exempelvis kostnadsbesparingar, ofta ökad robusthet i drift och förvaltning samt tillgång till en ofta hög teknisk kapacitet och kompetens hos leverantörerna. Till *nackdelarna* hör bland annat att ett beroendeförhållande skapas mellan beställare och leverantör och kompetensförsvagning (framförallt på längre sikt) hos beställaren. Beroendeförhållandet gör att det kan vara besvärligt att ta hem en verksamhet som en gång placerats hos en tjänsteleverantör.

Företag som exempelvis Microsoft, Yahoo och Google bygger nu stora datacenter i USA för att kunna erbjuda en rad olika tjänster. Deras kunder behöver inte längre lagra data, program eller applikationer på sina egna servrar utan detta tillhandahålls av leverantören. Hanteringen av information och styrning av program sker över Internet. Upplägget kallas ofta för Cloud Computing[21] och har fått stor uppmärksamhet det senaste året. Tjänsten är dock idag bara i ett utvecklingsskede och har inte kommit igång i någon större omfattning. Det finns från vissa håll en tveksamhet till Cloud Computing, främst när det gäller säkerheten, men eventuellt har företagen framöver inte något val. Dels på grund av att IT-infrastrukturen har växt enormt och dels eftersom företagens datacenter idag ofta utgörs av en komplex underutnyttjad hårdvara som kräver alltmer personal, utrymme och elkraft för att drivas. Den ekonomiska utvecklingen gör också att företagen hela tiden måste bli mer effektiva och av den anledningen väljer outsourcing. Några av de fördelar som finns är att företagen kan minska sina IT-investeringar och IT-personal och få pengar över till produktutveckling och koncentrera sig på sin kärnverksamhet. I och med ett ökat behov av lagringskapacitet är det positivt för många att kunna köpa lagring som en tjänst i stället för att köpa och administrera allt fler diskar och servrar. I dagsläget är det framförallt de mindre företagen som är mest positiva till detta då de ofta inte själva har den expertis och erfarenhet av att driva stora datacenter som leverantörerna av dessa tjänster har.

[21] För mer information
http://www.economist.com/specialreports/displayStory.cfm?STORY_ID=12411882

Det finns flera olika typer av Cloud Computing. Bilden nedan försöker tydliggöra att företag och förvaltning idag har ett flertal valmöjligheter.



Källa: Microsoft

En viktig balansgång är den mellan de fördelar ett alternativ erbjuder och vad det kan få för konsekvenser ur säkerhetssynpunkt. När ett företag eller förvaltning idag planerar att lägga ut delar av sina system eller verksamhet hos en extern leverantör är det flera säkerhetsaspekter som bör beaktas. En del av kontrollen går förlorad och i många fall hanteras informationen i ett annat land med andra lagar och regleringar vilket kan få konsekvenser. Organisationen har att ta ställning till om det bara är tillåtet att deras data hanteras inom Sveriges gränser, om det kan ske inom EU eller även utanför EU.[22] Andra frågor om säkerheten som bör ställas är hur leverantören sköter säkerhetskopiering? Hur är data säkrad mot intrång och annat missbruk? Går det att lita på att ingen annan kommer åt informationen och att den är tillgänglig utan dröjsmål och avbrott? Går det att lita på att företaget som levererar tjänsten finns kvar om ett år? Går det att byta tjänsteleverantör på ett enkelt sätt? Hur ser den rättsliga regleringen ut?

4.5 Virtualisering och Service Oriented Architecture

Allt fler organisationer använder sig av virtualisering och den ökningen ser ut att hålla i sig även framöver. Om sårbarheter uppstår i de produkter som används för att skapa virtuella servrar finns möjligheten att komma åt inte bara en utan hela serverparken i ett företag. Skadorna kan bli stora om man kör alla

[22] Inte bara personuppgiftslagens (1998:204) regler aktualiseras utan även annan reglering kan vara tillämplig, exempelvis säkerhetsskyddslagen (1996:627).

virtuella servrar på samma maskin. Här krävs samma säkerhetstänkande som vid annan informationshantering.

I och med den snabba förändringen som sker i verksamheter idag och att många system inte fungerar ihop har olika IT-stöd växt fram för att kunna erbjuda mer flexibilitet. Service Oriented Architecture (SOA) eller tjänsteorienterad arkitektur är ett väldefinierat begrepp inom detta område och syftar på att olika system och applikationer ska kunna kommunicera med varandra genom standardiserade gränssnitt. Många analyser visar dock på att det under 2008 var ett vikande intresse för SOA, eller snarare själva begreppet som sådant. Nyttan med standardiserade gränssnitt för elektroniska tjänster finns kvar men utvecklas i nya former och under andra namn.

4.6 Data Loss Prevention

Data Loss Prevention (DLP) möjliggör för organisationer att förhindra att känslig information lämnar organisationen och kommer i orätta händer. Tidigare har fokus riktats mot att förhindra inkräktare men i och med att informationsförluster blir ett allt större problem har behovet för denna typ av teknik ökat. Det är många gånger svårt att inte bara förhindra informationsförlust och utan även upptäcka att det har hänt. DLP kan skapas på flera sätt, exempelvis genom att skapa hinder mot att känslig information kopieras till USB, stoppa kopiera/klistra in-funktionen, se till att accessrättigheterna efterlevs/inte ändras, skydda sig mot att information skickas via webbmail eller direktmeddelanden.

DLP är fortfarande ett relativt nytt begrepp och har inte formats till några övergripande helhetslösningar. Det sker dock en ständig utveckling och funktioner byggs in i olika typer av säkerhetsprodukter. För att implementera en DLP-lösning krävs att en organisations data analyseras på djupet för att identifiera skyddsvärd information och att säkerhetsklassa den. En anledning till att organisationer väntar med att implementera DLP fullt ut är att det anses vara ett omfattande och kostsamt arbete.

4.7 Radio Frequency Identification

Radio Frequency Identification (RFID) är en teknik för att läsa och spara information i ett RFID-chip som i princip kan sägas vara uppbyggd av en radiomottagare, ett minne och en radiosändare. RFID-chip beskrivs oftast som en ersättning till dagens streckkod men skiljer sig dock från streckkod på det sättet att ett RFID-chip är unikt. Tekniken används inom allt fler områden som exempelvis svenska passhandlingar, lagervaror, medicinska förpackningar, inpasseringssystem, kollektivtrafik med mera. Med hjälp av chipet går det exempelvis hämta information om en specifik produkt och utan fysiskt kontakt spåra var den befinner sig geografiskt. Tekniken är relativt billig och det finns en lång rad användningsmöjligheter.

Under 2008 har allvarliga säkerhetsbrister upptäckts, dessa redovisas närmare i avsnitt 6.3.3

4.8 Förändrade beteendemönster på grund av ny lagstiftning

Under 2008 har flera regelverk som enligt vår bedömning kan komma att få användare att förändra sina handlingsmönster trätt ikraft alternativt förberetts. Det handlar främst om lagen om signalspaning i kabel (2008:717) och förändringarna i det immaterialrättsliga regelverket[23], baserade på det så kallade IPRED-direktivet. Båda ger utvalda grupper ökad tillgång till viss information som inte tidigare varit tillgänglig.

I lagen om signalspaning får FRA under vissa premisser möjlighet att bedriva signalspaning i kabel för trafik som går över landets gränser. Detta utgör en tydlig skillnad mot tidigare förhållanden då den typen av spaning endast fick göras i etern. Skälen till utvidgningen var att eftersträva teknikneutralitet. Lagen reglerar såväl integritetsaspekter som inriktning. Se vidare avsnitt 7.3.2

Förändringarna i upphovsrättslagen underlättar arbetet att lagföra upphovsrättsintrång genom att ge upphovsrättsinnehavare rätt att efter domstolsbeslut begära ut uppgifter från teleoperatörer om vem som innehar den IP-adress till vilken upphovsrättsskyddat material olagligt laddats ned.[24] Regleringsförändringen bygger på ett EG-direktiv[25] och har som syfte att motverka immaterialrättsliga intrång. Se vidare avsnitt 7.3.2.

Debatten kring regelförändringarna har kretsat kring integritetsfrågor och tidvis varit intensiv. Även ur ett internationellt perspektiv har den här typen av frågor väckt uppmärksamhet, som ett exempel kan nämnas integritetsdiskussioner för några år sedan rörande signalspaningssystemet Echelon.[26] Både regelförändringarna och de därtill knutna debatterna kan leda till en ökad användning av kryptering som ett sätt att försvåra insyn i trafiken. Även en minskning av antalet oskyddade och okrypterade trådlösa nätverk är en möjlig utveckling.[27] Detta i syfte att hindra att någon obehörigen utnyttjar ett oskyddat trådlösa nätverk för att ladda ned upphovsrättsskyddat material.

---

[23] I prop 2008/09:67 föreslås ändring av lag om upphovsrätt till litterära och konstnärliga verk (1960:729), varumärkeslagen (1960:644), patentlagen (1967:837) m fl

[24] I övrigt sker inte någon förändring vad gäller krav på bevisning. Det är fortfarande nödvändigt att visa vem som suttit vid tangentbordet i samband med att upphovsrättsskyddat material olovligt laddats ned.

[25] Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter

26 Se t ex http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN och http://www.cyber-rights.org/interception/echelon/

[27] KBM genomförde 2008 en kartläggning av antalet okrypterade trådlösa nätverk i tre större städer och det kan finnas skäl att upprepa kartläggningen de närmaste åren för att upptäcka eventuella förändringar.

5 Antagonistiska hot

5.1 Inledning

Ett antagonistiskt hot förutsätter en aktör (antagonist) som med avsikt och förmåga genomför skadliga handlingar. Till de icke antagonistiska hoten brukar man räkna naturkatastrofer och tekniska fel där den gemensamma nämnaren är att det saknas avsikt och tydlig avsändare. Med hänsyn till ofta förekommande svårigheter att skilja mellan icke antagonistiska hot och sårbarheter har vi valt att behandla dessa gemensamt i kapitel 6.

De antagonistiska hoten som vi redogör för i detta kapitel har delats upp beroende på syfte; hot riktade mot samhället i stort, respektive hot riktade mot individ/organisation. Någon klar gränslinje finns inte mellan de båda områdena. Omfattande angrepp mot ett större antal organisationer får inte sällan konsekvenser på samhällsnivå och direkta angrepp mot centrala samhällsfunktioner, exempelvis infrastruktur, innebär ofta i praktiken angrepp mot vissa enskilda organisationer. Trots gränsdragningsproblematiken har vi valt att göra en uppdelning. Detta främst för att tydliggöra den spännvidd som finns när det gäller de antagonistiska hotens syfte, omfattning och konsekvens.[28] Samtliga delavsnitt innehåller en kort beskrivning, redogörelse för hotets betydelse ur både ett informationssäkerhets- och samhällsperspektiv, bedömning av utveckling under 2008 samt resonemang om hotets konsekvenser. Av särskilt intresse finner vi utvecklingen av hot mot *digitala kontrollsystem* (SCADA) som tidigare endast rörde de administrativa systemen. Området informationsoperationer är också intressant där vi ser en trend mot situationer där väpnade konflikter även fortsättningsvis kommer att ske parallellt med cyberangrepp.

5.2 Samhällsnivå

5.2.1 Hot mot samhällsviktiga verksamheter

Genom att följa hotbildsutvecklingen hos våra samhällsviktiga verksamheter har vissa trender kunnat iakttas. Vi har valt att lyfta följande exempel, som vi anser vara av extra stort intresse med tanke på de inledningsvis beskrivna målen att kunna förhindra eller hantera störningar i samhällsviktig verksamhet, beaktandet av förtroende och integritetsskydd och effektivt

[28] Som underlag för kapitlets iakttagelser och bedömning har vi bland annat använt oss av resultaten från ett samarbetsprojekt mellan Brottsförebyggande rådet (BRÅ) och KBM, som även var uppdragsgivare, angående strategiska IT-incidenter som kan ha konsekvenser för samhällsviktiga verksamheter. BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008

utnyttjande av IT. Under rubriken informationsoperationer beskrivs förhållanden som mer direkt knyter an till frågor angående nationell säkerhet.

- *Under 2008 har området digitala kontrollsystem (SCADA- system) fått ökad uppmärksamhet i och med att det för första gången hittills skapats publikt tillgänglig, och lättanvänd, attackkod som utnyttjar en välkänd sårbarhet i ett relativt väl spritt SCADA-system.*

Sammanfattningsvis är det mycket svårt att ge någon entydig bild av de antagonistiska hoten mot SCADA-system i samhällsviktiga verksamheter. SCADA- system utgör en kritisk del av de system som försörjer samhället med elektricitet, värme, dricksvatten, bränslen samt transporter. Till skillnad från administrativa system, där fördröjning kan vara acceptabel och tillgänglighetsavvikelser kan tolereras kontrollerar SCADA-system tidskritiska verksamheter och tillgänglighetskraven är därför mycket höga. Dessa system har tidigare haft ett gott skydd genom att de varit isolerade från andra system och omgärdats av god fysisk säkerhet.[29] Genom integration med kontorsnätverk utsätts nu SCADA-system i stor utsträckning för samma typ av hot som tidigare endast drabbade de administrativa datasystemen. Under 2008 har området digitala kontrollsystem (SCADA- system) fått ökad uppmärksamhet i och med att det för första gången skapats publikt tillgänglig, och lättanvänd, attackkod som utnyttjar en välkänd sårbarhet i ett relativt väl spritt SCADA-system.[30] SCADA-säkerhet har behandlats vid hackerkonferenser sedan många år tillbaka, och relativt detaljerade tekniska diskussioner pågår i olika forum. Under senare år verkar området även ha fått en ökad uppmärksamhet bland mindre kvalificerade hackers och begagnad utrustning som används i kontrollsystem efterfrågas, och erbjuds, i olika sammanhang på Internet.

- *Det har påvisats fall av dataintrång hos myndigheter där sekretessbelagda uppgifter blivit tillgängliga för organiserad brottslighet.*

Även om det endast handlar om ett fåtal fall, är det ur ett samhällsperspektiv mycket allvarligt om kriminella kan ta del av sekretessbelagd information från våra myndigheter. Information om myndigheters arbete och tillvägagångssätt har tidigare visat sig vara eftertraktad i kriminella miljöer. Om människor upplever att deras personuppgifter inte förvaras på ett säkert sätt utgör detta ett hot mot den personliga integriteten och ur ett samhällsperspektiv blir det ett problem om medborgarna tappar förtroendet för myndigheternas kompetens och förmåga. Tillgänglighets- och överbelastningsattacker tillhör

[29] Exempelvis låsta dörrar, larm och stängsel

[30] Läs mer kap 6.2.2

annars vardagen för de flesta myndigheter och i de allra flesta fall får de inte några allvarliga konsekvenser utan hanteras av det tekniska skyddet.[31]

- *Bedrägerierna inom den finansiella sektorn riktar sig främst mot användarna*

De svenska bankerna har överlag en hög säkerhet. Bedragarna utnyttjar istället brister hos den enskildes säkerhetssystem eller i dess säkerhetsmedvetande.[32] Finansiella tjänster är ett av de huvudområden som har strategisk betydelse för det svenska samhällets funktionssätt. Inom detta område är förtroendeskador ett av de stora hoten då Internetbaserade finansiella tjänster idag har en omfattande användning. Det kan få stor betydelse för samhället om förtroendet för Internetbaserade finansiella tjänster skulle urholkas. En fortsatt utveckling av hoten mot användare kan leda till frågeställningar för bankerna om vilka krav på säkerhet de kan ställa på användarna. Eftersom bankernas system inte är angripna har de ingen juridisk skyldighet att ersätta bedragna kunder. Ofta väljer de dock att ersätta de som drabbats av Internetbedrägerier förutsatt att de polisanmält brottet.[33]

- *Det finns uppgifter om att media har undvikit att rapportera om dataintrång och stulen information.*

Medieföretag har avstått från att rapportera om dataintrång som drabbat dem själva alternativt konkurrerande medieföretag. Åtminstone i ett fall uppger ett företag som utsatts för dataintrång och fått känslig information publicerad på nätet att man inte vågat gå vidare med en polisanmälan av rädsla för att angreppen ska trappas upp. De misstänker också att konkurrerande mediebolag avstår från att rapportera om händelsen för att undvika att själva bli en måltavla för dessa grupper.[34] Media har i ett demokratiskt system till uppgift att granska samhället och informera om viktiga händelser. Misstanken om en utbredd rädsla för repressalier från angripare vid en anmälan är därför särskilt alarmerande då medias trovärdighet som objektiv granskare och nyhetsförmedlare skulle kunna undermineras. Medieföretag är liksom andra organisationer frekvent utsatta för försök till tillgänglighetsattacker,

---

[31] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 33

[32] Vanligt är då med s.k. Man-in-the-middle-attacker, där bedragaren först infekterar offrets dator med en trojan. När kunden sedan försöker logga in på sitt bankkonto via Internet visar bedragaren en falsk webbsida där kunden skriver in sina inloggningsuppgifter. Bedragaren kan sedan använda inloggningsuppgifterna för att flytta pengar från offrets konto.

[33] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 22

[34] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 36

överbelastningsattacker och dataintrång. Majoriteten av dessa hanteras av det tekniska skyddet.[35]

5.2.2 Informationsoperationer

Informationsoperationer (IO) kan nyttjas som en form av icke-militär maktutövning men även som ett komplement till konventionella militära insatser. Informationsoperationer kan utgöra ett asymmetriskt[36] hot vilket bl a innebär att angrepp mot en nation kan utföras av allt från en annan statsmakt till en liten grupp individer eller till och med av en enskild person. De verktyg som används är ofta desamma som vid vardagliga handlingar i fredstid. Angriparen har även en stor fördel i det att det går att utföra angrepp anonymt.

Begreppet IO används främst i USA och inom NATO. I Sverige finns ännu ingen officiell definition men SIS definierar begreppet som: *"samlade och samordnade åtgärder i fred, kris och krig till stöd för egna politiska eller militära mål genom att påverka eller utnyttja en motståndares eller annan utländsk aktörs information och/eller informationssystem medan man samtidigt utnyttjar och skyddar egen information och/eller informationssystem. Det yttersta målet är att påverka det mänskliga beslutsfattandet. Informationsoperationer kan vara såväl offensiva som defensiva operationer."*[37]

Informationsoperationer kan utföras som en cyberattack t ex genom att olovligen ta sig in i ett datasystem, det kan vara en förmåga att utnyttja olika nätverk för kommunikation eller en handling i syfte att manipulera information. För att åstadkomma något av detta finns olika tekniker, t ex genom att plantera in skadlig kod i olika system för att på så sätt obemärkt kunna stjäla viktig information. Informationsoperationer kan också genomföras med hjälp av överbelastningsattacker mot ett system i syfte att störa en verksamhet eller helt sätta den ur funktion.

Nedan följer några exempel hämtade från nyhetsnotiser under det gångna året.

Dataspionage
Den finska staten och företag inom den finska vapenindustrin har utsatts för dataspionage. En eller flera anställda har fått e-post som innehållit virus vilket gjort det möjligt för angriparen att komma över information på enskilda handläggares datorer likväl som till lösenordsskyddade nätverk. De första attackerna ägde rum under 2004 och sen har de ökat i frekvens. Under 2008 har ökningen varit dramatisk. Några attacker har spårats till Kina men för den skull behöver attackerna inte vara utförda där. Attackerna har varit av det slaget att en anställd har fått e-post från en kollega eller annan känd person rörande ett möte eller annan fysisk händelse.

[35] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 34

[36] Asymmetriskt hot är benämningen på hot som har sin grund i att även en tekniskt eller materiellt svagare aktör kan anpassa och utnyttja sitt agerande för att utnyttja motpartens resursmässigt, politiskt eller psykologiskt svagare sidor. Ur SOU 2004:32, s 19

[37] SIS Terminologi för informationssäkerhet utgåva 3, 2007

Meddelandena har innehållit bifogade Word- Excel- eller PDF-dokument som innehållit skadlig kod anpassad för den attacken. Datorn har fortsatt att fungera helt normalt efter den infekterats.[38]

DDoS-attacker/ överbelastning
Flera webbplatser som drivs av Radio Free Europe och som riktar sig mot Vitryssland överbelastades under två dygn i en attack på uppemot 50 000 ping-anrop per sekund. Attacken startade på årsdagen av kärnkraftshaveriet i Tjernobyl och Radio Free Europe bevakade då demonstrationer där tusentals personer protesterade mot att många drabbade inte fått kompensation och mot regeringens beslut att bygga ett nytt kärnkraftsverk. Radio Free Europe finansieras av USA för sprida information i länder där demokratin är hotad.[39]

Som ytterligare exempel på informationsoperationer kan nämnas när defekter redan i produktionsstadiet avsiktligt läggs in i hård- och mjukvara som sedan exempelvis säljs till myndigheter och/ eller företag. Någon enskild producent eller enskilt land pekas sällan ut i de här fallen. Uppgifter i media hänvisar till en analys gjord av US Air Force, december 2007, som visade på att mycket av Pentagons operativsystem är så kallade COTS-komponenter (standardprodukter) som har tillverkats utomlands. Orsaken till varför man köper de här produkterna och därmed utsätter sig för risker uppges vara kostnadsmässiga.[40]

5.2.3 Internets militarisering

Internet skapades från början som ett militärt projekt men har med tiden blivit oumbärlig för civil verksamhet i alla dess former dock utan att omfattas av någon internationell gemensam reglering. Idag kan Internet utnyttjas för att skapa hot mot nationers säkerhet och många länders militärer förbereder sig för att defensivt men även offensivt kunna hantera cyberhot i framtida konflikter.[41]

IT-relaterade angrepp i form av cyberattacker, karaktäriseras av att de verktyg som används är de samma som förekommer i normalbilden av ständigt pågående småskaliga attacker. Det är därför inte troligt att ett angreppsverktyg ensamt kan ställa till stor skada utan det är kombinationen av flera metoder och verktyg samt hög kapacitet som kan framkalla en farlig situation. Att skaffa fram relevanta underrättelser om förberedelser för ett angrepp har därför visat

[38] Nyhetsbrevet Delete nr. 78, www.hs.fi/english/article/Finnish+state+and+armaments+industry+targeted+by+online+espionage/1135237080345

[39] Nyhetsbrevet Delete nr. 76, http://www.securityfocus.com/news/11515 http://sakerhet.idg.se/2.1070/1.159392

[40] Council on foreign relations ,*The Evolution of Cyber Warfare*, Greg Bruno, Februari 2008, http://www.cfr.org/publication/15577/#2

[41] http://www.ccdcoe.org/8.html

sig vara mycket viktigt och nödvändigt för att kunna presentera en övergripande lägesbild.[42]

Cyberattacker har gett ytterligare en dimension åt dagens konflikter. Allt fler länder uppger att de blir utsatta för cyberattacker med anknytning till särskilda säkerhetspolitiska omständigheter. De storskaliga nätverksattackerna mot Estland i maj 2007 då medier och myndigheter fick sina webbtjänster utslagna av överbelastningsattacker är den cyberattack som har rönt mest medial uppmärksamhet. Omvärlden blev påmind om informationssamhällets sårbarhet och frågor väcktes om informationsoperationer som ett icke-militärt verktyg för maktutövning.[43] Händelserna beskrevs efteråt i media som en av de absolut största och mest sofistikerade cyberattack någonsin mot en suverän stat.[44] Vissa experter hävdar dock att det vi fick se endast var toppen av ett isberg med tanke på den mängd attacker som sker. Flera stater har vid upprepade tillfällen pekats ut i media för att ha genomfört liknande attacker. Vanligtvis tillbakavisas alla beskyllningar av länderna i fråga.[45]

Händelserna i Estland[46] följdes av ett flertal incidenter under 2008. Georgien drabbades i augusti 2008 av koordinerade cyberattacker mot bland andra utrikesdepartementets webbsida. Angreppen uppges ha haft många likheter med händelserna i Estland 2007. En stor skillnad var att cyberattackerna i Georgien skedde parallellt med väpnad strid på marken. En allvarlig konsekvens av liknande attacker är att samhällets förmåga att fungera och leda påverkas negativt genom att möjligheten att kommunicera och informera medborgarna blir lidande. Georgien, som inte har kommit lika långt inom sin IT-utveckling som Estland, påverkades sannolikt mer av de väpnade striderna än av de digitala attackerna.

I samband med de israeliska attackerna mot Gaza i januari 2009 uppgavs både israeliska och palestinska webbsidor ha blivit attackerade bland annat i form av *defacement*[47]. Företeelsen brukar benämnas *hacktivism*, det vill säga en fusion av hackning och politisk aktivism och har setts vid flertalet tidigare konflikter.[48] Båda sidor uppgavs ha distribuerat verktyg för att utföra vissa

---

[42] Att snabbt kunna sätta ihop en stabsfunktion med aktörer från samtliga aktuella områden visade sig vara mycket värdefullt för det estniska hanterandet av angreppen 2007.

[43] http://www.aff.a.se/vf2008_2/Information%20Nicander%20sid%2036.htm

[44] T ex Computer Sweden 2007-06-12

[45] Council on foreign relations, *The Evolution of Cyber Warfare*, Greg Bruno, Februari 2008, http://www.cfr.org/publication/15577/#2

[46] De storskaliga nätverksattackerna mot Estland har lett till en rad initiativ inom NATO som beskrivs närmre i stycke 7.5.5 *Internationell samverkan*

[47] Defacement innebär ofta att en angripare ersätter en ursprunglig webbsida med en ny, inte sällan innehållande politiska budskap. Aktiviteten har ibland beskrivits som elektronisk graffiti.

[48] http://www.theregister.co.uk/2009/01/09/gaza_conflict_patriot_cyberwars/

angrepp på motståndarens webbsidor. Att genom Internet rekrytera sympatisörer är en metod som har använts vid flera tillfällen.

Det råder delade meningar om huruvida ett hot i form av cyberkrig existerar och hur det i så fall ser ut. Ännu finns ingen definition av var gränsen går för när en cyberattack kan likställas vid ett väpnat anfall eller gemensam strategi kring vilka motåtgärder som då kan anses vara legitima. [49] En metod som förefaller vinna visst gehör bland internationella aktörer kan förenklat beskrivas som ett antal satta kriterier som skall uppnås för när ett angrepp skall kunna likställas vid ett väpnat angrepp. Dessa kriterier är att:

- händelsen har vållat stor skada
- nationsgränser har forcerats
- det inträffade har skett inom minuter eller timmar
- attacken har riktats mot ett specifikt mål.[50]

En av utmaningarna vi står inför är att mäta risken för angrepp. Vissa experter påstår att det pågår kontinuerliga attacker inom ramen för vad man skulle kunna kalla ett ”tyst” cyberkrig där mjuka mål angrips längre ut på kedjan i form av produkter i syfte att sedan klättra mot det primära målet. Syftet med att angripa dessa delar uppges vara att säkerheten är mindre robust där. Ett sådant pågående skeende uppges heller inte vara lika dramatiskt på samma sätt som en traditionell terrorattack och undgår därför upptäckt.

Måltavlor och konsekvenser av IT-relaterad brottslighet kan ha samma karaktär som politiskt eller militärt motiverade aktioner. Som ett exempel på det kan nämnas en händelse i februari 2009 då franska attackflygplan uppgavs ha blivit hindrade från att lyfta på grund av ett datavirus som hade drabbat ett internt datanätverk där nödvändiga instruktioner fanns. Den bakomliggande orsaken var troligen att tidigare utskickade varningar om detta datavirus från det drabbade IT-företaget hade ignorerats av berörda. [51]

Farhågan är att det så småningom kommer att finnas aktörer med tillräcklig mängd information och som är djärva nog att utföra cyberattacker tillräckligt stora för att störa och slå ut viktig nationell infrastruktur.[52] Flera bedömare anser att cyberangrepp i form av rena nätverksattacker kommer att bli ett normalt inslag parallellt med väpnade strider i konfliktsituationer framöver.[53]

När ett land drabbas av ett angrepp är det inte otänkbart att hjälp skjuts till från tredje part exempelvis genom teknisk expertis. Eller som i fallet Georgien 2008 då flera myndigheters webbplatser flyttades och lades upp i andra länder

[49] Se vidare under avsnitt 6.2.8.3 angående ett folkrättsligt perspektiv.
[50] Sk “Smith’s Analyse”, uppgifter från *Cyber Warfare conference*, Defence IQ PC, London 2009
[51] French fighter planes grounded by computer virus, Daily Telegraph, 07 Feb 2009
[52] McAfee, *Virtual Criminology Report - Cybercrime Versus Cyberlaw*, 2008
[53] B la: http://www.ccdcoe.org/8.html

som ett sätt att undkomma angreppen. Även NATO som nyligen har utvecklat en cyberförsvarspolicy och ett koncept för cybersäkerhetsfrågor sände ut folk till Georgien som stöd vid angreppen. Vad händer om en tredje part ses som en del i en pågående konflikt?

5.3 Organisation och individnivå

5.3.1 IT-relaterad brottslighet

Begreppet IT-relaterade brott [54] kan syfta på *”en handling som innefattar otillåten insyn i eller påverkan på ett informationssystem”*[55], en vidare ansats innefattar även brott där datorn används som ett verktyg eller hjälpmedel vid brottet t ex har Internet underlättat etableringen av svarta marknader och hjälpt dem nå nya dimensioner. Som exempel kan nämnas försäljningen av läkemedel över Internet som innefattar många oseriösa aktörer. [56]

Det framgår tydligt i de flesta undersökningar att möjligheten att tjäna pengar har kommit att bli den största drivande faktorn när det gäller IT-relaterade brott. IT-relaterade brott riktade mot organisationer eller individer har samma syfte som traditionella brott så som bedrägeri, utpressning, förtal och sabotage. Till skillnad från traditionella metoder anses IT-brottslighet ofta vara en relativ enkel, säker och lukrativ väg till snabba pengar. Det finns flera skäl till detta. Ett är att den kriminelle har möjlighet att agera anonymt. En skicklig förövare använder sig av metoder som gör det svårt att spåra denne eller som leder spåren till fel land, organisation eller person. Ett annat är oviljan hos offren att anmäla brottet.[57]

Aktörerna bakom IT-relaterade brott har visat sig vara både enskilda individer och tillfälligt sammansatta grupper. Det förekommer en kunskapsöverföring mellan enskilda, ofta ungdomar och kriminella organisationer, en överföring som går i båda riktningarna. De mest systematiska bedrägerierna har till stor del kopplingar till organiserad brottslighet med en påtagligt internationell karaktär. Dessa grupper har tillgång till omfattande resurser i form av bland annat avancerade verktyg, botnät och så kallade målvakter. Målvakterna upplåter, mot betalning, sina bankkonton för transaktioner och förmedlar

[54] Enligt Kommissionen, KOM/2007/0267 avser begreppet IT-relaterad brottslighet tre olika kategorier av brottslig verksamhet. Den första omfattar traditionella brottsformer som bedrägeri eller förfalskning, som i detta sammanhang begås med hjälp av elektroniska kommunikationsnät eller informationssystem (nedan kallade ”elektroniska nät”). Den andra kategorin rör offentliggörande av olagligt innehåll via elektroniska medier (t.ex. barnpornografiskt material eller hets mot folkgrupp). Till den tredje kategorin hör brott som uteslutande riktas mot elektroniska nät, dvs. angrepp mot informationssystem, överbelastningsattacker och olaga intrång i informationssystem (s.k. hackning). Gemensamt för alla dessa brottskategorier är att de kan begås i stor skala och att det geografiska avståndet mellan den brottsliga handlingen och dess följdverkningar kan vara stort.

[55] SIS Terminologi för informationssäkerhet utgåva 3

[56] För mer information se: Läkemedelsverket, http://www.lakemedelsverket.se/Tpl/NormalPage____1034.aspx

[57] Läs mer kap 6.2.8.6

pengarna vidare därifrån. De rekryteras genom sociala nätverk eller genom webbsidor där ett falskt företag söker medarbetare. Olika specialistfunktioner kopplas in vid de organiserade bedrägerierna, rekryteringen av målvakter flyttar runt mellan europeiska länder och för att få korrekt språk vid exempelvis nätfiske anlitas tolkar. Denna brottlighet kan liknas vid ett kriminellt affärsnätverk där brottsverktyg, specialistkompetens och hela brottskoncept köps och säljs. Nätverken består av till synes löst sammansatta celler där personer med rätt kunskap och kapacitet tillfälligt ansluts för att fylla en viss funktion. Genom att använda sig av Internet som kontaktyta förblir aktörerna anonyma för varandra och få av dem har en helhetsbild av vad som egentligen sker. Misstankar finns att nätverken både kan agera värdar för enskilda individer och för mindre organisationer som säljer tjänster och produkter för IT-relaterade brott, men även att grenar av internationell organiserad brottslighet styr större operationer själva.[58]

Den vanligaste typ av information som blir stulen är den rörande kreditkortsuppgifter och därefter personliga identifierande data.[59] Den tillhörande svarta marknaden för dessa uppgifter är mycket stor och kan liknas med virtuella varuhus. De stulna uppgifterna kan till exempel användas för att köpa varor på Internet eller ta lån i en annan persons namn. Undersökningar visar att då ett intrång har gjorts tar det ibland bara minuter innan informationen blivit stulen men det kan ta månader eller år innan skadan upptäcks.

5.3.2 Nätfiske

Nätfiske uppges växa, särskilt inom den finansiella sektorn. De allra flesta nätfiskeattacker uppges vara riktade mot finansiell verksamhet och utgör enligt vissa undersökningar så mycket som 95 procent av fallen.[60] Det finns en trend som pekar på att mindre skyddade finansiella institutioner faller offer för den här typen av brottslighet i en ökande takt. Nya organisationer blir hela tiden drabbade och spridningen av nätfiske sker globalt. Det har tidigare varit aktörer i främst Europa och Nordamerika som drabbats men nu sker många nya nätfiskeattacker mot organisationer i Mellanöstern och Sydamerika.[61] En annan trend är att angriparna riktar in sig på mindre webbplatser för sociala nätverk med färre användare i och med att de stora etablerade webbplatserna har förbättrat säkerheten.[62] Sårbarheter i webbapplikationer behandlas närmare i avsnitt 6.3.4.

---

[58] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?,* 2008

[59] Verizon business, *Data breach investigations report*, 2008

[60] Se t ex Symantec, *Global Internet Security Threat Report, trends for July-December 2007*, 2008

[61] Cyveillance, White paper, *Online financial fraud and identity theft report*, 2008

[62] Microsoft*, Security Intelligence Report January through June 2008,* 2008, s 69

5.3.3 IT-relaterad utpressning

IT-relaterad utpressning måste uppmärksammas eftersom det förekommer uppgifter om att utpressare ofta lyckats med att få de pengar de krävt. Polisen kan inte bekräfta företeelsen utan den kan härledas till uppgifter från IT-säkerhetsföretag. Något som dessa företag uppmärksammat på senare tid är kriminella som tar sig in i ett företags system och krypterar lagringsmedia som kan vara information i ekonomisystem, kundregister med mera. Efter en viss tid tar de kriminella kontakt med företaget och meddelar att de mot betalning kan dekryptera informationen. I och med att krypteringen är stark[63] finns det till synes ingen annan utväg än att betala, vilket mest troligt resulterar i att fler anammar denna verksamhet.[64]

5.3.4 Virus och skadlig kod

Den största risken med stora angrepp av Internetvirus med bred bas anses av många vara förbi. Sådana angrepp genomfördes tidigare till stor del för att hackaren skulle uppnå uppmärksamhet och berömmelse bland sina likar. Den nya generation säkerhetshot som sprids idag består av skadliga angrepp ledda av cyberbrottslingar som är riktade mot specifika företag för personlig eller ekonomisk vinning. Metoderna blir alltmer sofistikerade och aktörerna mer organiserade och ekonomiskt motiverade. Helt ska dock inte hotet med breda angrepp avskrivas. Detta visades inte minst när region Skåne i januari 2009 smittades av ett virus som till att börja med smittade personalens e-postsystem men sedan spred sig vidare till medicinsk utrustning. [65]

Skadlig kod[66] kan idag köpas anpassad för ett valt ändamål, komplett med regelbundna uppdateringar och tillhörande ”kundsupport”.[67] Det finns flera fall där företag drabbats av riktade utskick innehållande skadlig kod. Den skadliga koden skickas exempelvis med en mötesförfrågan eller en PDF-fil vars innehåll för mottagaren förefaller röra verksamheten. Det kan dessutom röra sig om en version av skadlig kod som antivirusprogrammet inte kan upptäcka för tillfället. När mottagaren har öppnat filen aktiveras en trojan som öppnar dörren för vidare dataspionage, datastöld och installering av annan skadlig kod. Norge har t ex uppgett en ökad trend av målriktade trojaner under året. De verksamheter som har drabbats uppges finnas inom försvarssektorn, aktörer inom högteknologisk industri som elektronik, försvar, flyg och petrokemi men drabbade är även människorättsorganisationer och ledare på olika nivåer. Trojaner används också för att ta kontroll över bankkunders datorer.

---

[63] Till skillnad mot svag kryptering, som inte sällan kan knäckas med hjälp av olika hjälpmedel, är stark kryptering använd på korrekt sätt så komplex att krypteringsnyckel krävs för att åter göra den krypterade informationen läsbar.

[64] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?,* 2008

[65] Läs mer i kapitel 6.2.7 angående sårbarheter i Hälso- och sjukvård

[66] Ett samlingsnamn för virus, trojaner m m

[67] http://www.ccdcoe.org/8.html

Det uppges stora skillnader mellan olika trojaner som används vid den här typen av bedrägerier. De enklaste går att hitta gratis på Internet medan de mer sofistikerade och dyrare varianterna har mindre spridning. Ofta utnyttjas sårbarheter i icke uppdaterad programvara för att sprida skadlig kod men det är svårt att skydda sig mot de mer sofistikerade trojanerna eftersom de antivirusprogram och brandväggar som framförallt privatpersoner normalt använder inte upptäcker dessa.

År 2008 uppvisade även ett ökat problem med *Drive-by downloads*[68], vilket innebär att det räcker med att besöka en preparerad webbplats för att bli infekterad. Många användare surfar med dåligt uppdaterade webbläsare som gör att de är sårbara för denna typ av attacker.

5.3.5 Spam

Spam eller oönskad, obeställd e-post fortsätter att vara ett problem för många verksamheter. Det förekommer att så mycket som mer än vartannat mail inom en verksamhet är spam. Ett av de stora problemen för de drabbade är inte bara mängden i sig utan även hantera plötsliga mängdökningar av olika utskick eller skräppost. För att kunna hantera dessa måste det finnas en beredskap vilket kräver planering och stora resurser. Statistik från intresseorganisationer tyder på att det i grunden är en förhållandevis begränsad grupp som ligger bakom majoriteten av spamutskick.[69] Det har visat sig att riktade punktinsatser där man lyckats spåra och stänga av specifika botnät som förmedlar spam har resulterat i en kraftig om än tillfällig nedgång av mängden spam. I november 2008 stängdes ett okänt webbhotel[70] ned efter uppgifter om att det hade härbärgerat servrar till många av världens spamskickande botnät. Inom loppet av några timmar uppgavs andelen spam över hela världen sjunka med cirka 60 procent. Efter 3-4 veckor hade nivåerna i stort sett återgått till det normala igen men händelsen visar på att det går att störa distributionen av spam och att det är viktigt att kartlägga distributionskedjorna för att kunna finna sätt att motverka spamspridningen.

5.3.6 Social Engineering

Social engineering handlar om manipulering av människor där sociala knep används för att bygga förtroende som kan ge åtkomst till känslig och hemlig information.[71] En attack genom social engineering har ett tydligt syfte och målgruppen är begränsad till skillnad från mer traditionellt nätfiske där mycket av styrkan ligger i ett stort spridningsområde för att öka chanserna. Studier har visat att bedragare på nätet blivit alltmer skickliga i att manipulera människor med hjälp av social engineering genom att utnyttja deras psykologiska svagheter, en framgångsrik metod. Den stora skillnaden mellan social

[68] Läs exempelvis: http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html

[69] Läs exempelvis http://www.spamhaus.org

[70] Webhotel McColo se bla. *Q4 2008 Internet Threats Trend Report* www.halonsecurity.com

[71] SIS Terminologi för informationssäkerhet utgåva 3

engineering och nätfiske, som också är en form av manipulation, är den högre graden av personlig kontakt som det förstnämnda innebär. För att hantera detta är vanligt säkerhetsarbete och enstaka kurser för användare och anställda ofta inte är tillräckliga. Teoretisk information behöver kompletteras med exempelvis interna kontroller och praktiska övningar för att uppnå nödvändiga beteendeförändringar hos personalen.

Framtida hot beskrivs i en aktuell svensk avhandling vara ett slags automatiserat social engineering där mjukvara med en enkel form av artificiell intelligens kan efterlikna mänskligt beteende online.[72] Syftet är att manipulera användare som inte vet med vem eller vad de kommunicerar. Det här skulle i förlängningen kunna leda till förtroendeproblem för exempelvis olika tjänster på internet. Flera experter påpekar betydelsen av extra uppmärksamhet mot social engineering i tider av ekonomiska svårigheter då människor möjligen har större benägenhet att låta sig luras av bedrägerier i form av erbjudanden om snabba lättförtjänta pengar.[73]

5.3.7 Botnät

Ett botnät är en samling datorer som infekterats av skadlig kod med en styrmekanism som gör det möjligt för personer bakom botnäten att kontrollera datorerna, ofta utan användarens vetskap. Detta innebär att medborgare eller organisationer ofrivilligt kan delta i kriminell aktivitet. Det är till stor del mängden datorer som styrs från en och samma källa som gör ett botnät effektivt och det används ofta till spam och DDoS-attacker.

Enligt uppgifter från många bedömare är antalet drabbade datorer världen över flera miljoner, men det är omöjligt att ge några exakta siffror i sammanhanget. Vissa bedömare anser att minst 12 miljoner datorer i världen tillhör ett botnät med ett genomsnitt på 280 000[74] nya anslutna datorer per dag. Cirka 350 000 kapade datorer uppges dagligen vara i bruk och det har upptäckts botnät med fler än 5 miljoner kapade datorer.[75] Som beskrivs i avsnittet angående spam 5.3.5 minskade antalet aktiva botnät under en kortare period år 2008 vilket resulterade i märkbart färre spamutskick.

Det finns ingen klar statistik över hur utbredningen av botnät ser ut i Sverige. PTS har i en färsk rapport kommit fram till att uppskattningsvis färre än en procent av bredbandsanslutna datorer i Sverige är drabbade. Enligt Shadowserver, som är en organisation med inriktning på att spåra botnät och analysera dess utbredning i världen observerades i snitt 1436 kapade svenska datorer under perioden januari till september 2008. En svensk

---

[72] "Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks", Marcus Nohlberg, Stockholms Universitet 2009

[73] Nyhetsbrevet Delete nr. 81,/08, http://www.darkreading.com/shared/printableArticle.jhtml?articleID=211601123

[74] Halon security Rapport , *Q4 2008 Internet Threats Trend Report*, 2009, www.halonsecurity.com

[75] Uppgifter från Cyber Warfare conference, Defence IQ PC 2009

Internetleverantör konstaterade vid en mätning i oktober 2008 att det fanns 5000 kapade datorer i det egna bredbandsnätet. Ur ett nationellt perspektiv skulle det motsvara en förekomst av ca 27000 kapade datorer totalt i Sverige.[76] Som synes skiljer sig uppgifterna åt.

En aktör kan hyra ett botnät för att exempelvis utföra spionage, sabotage eller utpressning. Den tekniska utvecklingen har lett till att de kapade datorerna kan uppdateras flera gånger i timmen med skadlig kod och nya kommandon.

Oavsett vad ett botnät har för syfte innebär det ofta stora hanteringskostnader för de verksamheter som drabbas. Det stora utbudet har troligen att göra med en ökad efterfrågan på en marknad där vem som helst utan några särskilda kunskaper kan köpa eller hyra ett botnät. Konsekvenser av detta är att alltfler har tillgång till de verktyg som behövs för att utföra sofistikerade attacker och risken är att fler lockas att utföra kriminella handlingar.

[76] Post- och telestyrelsen, Botnät - Kapade datorer i Sverige, PTS-ER-2009:11

6 Sårbarhet och risker

6.1 Inledning

I detta kapitel riktas fokus mot sårbarhet och risker i samband med informationshantering. Liksom i kapitel 5 om hot har en indelning skett av sårbarheter som identifierats på samhällsnivå respektive på organisations- och individnivå. På samhällsnivå har vi valt att fokusera på elektroniska kommunikationer, digitala kontrollsystem, kryptografiska funktioner, mediesektorn, offentlig verksamhet, finansiella tjänster, hälso- och sjukvård samt brottsbekämpning. Samtliga karaktäriseras av att bristande informationssäkerhet innebär en negativ påverkan för samhället. Känsliga uppgifter kan komma i fel händer, betalningsströmmar kan hejdas eller omdirigeras, misstänkta brott kan inte utredas. Medborgarna förutsätter att informationshanteringen inom dessa områden ska fungera och vara säker. Under rubriken organisations- och individnivå har vi valt att fokusera på funktioner som är avgörande för att den enskilda organisationens eller individens verksamhet ska fungera. Det bör nämnas att det inte går att göra en helt invändningsfri uppdelning mellan samhällsnivå respektive organisation och individnivå.

Samtliga delavsnitt innehåller en kort beskrivning, redogörelse för sårbarhetens/riskens betydelse ur både ett informationssäkerhetsperspektiv och ett samhällsperspektiv, bedömning av utveckling under 2008 samt resonemang om konsekvenser och förekomst. Vi bedömer att sårbarheter i SCADA-system och behovet av säkra produkter och tjänster bör uppmärksammas.

6.2 Samhällsnivå

6.2.1 Elektroniska kommunikationer

Alla delar av samhället drabbas i någon utsträckning om de elektroniska kommunikationerna faller bort. Tillsammans med elförsörjningen är de direkt avgörande för att upprätthålla normal funktion i vårt samhälle. Många gånger drivs verksamheter av el, medan de styrs och kontrolleras genom elektroniska kommunikationer. Det är komplicerat att skapa redundans för elektroniska kommunikationer eftersom operatörerna ofta hyr kapacitet av varandra.[77]

PTS genomförde hösten 2007 och under våren 2008 en planlagd tillsyn angående god funktion och teknisk säkerhet hos tjänstetillhandahållare inom telefoni, mobil telefoni, IP-telefoni, Internet, nätkapacitet, fast mobil, e-post

[77] KBM, *Klarar vi krisen? Samhällets krisberedskapsförmåga 2007*, KBM:s temaserie 2008:2. I rapporten analyserades både elektroniska kommunikationer och elförsörjning närmare och flera brister konstaterades.

och TV.[78] Med säkerhet menas i sammanhanget arbete med att förebygga avbrott och störningar genom riskanalyser och riskhantering, planering för hantering av avbrott och störningar samt uppföljning av dessa när de inträffar.

Enligt PTS allmänna råd bör säkerhetsarbete beslutas om på ledningsnivå och följas i verksamheten. Tillsynen visar att detta sker hos 9 av 10 tjänstetillhandahållare, såväl vid normala förhållanden som vid extraordinära händelser. Det är dock inte alla som följer upp att de beslutade åtgärderna genomförs. Den största bristen i säkerhetsarbetet uppges vara avsaknaden av dokumenterade rutiner. Dokumenterade rutiner behövs för att kunna säkerställa att säkerhetsarbetet blir kontinuerligt och systematiskt, mer enhetligt och mindre personberoende. Några tjänstetillhandahållare ser säkerhetsarbete som aktiviteter kopplade till teknisk infrastruktur men de bestämmelser som finns gäller alla aktörer som tillhandahåller elektroniska kommunikationsnät eller tjänster, oavsett teknik. PTS påpekar vikten att ta med de mjuka faktorerna så som *personal*, *kompetens* och *processer* i säkerhetsarbetet. De glöms annars lätt bort i sammanhanget trots att de i allra högsta grad bidrar till tjänsternas och nätens goda funktion och tekniska säkerhet. Vad det gäller *uppgraderingar* och *ändringar* är det viktigt att informera användarna om dessa eftersom de kan påverka driftsäkerheten och därmed användarnas möjligheter att nyttja elektroniska kommunikationstjänster. Trots detta underlåter 2 av 10 att informera sina kunder om sådana förändringar.[79]

6.2.2 Digitala kontrollsystem

Under 2008 började icke-fackpress på allvar upptäcka att det rapporterades sårbarheter även när det gäller digitala kontrollsystem (SCADA). Den första renodlade SCADA-sårbarheten rapporterades av US-CERT i maj 2006 och sedan dess har 23 specifika SCADA-sårbarheter dokumenterats och rapporterats. Större delen av sårbarheterna är vad som inom den traditionella IT-världen skulle bedömas som relativt vanliga sårbarheter, exempelvis av typen buffer overflow. När det gäller IT-säkerhet i SCADA-system brukar den ofta anses ligga 5-15 år efter den traditionella IT-världen. Följande exempel väckte stort intresse både i fackpress och annan media och illustrerar tydligt att det saknas bra processer för att rapportera och hantera sårbarheter.

Exempel – Sårbarhet i CitectSCADA
En av de mest uppmärksammade händelserna under 2008 är rapporteringen av en sårbarhet i CitectSCADA.[80] I slutet av januari upptäckte

[78] Tillsynen var ämnad att följa upp hur bestämmelserna om god funktion och teknisk säkerhet efterlevs enligt lagen om elektronisk kommunikation (LEK)

[79] God funktion och teknisk säkerhet i elektroniska kommunikationer - PTS-ER-2008:13

[80] Citect Pty Ltd ägs sedan 2006 av Schneider Electric och levererar programvara för industriell automatisering i mer än 80 länder genom ett nätverk av fler än 500 partners. CitectSCADA är ett HMI/SCADA-programvarupaket som körs på persondatorer av standardtyp med Microsoft operativsystem

säkerhetsföretaget Core Security Technologies en sårbarhet i programvaran och kontaktade Citects support.[81] Processen som följde tog mer än fem månader och inledningsvis såg Citect inget behov av att ta fram en uppdatering (patch) utanför ordinarie uppgradering av systemet. Först efter att Core skjutit på offentliggörande av sårbarheten tre gånger samt blandat in CERT-organisationer i Australien, USA och Argentina, tog Citect fram en patch. Den 11 juni 2008 släpptes ”CORE Security advisory CORE-2008-0125”. Citect uppmanade sina kunder att uppgradera systemet men tonade ned allvarligheten av säkerhetshålet i ett pressmeddelande. Den 5 september 2008 släpptes en attackkod (exploit) som utnyttjar sårbarheten, i form av en modul till det publikt tillgängliga attackpaketet Metasploit. Kort därefter ändrade Citect sitt initiala pressmeddelande och poängterade allvarligheten i säkerhetshålet.[82]

Det finns ett antal faktorer som gör exemplet CitectSCADA intressant. Först och främst kan det vara värt att notera att Core Security Technologies inte är en traditionell SCADA-konsult, och att det därför är ett exempel på hur problematiken börjar bli alltmer intressant för andra än de specifika leverantörerna och användarna i SCADA- branschen. Sårbarheten i programvaran var av typen buffer overflow och skulle kunna, om den utnyttjas, leda till att en obehörig person kan stänga ned programvaran (en DoS-attack) eller exekvera egen kod i systemet. Tillängligheten hos SCADA-system är kritisk och även om en angripare inte lyckas ta kontroll över en verksamhet som styrs av programmet, kan en DoS-attack leda till allvarliga konsekvenser. Eftersom Core har dokumenterat och offentliggjort alla sina kontakter med Citect går det att studera själva förloppet mycket tydligt. Exemplet kan därför även ses som en illustration av det faktum att många SCADA-leverantörer saknar processer för hur sårbarheter ska hanteras och rapporteras. Citect ansåg inledningsvis att det inte var nödvändigt att ta fram en patch och först efter det att Core gjort upprepade påtryckningar och meddelat att man menade allvar med att publicera sårbarheten ändrade sig företaget. Core gjorde även upprepade försök att få Citect att ge ett datum för när en patch skulle vara framtagen, men Citect förhalade detta ett flertal gånger – bl a genom att hävda att det vara ett företagsinternt, kommersiellt, beslut. Värt att notera är också att Citect hela tiden kommunicerade i klartext med Core via e-post. Företaget hade inte möjligheten att använda vanlig kryptering som t ex PGP. Mycket intressant är också det förlopp som följde rapporteringen av sårbarheten.

Efter det att Citect i sitt pressmeddelande tonat ned sårbarhetens allvarlighet släpptes en exploit som skrivits för attackpaketet Metasploit – den första publika exploit-koden som riktats specifikt mot SCADA-system. Offentliggörandet av exploit-koden följdes av en hel del debatt i SCADA-kretsar. Det är dock viktigt att ha i minnet att sårbarheten i sig var ganska enkel

http://www.citect.com/index.php?option=com_content&view=article&id=1457&Itemid=1314

[81] http://www.coresecurity.com/content/citect-scada-odbc-service-vulnerability

[82] http://www.citect.com/documents/news_and_media/CitectSCADA-security-response.pdf

och att exploit-kod av den här typen släpps dagligen i den traditionella IT-världen för lättanvända attackpaket som Metasploit. En hel del icke-publik exploit-kod har synts till under de senaste två åren enligt välkända konsultbolag som exempelvis Digital Bond, och många experter har därför förväntat sig att det ska komma publik exploit-kod riktad mot SCADA förr eller senare.

I dagsläget finns inga uppgifter om huruvida någon användare drabbats av ett intrång till följd av sårbarheten i CitectSCADA. Det finns heller inga uppgifter om hur många användare som faktiskt installerat den patch som Citect släppte. Fortfarande saknar många användare rutiner för hur system ska uppgraderas och många SCADA-system saknar även antivirus och intrångsdektekteringssystem (IDS). Under de senaste åren har dock alltmer specialtillverkad hårdvara – exempelvis brandväggar som känner igen protokoll som används i SCADA-system – kommit ut på marknaden. Även på programvarusidan börjar förändringar kunna skönjas. I dag finns omkring 25 000 plug-ins till Nessus som är det vanligaste programmet för att skanna efter en viss sårbarhet. För närvarande är 40 av dessa plug-ins specifikt relaterade till SCADA-system. Eftersom vanliga IT-komponenter används mycket flitigt i SCADA-system är många traditionella Microsoft och UNIX-sårbarheter också kritiska för SCADA-system.

I lägesbedömning av samhällets informationssäkerhet från KBM för 2008 rapporterades om CIA:s presentation om ett antal attacker mot SCADA-system.[83] Presentationen innehöll inga närmare tekniska detaljer eller uppgifter om vilka typer av angripare det handlade om. Ingen uppföljning av presentationen har skett under 2008 och informationen är alldeles för knapphändig för att vara praktisk användbar för dem som använder SCADA-system. Bristen på öppenhet kring incidenter fortsätter att vara ett problem inom området och i samband med det ökade intresset från icke-fackpress som följde sårbarhetsrapporteringen har återigen flera gamla incidenter tagits upp i media. Under 2008 har få nya incidenter rapporterats. Nedan beskrivs dock en incident som fick stor uppmärksamhet och särskilt illustrerar problematiken med att integrera SCADA-system med administrativa IT-system.

Exempel – Störning i Edwin I. Hatch Nuclear Power Plant, Unit 2
Den 7 mars 2008 tvingades kärnkraftsreaktorn Hatch 2 i USA till ett snabbstopp efter att en programvaruuppdatering gjorts i en dator i anläggningens kontorsnätverk. Efter 48 timmar kunde anläggningen startas igen. Den dator som uppdaterades övervakade kemiska och diagnostiska data från anläggningens primära kontrollsystem och programvaran var konstruerad för att synkronisera data i det primära kontrollsystemet med data i datorn i kontorsnätverket. När datorn i kontorsnätverket startades om ställdes data i kontrollsystemet om och anläggningens säkerhetssystem uppfattade detta som en möjlig sänkning i vattenreservoaren i reaktorns kylsystem. Anläggningens säkerhetssystem fungerade alltså korrekt och

[83] Vid konferensen SANS SCADA Security Summit i New Orleans i januari 2008.

enligt uppgifter i den incidentrapport som lämnades till U.S. Nuclear Regulatory Commission (NRC) påverkades inte anläggningens säkerhet.[84]

Integrationen mellan SCADA-system och kontorsnätverk fortsätter och den varken kan, eller bör, stoppas. I den vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter[85] som togs fram av KBM och ett antal myndigheter i samverkan med industrin under 2008, rekommenderas att integrationen måste ske på ett kontrollerat sätt. För vissa typer av extremt kritiska system kan dock den enda lösningen vara att fullständigt isolera SCADA-system från andra nätverk.

6.2.3 Kryptografiska funktioner

Information bör skyddas då den hanteras, lagras samt vid kommunikation mellan organisationer. Kryptografiska funktioner kan nyttjas för att garantera konfidentialitet, riktighet och tillgänglighet.

Då en organisation skall införa kryptografiska funktioner bör detta vara väl förankrat i hela organisationen från ledning till slutanvändare eftersom det är viktigt att det finns resurser i form av medel och personal för att utveckla, införa och förvalta det krypto som skall införas. Dessutom måste slutanvändarna informeras, utbildas samt få tillgång till en användarinstruktion. Tekniken utgör enbart en mindre del av en säker lösning som omfattar kryptografiska funktioner. Den större delen består av regelverk, rutiner, utbildning och en aktiv medverkan från personalen. Dessa delar måste utvecklas och göras kända inom organisationen. Då en angripare planerar att attackera ett system där kryptografiska funktioner nyttjas tittar denne först på regelverket för att där finna svagheter i rutiner samt i hanteringen av kryptonycklar eller certifikat. Brister i slutanvändarens utbildning eller dennes förståelse för vikten av att följa användarinstruktioner och fastställda rutiner underlättar för angriparen att genomföra en framgångsrik attack.

Sårbarheter uppkommer inte bara vid implementering utan det är även av vikt att välja rätt kryptografisk funktion. Inom offentlig verksamhet finns idag inga heltäckande riktlinjer för val av kryptografisk funktion, vilket kan leda till osäkerhet. I handlingsplanen för samhällets informationssäkerhet föreslås att generella råd och rekommendationer bör utarbetas som riktar sig till statliga myndigheter men även till kommuner, företag m.fl. Syftet är att uppnå en

[84] I dagsläget finns ingen officiell rapport från NRC om incidenten. Beskrivning av händelseförloppet ovan har hämtats från Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html, vilka bl a intervjuat representanter för det företag som sköter teknikdriften i anläggningen.

[85] KBM, *Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter*, 2008

likartad säkerhetsnivå som underlättar möjligheten till informationsutbyte mellan myndigheter och mellan olika funktionssystem.[86]

6.2.4 Mediesektorn

Nyhetsmedierna bedriver samhällsviktig verksamhet ur flera perspektiv, såväl under normala förhållanden som vid extraordinära händelser. Medierna ingår i samhällets varnings-, larm- och informationssystem. Delar av mediesektorn är därför mycket viktiga för alarmering och krishantering vid extraordinära händelser, både för att sprida information och för beslutsfattandet i samhället i stort. Viktigt meddelande till allmänheten (VMA), myndighetsmeddelanden samt kärnkraftslarm är exempel på viktiga informationssystem som på olika sätt är beroende av fungerande mediekanaler.

Ur ett demokratiskt perspektiv är medierna nödvändiga som en daglig källa för vår omvärldsbevakning, för det fria ordet och för opinionsbildningen. Att allmänheten förväntar sig ständig tillgång till sina ordinarie informationsskällor märks så fort ett avbrott inträffar.

Elavbrott, avbrott i elektroniska kommunikationer och hot mot journalister är de tre hot som större medieföretag upplever är mest sannolika att de ska inträffa. Efter brand är elavbrott och avbrott i elektroniska kommunikationer de händelser som anses medföra de allvarligaste konsekvenserna.

Hittills har endast blåljusmyndigheter, som polis och räddningstjänst, anslutits till Rakelsystemet[87], men gruppen användare kommer att utökas och medieföretagen har uttryckt ett behov att få ansluta särskilt berörda medier till systemet. Rakel kan exempelvis användas för att förmedla VMA genom att säkra kommunikationen mellan SOS Alarm och Sveriges Radio.[88]

Digital-tv-övergången har förändrat förutsättningarna för att hantera störningar och använda alternativa distributionsvägar. Tekniska system är ofta sårbara i samband med större förändringar. Teknikskiften medför förnyade behov av inlärning och kan påverka säkerhet och beredskap negativt under en övergångsperiod. En central aktör inom mediesektorn är Teracom som äger och ansvarar för det digitala såväl som det analoga markbundna TV- och radionätet. Även om Teracom har erfarenhet av digitala sändningar sedan nästan tio år är erfarenheten av att arbeta med improviserade lösningar i en krissituation ännu inte lika omfattande som i den analoga miljön.

PTS har beslutat att Teracom har en generell skyldighet att ge andra aktörer tillträde till marknätet. Konsekvenserna av detta är i dagsläget svåra att bedöma. Under 2008 har Näringsdepartementet låtit utreda konsekvenserna

[86] Handlingsplan för samhällets informationssäkerhet, s 49

[87] Rakel är ett gemensamt radiokommunikationssystem för organisationer i samhället som arbetar med allmän ordning, säkerhet eller hälsa. Från och med 1 januari 2009 ansvarar MSB för Rakelverksamheten.

[88] Styrelsen för psykologiskt försvar, *Risk- och sårbarhetsanalys av mediesektorn 2008,* 2008, s 23

av en utförsäljning av det statligt ägda Teracom. En utförsäljning bör föregås av en grundlig analys av vilka konsekvenser det kan få för Teracoms säkerhets- och beredskapsarbete utifrån ett samhällsperspektiv.

6.2.5 Offentlig verksamhet

6.2.5.1 Kontinuitetsplanering

Inom ramen för arbetet med lägesbedömningen utreddes hur kontinuitetsplanering hanteras i kommuner. Stora brister påvisades och de största är relaterade till planeringen för hur verksamheterna arbetar med att motverka och agera vid oplanerade avbrott. Brister i kommunernas kontinuitetsplanering har även konstaterats i det löpande arbetet som bedrivits av KBM respektive MSB, exempelvis vid aktivt stöd från myndigheten för att driva planeringsprocessen, samt i samband med länsstyrelsernas utbildning i informationssäkerhet riktad mot kommuner.

Inom kommunerna finns i de flesta fall policydokument med definierade ansvarsroller och inriktning för hur arbetet med informationssäkerhet ska genomföras. Policydokumenten ger dock som regel ingen direkt ledning vad gäller kontinuitetsplaneringens omfattning. Inte i något fall har ledningen angett om det finns särskilda skäl att upprätta en katastrofplan. Dessutom saknas som regel inriktning för hur kontinuitetsplaneringen ska samordnas mellan ledning, verksamhet och IT-stöd. Ansvaret för att hantera avbrott ligger tydligt i linjeorganisationen men samtidigt saknas insikten om hur beroende den egna verksamheten är av IT-stödet. Olika ansvarsroller gällande informationssäkerhet finns definierade men i flera fall är innebörden oklar, detta gäller särskilt systemägarrollen.

Kommunen måste fungera även om det uppstår en störning i form av ett avbrott. Därför är det viktigt att identifiera vilka verksamheter i kommunen som är helt nödvändiga för att kunna undvika oacceptabla konsekvenser för medborgarna. I de flesta kommunerna har planeringsprocessen för att hantera avbrott påbörjats. Förankrade och fastställda acceptabla avbrottstider för verksamheterna är avgörande ingångsvärden för kontinuitetsplaneringen när det gäller kommunens viktigaste IT-system. Dessa värden saknas i många av de kartlagda kommunerna. Beräkning av avbrottstid baseras exempelvis på vilken servicenivå som ska upprätthållas vid ett avbrott, kritiska tidpunkter eller hur den extra arbetsanhopningen efter ett avbrott ska hanteras. I vissa fall har avbrottstider bestämts utan dessa ingångsvärden.

Planering för hur verksamheterna ska kunna bedrivas vid ett avbrott med hjälp av olika reservrutiner för informationshantering saknas genomgående. Arbetet har inte påbörjats eller genomförts vid någon av de tio besökta kommunerna. Brist på reservrutiner medför att risken för att flera viktiga samhällsfunktioner inom kommunen kan få en väsentligt lägre servicenivå gentemot allmänheten i händelse av oplanerade avbrott. Beroende på när i tiden ett avbrott inträffar kan konsekvenserna öka. Bedömning av genomförbarheten i verksamheternas reservrutiner är grunden för att kunna avgöra om servicenivån är acceptabel eller inte.

På IT/driftnivån finns i de flesta fall förutsättningar för att hantera en avbrottssituation. Svagheterna är att befintlig systemdokumentation inte är sammanhållen eller helt aktuell, därutöver finns svårigheter att hantera personberoendet. Kontinuitetsplaner finns i de allra flesta fall på IT/driftsnivå. Dessa är dock inte koordinerade med verksamheternas krav i de fall nödvändiga ingångsvärden från verksamheterna saknas.

Det finns stora svårigheter att hålla planeringen aktuell samt att få kontinuitet i hela planeringsprocessen. Vid de besökta kommunerna har vid flera tillfällen processen startats upp men successivt tappat fart. Omtag görs då i planeringen vilket i många fall leder till att tidigare erfarenheter och kunskaper inte beaktas i planeringsprocessen.

6.2.5.2 Andra administrativa och tekniska sårbarheter

En enkätundersökning riktad till myndigheter indikerar på mycket varierande informationssäkerhetsnivåer hos de tillfrågade när det exempelvis gäller informationssäkerhetspolicy, hotbildsanalyser, incidenter och hantering av logguppgifter.

Mindre myndigheter saknar i högre utsträckning än de större motsvarigheterna informationssäkerhetspolicy. Flera myndigheter uppgav att de hade en IT-säkerhetshandbok, IT-säkerhetsinstruktion eller IT-säkerhetspolicy men saknade en övergripande informationssäkerhetspolicy.

Av de 73 myndigheter som svarade på enkäten uppgav 71 procent att de upprättar hotbildsanalyser.

Flera incidenter rapporterades. Det är bland annat brott mot upphovsrätt, intrångsförsök i IT-system, hackade datorer, DoS-attacker, virus och trojaner, botnät-infektioner och diverse skadlig kod. Även andra typer av händelser har förekommit såsom temperaturstegringar och strömbortfall för datorhall, ofullständiga säkerhetskopior för flertal system och användardata samt hot riktade mot personalen.

68 procent av de myndigheter som svarade på enkäten uppgav att de samlar in och lagrar loggуppgifter, endast 32 procent analyserade dessa kontinuerligt.

Många myndigheter uppger att de skulle kunna tänka sig att rapportera incidenter till Sveriges IT-incidentcentrum, SITIC, som PTS ansvarar för.

6.2.6 Finansiella tjänster

För samhället är det av största vikt att det för finansiellt samhällsviktiga tjänster finns en mycket hög driftsäkerhet i betalningssystemet. Kärnan i betalningssystemet är clearingsystemet för stora betalningar (RIX), Bankgirot, Värdepapperscentralen (VPC), Dataclearingen[89] och storbankernas

[89] Dataclearingen är ett system för betalningsförmedling från konto till konto. Bankgirocentralen sköter driften och bankföreningen är systemägare. Under 2008 förmedlades drygt 99 miljoner transaktioner.

uppkoppling mot systemen. Enligt Finansinspektionen (FI) är det i regel endast störningar i de fyra storbankerna och de centrala finansiella infrastrukturbolagen som kan slå ut de grundläggande finansiella tjänsterna i samhället i stort. Störningar hos de mindre lokala bankkontoren, mindre finansiella företag, enstaka kortterminaler och bankomater är enligt FI försumbar ur ett samhällsperspektiv.[90]

Idag genomförs bara några promille av alla betalningar med kontanter, resten hanteras genom datoriserad infrastruktur som kopplar samman olika finansiella aktörer.[91] Skador på betalningssystemen och finansiella tjänster kan medföra allvarliga konsekvenser för samhällsekonomin och kan i förlängningen påverka förtroendet för hela det finansiella systemet[92]. I avsaknad av rättsliga krav på att företag ska hålla en lägsta driftsäkerhet för betaltjänster arbetar FI för att bredda samverkan till att omfatta även sektorer utanför FI:s ansvarsområde såsom myndigheter och företag inom el, tele- och Internetsektorn.[93]

FI har endast tillsynsansvar över vissa delar av betalningssystemet. RIX, kortläsare, värdetransporter och vissa delar av clearingen av kortbetalningar är exempel på områden som ligger utanför FI:s ansvar. Det finns även delar av betalningssystemet som ligger utanför Sverige och som står under utländska myndigheters tillsyn alternativt helt saknar tillsyn.[94]

En betydande del av den finansiella infrastrukturen utgörs numera också av allmänheten som genom privatdatorer kommunicerar med Internetbanker. När privatpersoner blir en del av den finansiella infrastrukturen kompliceras det säkerhetsarbete som i övrigt ligger hos finansiella institut och statliga myndigheter.[95] Bedrägerier som riktar sig mot användare av Internetbanktjänster är ett vanligt IT-relaterat brott. Bedragarna utnyttjar brister i privatpersoners säkerhetssystem eller brister i deras säkerhetsmedvetande. På så vis får bedragarna tillgång till de uppgifter som behövs för att använda sig av personliga Internetbaserade finansiella tjänster, exempelvis att genomföra transaktioner och värdepappershandel.

Den sammanlagda förlusten av bedrägerierna kan uppgå till betydande summor och innebära förtroendeskador för Internetbaserade finansiella

---

http://www.bankforeningen.se/Publicerat/Nyhetsbrev/Nyhetsbrev%20nr%201%20februari%202009/Drygt%2099%20miljoner%20transaktioner%20i%20Dataclearingen.aspx?tipsa=true

[90] Finansinspektionens rapport 2008:10, *Ansvaret för betalningssystemet*, s 3.

[91] Sveriges Riksbank, *Sårbarheter i det moderna betalningsväsendet,* Srejber, E. tal på Sveriges säkerhetsting i Eskilstuna 2006-10-18.

[92] Riksrevisionen, *Krisberedskap i betalningssystemet*, RiR 2007:28

[93] ”Ansvaret för betalningssystemet, Finansinspektionens rapport 2008:10, sid 1.

[94] ”Ansvaret för betalningssystemet, Finansinspektionens rapport 2008:10, sid 4.

[95] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008 sid 21.

tjänster. Ett problem i bekämpningen av de organiserade bedrägerierna är att det är svårt att erhålla en helhetssyn då varje enskilt fall behandlas som ett enskilt ärende.[96] Vid enskilda brott med lågt straffvärde har Polisen inte möjlighet att använda sig av hemlig teleövervakning i utredningarna och kartläggningen av bedrägerierna eftersom teleövervakning enligt rättegångsbalken förutsätter ett lägsta straffvärde på fängelse i 6 månader.[97] I dessa fall är det inte heller möjligt att begära ut IP-adresser från operatörer eftersom lagen om elektronisk kommunikation endast tillåter att sådana uppgifter lämnas ut när det föreligger misstanke om brott för vilket det inte är föreskrivet lindrigare straff än 2 år.[98]

Ett annat problem är den internationella karaktären på bedrägerierna som behandlas i stycke 6.2.8.4. om gränsöverskridande samarbete.

6.2.7 Hälso- och sjukvård

Elektroniska patientjournaler utgör en central del i vårdens informationssystem. De innehåller känslig information i många former vilken, inte minst på grund av lagkrav, måste ges ett ändamålsenligt skydd. Den 1 juli 2008 trädde den nya patientdatalagen ikraft och det är därmed möjligt att genomföra den nationella IT-strategin inom vård och omsorg, som presenterades 2006, fullt ut. Syftet är att med hjälp av IT få till stånd en bättre samverkan mellan hälso- och sjukvårdens aktörer och en starkare patientorientering i verksamheten. Det är av stor betydelse att patientinformation som delas mellan olika vårdinstanser kan överföras på ett säkert sätt för att garantera och upprätthålla en god patientvård och trygga patientens integritet.

Den svenska sjukvården har dock under året drabbats av flera allvarliga IT-haverier och systemfel.[99] Främst handlar det om incidenter med journalsystem som havererar och gör patientjournaler otillgängliga. Enligt en avhandling om informationssäkerhet inom vårdsektorn är ett av de största säkerhetsproblemen att patientinformation inte är tillgänglig vid behov.[100] Exempelvis ledde i januari 2008 ett strömavbrott vid Universitetsjukhuset i Lund till att det elektroniska journalsystemet slogs ut under tre timmar. Sjukhusledningen bedömde störningarna som mycket allvarliga och katastrofläge var nära att utlösas. I Region Skåne fick i januari 2009 ett virus genom regionens interna e-postsystem snabb spridning till medicinteknisk utrustning.

---

[96] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 29.

[97] Rättegångsbalk (1942:740), 27 kap 19 §

[98] Lag (2003:389) om elektronisk kommunikation 6 kap 22 § p 3

[99] Se exempelvis Computer Swedens sammanställning av den svenska sjukvårdens IT-haverier och systemfel under 2008. Se http://computersweden.idg.se/2.2683/1.213345/ett-ar-av-haverier-och-it-problem

[100] Rose-Mharie Åhlfeldt, *Information Security in Distributed Healthcare,* Stockholms University & University of Skövde, 2008.

Media har även rapporterat om brister som uppdagats i samband med penetrationstester av landstingens säkerhetssystem. Vid ett fall gick det att komma åt recepthanteringssystemet från Apoteket AB, vilket i praktiken innebär att man hade kunnat skriva ut recept. [101]

I avhandlingen om informationssäkerhet inom vårdsektorn uppmärksammas en rad behov av åtgärder. När det gäller den tekniska säkerheten är det av stor vikt att se över och förbättra hur man hanterar verifiering, auktorisering och signering. Även verktygen för logghantering, den öppna åtkomsten och integreringsproblem mellan olika system och frånvaron av kryptering för känslig information behöver diskuteras. Inom den administrativa säkerheten består problemen främst av avsaknad av styrande juridiska och organisatoriska dokument gällande hur man ska hantera information och tydliga arbetsrutiner för detta. Genom att skapa policies för informationssäkerhet och IT-strategier, utbilda personal och göra risk- och sårbarhetsanalyser kan man lyfta frågorna och tillgodose behoven.[102]

6.2.8 Brottsbekämpning

6.2.8.1 Bakgrund

IT-relaterad brottslighet[103] utgör idag ett allvarligt hot mot samhällets verksamheter. Nationell brottsbekämpning står inför en rad utmaningar, särskilt med tanke på att den ska motverka och hantera brottslighet som är global och gränslös. Kännetecknande för IT-relaterad brottslighet är att den kan begås i stor skala och att det geografiska avståndet mellan den brottsliga handlingen och dess följdverkningar kan vara stort.

Brister i länders nationella IT-relaterade brottsbekämpning och lagstiftning utnyttjas av den organiserade brottsligheten. Till skillnad från brottsbekämpande myndigheter, är de som begår IT-relaterad brottslighet inte bundna av juridiska och geografiska gränser. För att skapa funktionella och effektiva internationella regelverk och konventioner krävs det att enskilda stater använder likalydande brottsbeskrivningar.

De åtgärder som krävs för att effektivt förhindra dessa brott och ge nationer möjligheter att kunna lagföra dem måste utgå från ett synsätt som är

---

[101] *Hälsosam teknik, it i vården*, http://itivarden.idg.se/2.2898/1.212950/latt-att-hacka-sig-in-i-landstingsnat

[102] Rose-Mharie Åhlstedt, 2008, s 62.

[103] Enligt Kommissionen, KOM/2007/0267 avser begreppet IT-relaterad brottslighet tre olika kategorier av brottslig verksamhet. Den första omfattar traditionella brottsformer som bedrägeri eller förfalskning, som i detta sammanhang begås med hjälp av elektroniska kommunikationsnät eller informationssystem (nedan kallade ”elektroniska nät”). Den andra kategorin rör offentliggörande av olagligt innehåll via elektroniska medier (t.ex. barnpornografiskt material eller hets mot folkgrupp). Till den tredje kategorin hör brott som uteslutande riktas mot elektroniska nät, dvs. angrepp mot informationssystem, överbelastningsattacker och olaga intrång i informationssystem (s.k. hackning). Gemensamt för alla dessa brottskategorier är att de kan begås i stor skala och att det geografiska avståndet mellan den brottsliga handlingen och dess följdverkningar kan vara stort.

internationellt och gränsöverskridande. Internationella överenskommelser, som Europarådets IT-brottkonvention[104], är inte mer allomfattande än de stater som ratificerat[105] konventionen. [106] Även inom EU har behovet av internationella insatser på området identifierats och kommissionen har 2007 tagit ett allmänpolitiskt initiativ för att förbättra samordningen på europeisk och internationell nivå när det gäller kampen mot IT-relaterad brottslighet.[107]

Målen för EU:s initiativ är:

- att förbättra och underlätta samordningen och samarbetet mellan de myndigheter som bekämpar IT-relaterad brottslighet, andra berörda myndigheter och andra experter i EU.
- att i samordning med medlemsstaterna, berörda EU-organ, internationella organisationer och andra berörda parter utveckla en konsekvent politisk ram för EU i kampen mot IT-relaterad brottslighet.
- att öka medvetenheten om de kostnader och risker som IT-relaterad brottslighet medför.

Internationella experter[108] pekar på tre slutsatser som inverkar negativt på brottsbekämpningen:

- stater tar inte IT-brottsligheten på allvar,
- det gränsöverskridande arbetet prioriteras inte tillräckligt av nationella stater, och
- kompetensen hos de brottsbekämpande myndigheterna ligger på en för låg nivå för att kunna hantera brottsligheten.

Vi har valt att fokusera på behovet av en internationellt harmoniserad lagstiftning, folkrätt och informationsoperationer, ett gränsöverskridande juridiskt och polisiärt samarbete, kompetenshöjande IT-utbildning för brottsbekämpande myndigheter samt mörkertalet gällande anmälan av IT-relaterade brott

6.2.8.2 Lagstiftning

För att skapa funktionella och effektiva internationella regelverk och konventioner krävs det att enskilda stater använder likalydande

---

[104] Europarådets konvention
http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[105] Ett beslut av en lagstiftande församling att godkänna ett avtal eller ett fördrag och används ofta om godkännande av internationella avtal och konventioner.

[106] Försvarshögskolan, Nina Wilhelmsson *Folkrättsliga aspekter på cyberhot och skydd mot informationsoperationer.*2008, s 14

[107] KOM(2007) 267 Meddelande från kommissionen till Europaparlamentet, Rådet och Europeiska Unionens Regionkommitté, Att införa en allmän politik för kampen mot IT-relaterad brottslighet

[108] Sammanställning återfinns i McAfee, *Criminology Report,* 2008

brottsbeskrivningar. Bristande harmonisering skapar svårigheter när det gäller möjligheterna till utlämning, åtal och jurisdiktion mellan stater.

Europarådets IT-brottskonvention (Convention on Cybercrime) från 2001 omfattar straffprocessuella regler och ett system för internationellt samarbete för de stater som ratificerat konventionen. 46 stater, både i och utanför Europa, har skrivit under konventionen men endast 23 har än så länge ratificerat den.[109] Sverige hör till de länder som ännu inte ratificerat konventionen. Ett effektivt internationellt samarbete underlättas av ett gemensamt regelverk och det faktum att så många länder fortfarande inte har ratificerat IT-brottskonventionen gör att den inte får full genomslagskraft.

IT-brottskonventionen kritiseras av vissa som en alltför teknikberoende konvention. Numera vanliga IT-relaterade brott som nätfiske och identitetsstölder existerade inte då konventionen arbetades fram vilket innebär att ingen vägledning finns i konventionen för att bekämpa och samarbeta mot dessa typer av brott.[110] Svårigheten med att formulera teknikberoende lagar är att de ofta snabbt blir inaktuella och omoderna, vilket ställer krav på lagstiftarna att skriva lagar som är mer fristående från tekniska specifikationer. Sådan teknikoberoende lagstiftning riskerar dock istället att bli generellt hållen och på det sättet ge mindre vägledning till hur en viss situation ska hanteras i det enskilda fallet. Sammantaget visar detta på ett komplext problem.

6.2.8.3 Folkrätt och informationsoperationer

Betraktar man informationsoperationer ur ett rättsligt perspektiv är FN-stadgan från 1945 om internationell fred och säkerhet och folkrätten av särskilt intresse.[111] Folkrätten reglerar förhållandet mellan stater och bland annat rätten att föra krig. Det generella våldsförbudet gör att en stat endast får tillgripa självförsvar vid väpnat angrepp eller om våldsanvändningen bemyndigats från FN:s säkerhetsråd. Skulle endera av dessa kriterier vara uppfyllt krävs det fortfarande att en motåtgärd (motattack) bedöms som nödvändig, är proportionell och sker omedelbart. Vad gäller rätten i krig regleras den av den humanitära rätten vilken förbjuder riktade angrepp mot civila mål (t ex. informationsinfrastruktur för el- och vattenförsörjning) enligt distinktionsprincipen.[112]

Problem uppstår när man omdefinierar välbeprövade begrepp som väpnat angrepp och traditionella vapen.[113] *”The speed and technical complexity of*

---

[109] Se http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=7&DF=2/27/2009&CL=ENG

[110] McAfee *Virtual Criminal Report 2008*, s 20.

[111] Rättsregler mellan stater och organisationer. När internationell sedvänja (staters gemensamma handlingssätt – praxis) följs av staters rättsövertygelse att gällande rätt återspeglas av sedvanan, talar man om allmän folkrätt eller sedvanerätt.

[112] Nina Wilhelmsson, s 13.

[113] Nina Wilhelmsson, s 7

cyber activities requires prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks."[114] Den tekniska utvecklingen ställer nya krav på konventioner inom de folkrättsliga ramarna, särskilt när det gäller principen att skydda den civila befolkningen vid väpnad konflikt samt arbetet med att begränsa metoderna för krigsföring.[115] Till skillnad från traditionell krigsföring ger IT en mindre grupp eller till och med en enskild person möjlighet att angripa en stat. FN-stadgan och folkrätten är endast tillämpbara i de fall en stat står bakom informationsoperationer.

Ur ett juridiskt perspektiv hamnar därför informationsoperationerna mot Georgien och Estland i en gråzon. Bristen på en uppenbar angripare samt det faktum att attackerna inte orsakade något påtagligt mänskligt lidande gör att det inte går att använda det internationella regelverket för väpnade konflikter[116] för att komma åt förövarna. Den folkrättsliga suveränitetsprincipen försvårar således för ett land som utsatts för cyberattacker att följa upp elektroniska spår utom landets gränser då folkrätten baseras på staters och organisationers förhållningssätt gentemot varandra.[117]

Estlands president efterfrågade i ett tal för FN:s generalförsamling september 2007 en gemensam FN-konvention mot cyberkrigföring och cyberterrorism. Inom NATO pågår även en debatt om att ge informationsoperationer samma status som angrepp mot ett lands sjö-, luft- eller landgräns enligt artikel 5 i Nordatlantiska pakten[118] vilken förpliktar NATO-länderna till samarbete och ömsesidigt bistånd i en situation där ett eller flera medlemsländer utsätts för anfall. Diskussioner inom NATO pekar dock på att ett sådant samarbete inte är troligt med tanke på svårigheten att bedöma var en cyberattack har sitt ursprung.

6.2.8.4 Gränsöverskridande samarbete

Risken med att inte ha ett välfungerande gränsöverskridande samarbete är att omfattningen och systematiken bakom IT-brottsligheten inte uppmärksammas. Nationell polis kan sällan på egen hand genomföra en heltäckande utredning av IT-relaterade brott. Svårigheter med att få rättshjälp från vissa länder innebär i praktiken att bedrägerier måste hanteras inom Sverige trots att såväl servrar som aktörer kan befinna sig på andra platser i världen. Följden blir en jakt på målvakter[119] utan större möjlighet att nå organisatörerna eller kartlägga systematiken bakom brottsligheten.

Polisen har även svårt att få en nationell helhetsbild av den IT-relaterade brottsligheten. Anledningen är att det är svårt att samordna de lokala

---

[114] Sofaer, Abraham D. & Goodman, Seymor E. et al. (2000) "*A proposal for International Convention on Cyber Crime and Terrorism*", CISAC Report, August 2000.

[115] Nina Wilhelmsson, s 7

[116] Law of Armed Conflict, (LOAC)

[117] Nina Wilhelmsson, s 12.

[118] http://www.NATO.int/docu/basictxt/treaty.htm

[119] Se avsnitt 5.3.1

polismyndigheternas information om olika fall. Man riskerar därför att missa omfattning och systematik bakom viss kriminalitet.[120] I syfte att ta ett samlat grepp om IT-relaterad brottslighet måste man därför hantera den organisatoriska strukturen med självständiga länspolismyndigheter.[121] Det finns exempel där banker uppmärksammat polisen på att det finns gemensamma mönster bakom brott i olika delar av landet varpå polisen då samordnat utredningarna av dessa brott på en polismyndighet, vilket har gett positiva resultat.

6.2.8.5 Utbildning

Vid skydd mot IT-relaterad brottslighet är kunskap om området av stor betydelse. IT som medel och mål i kriminell verksamhet är ett relativt nytt fenomen som följt den allmänna teknikutvecklingen.

Källor pekar på att de största kunskapsluckorna inom rättsväsendet återfinns inom domstolarna och bland försvarsadvokater.[122] Särskild uppmärksamhet har riktats mot hanteringen av IT-relaterad bevisning.[123] En ökad specialisering på de juridiskt/tekniskt/ekonomiskt komplicerade måltyperna skulle med största säkerhet leda till fördjupade kunskaper hos domarna inom det aktuella rättsområdet och därmed till ökad kvalitet i rättsutövandet. Det skulle troligen också leda till ökad effektivitet vilket i sin tur skulle leda till snabbare avgöranden i domstol i dessa typer av mål. En specialisering inom juridiskt/tekniskt/ekonomiskt komplicerade måltyper skulle därför leda till att medborgarnas krav på kvalitet och snabbhet i den dömande verksamheten bättre kan tillgodoses.[124]

I utredningen ”Framtidens polis” redovisas en framtidsanalys av BRÅ avseende organiserad brottslighet där man har identifierat ett antal trender som kan antas ha betydelse för samhällsutvecklingen och polisverksamheten. En trend anses vara en ökning av nya brott på grund av den tekniska utvecklingen.[125] En annan trend kommer att vara ett tydligare krav på specialisering och på poliser med särskild kompetens.

---

[120] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 67.

[121] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?,* 2008, s 29.

[122] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?,* 2008, s 53.

[123] Exempelvis ADBJ-seminarium den 16 oktober 2008 http://www.adbj.se/adbjweb/events.php?op=read&id=96

[124] Domstolsverket, *En förstudie i samarbete med Sveriges Domareförbund.* DV-rapport 2003:3, s 30.

[125] SOU 2007:39, *Framtidens polis,* s 101.

6.2.8.6 Mörkertal

Benägenheten att polisanmäla IT-relaterade brott är låg, vilket innebär att brottsbekämpande myndigheter har svårt att få kännedom om den IT-relaterade brottslighetens omfattning och karaktär. Få anmälningar innebär också svårigheter att lyfta fram behovet av resurser för brottsbekämpning.[126]

Det förekommer att verksamheter hanterar händelser internt som tekniska problem medan de i själva verket blivit utsatta för IT-relaterad brottslighet. Säkerhetsarbete och brottsbekämpning inom IT-området är ett område där privata företag tar ett ovanligt stort utrymme och ansvar. En problematik som uppkommer ur denna rollfördelning är att gränserna mellan brott och incident blir otydlig och att de formella brottsbekämparna förlorar överblicken på den IT-relaterade kriminaliteten. Vissa typer av brottslighet, t ex utpressning, hanteras enbart av IT-säkerhetsföretag och kommer oftast inte till polisens kännedom.[127]

Det finns en motvilja att anmäla IT-relaterade brott hos företag och organisationer som blivit utsatta. Flera förklaringar finns, bl a att företagen är rädda för ofördelaktig publicitet, att de klandrar sig själva för bristande säkerhet och att de vill undvika förtroendeskador för sitt företag eller organisation. En bidragande orsak är även upplevelsen av att polisen saknar resurser och kapacitet att utreda brotten. Utredningarna drar ut på tiden och slutresultatet upplevs ofta som magert.

Rädsla och hot om repressalier figurerar också som skäl att avvakta eller helt avstå från att polisanmäla. Rädsla för repressalier är en ovanlig anledning till att avstå från att polisanmäla brott och påminner om reaktionen hos brottsoffer och vittnen som utsatts för eller bevittnat brott begångna av organiserad brottslighet.[128]

6.3 Organisation och individnivå

6.3.1 Mobila enheter

Tack vare en snabb utveckling kan mobiltelefoner, USB-minnen, MP3-spelare och bärbara hårddiskar idag hantera en stor mängd information och, särskilt i fallet med mobiltelefoner med operativsystem, erbjuda en rad tjänster som tidigare krävt tillgång till datorer. Ökat antal användningsområden och kapacitet är inte bara ett stöd i verksamheten utan förutsätter även en rad överväganden när det gäller säkerhet.

---

[126] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 57.

[127] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 52.

[128] BRÅ/KBM, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008, s 59.

Verksamhetens *interna hantering* av mobila enheter uppvisar i många fall brister. USB-portar är vanligen inte blockerade vilket gör det enkelt att ansluta ett USB-minne med skadlig kod till organisationens datorer och nätverk. USB-minnen och bärbara hårddiskar är dessutom både portabla och har stor kapacitet vilket gör det enkelt att stjäla stora mängder information. Bärbara datorer utgör även de en säkerhetsrisk då dessa ofta saknar hårddiskkryptering och är lätta att stjäla. Dessutom går utvecklingen mot att föra över alltfler tjänster och information till mobiltelefoner[129] och andra mobila enheter som Personal Digital Assistant, PDA, vilket ställer höga krav på säkerhetsöverväganden.

När det gäller *yttre hot* pekar internationella studier på ökade risker för att mobiltelefoner kommer att utsättas för SMS-spam, virus och botnätattacker under 2009.[130] Särskilt ökad användning av mobiltelefoner för finansiella tjänster bidrar till att attackerna kommer att bli mer riktade och frekventa. Den ökade användningen och förändrade hotbilden mot mobila enheter gör att det är av stor vikt att säkerställa att även dessa omfattas av organisationens säkerhetspolicy och säkerhetskultur. Det finns idag ofta brister hos organisationerna när det gäller hantering av mobila enheter.[131]

Användningen av mobilt bredband växer. Den tekniska säkerheten i elektroniska kommunikationssystem i mobilt bredband är förhållandevis goda. Det finns idag inget känt eller förutsett sätt att kringå säkerheten (knäcka krypteringen) i 3G näten (UMTS) och säkerheten i 2G näten (GSM) är så pass hög att det krävs dyr utrustning och kompetens för att angripa dessa nät.[132]

6.3.2 Trådlösa nätverk (WLAN)

Förekomsten av oskyddade trådlösa nätverk (WLAN), det vill säga med okrypterad trafik, har länge betraktats som en potentiell säkerhetsbrist.[133] Det finns främst två hot som riktar sig mot trådlös kommunikation; avlyssning av trafik och obehörig åtkomst till det trådlösa nätverket.[134]

Allt fler användare sköter bankärenden[135], handlar och säljer varor och tjänster, sköter privata ärenden som rör barn, skola och sjukvård via sitt hemmanätverk. Dessutom är ett okänt antal människor som åtminstone i viss

[129] Särskilt s k smart phones

[130] Se till exempel Georgia Tech Information Security Center, *Emerging Cyber Threats Report for 2009*, http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

[131] http://www.atea.se/default.asp?ml=6796&naar=&p=5141

[132] PTS rapport Säkrare trådlös kommunikation (utkommer i april 2009)

[133] Det bör nämnas att även okrypterade WLAN ofta har skydd i form av inloggning och andra åtgärder. Hur effektivt skyddet är beror på åtgärderna och hotbild.

[134] Regelförändringarna baserade på IPRED direktivet kan förändra hotbilden när det gäller att utnyttja oskyddade WLAN. Se vidare 4.8

[135] Dessa sker dock i regel över krypterade förbindelser och är därmed väl skyddade mot avlyssning.

utsträckning arbetar hemifrån[136], anslutna via ett trådlöst nätverk. Förekomsten av oskyddade nät innebär att en mängd känsliga uppgifter kan förhållandevis enkelt avlyssnas. Eftersom utvecklingen går mot ökad användning av Internet för en rad olika tjänster utgör oskyddade trådlösa nätverk en risk.[137] En av de största riskerna består i att utomstående kan bereda sig tillgång till det trådlösa nätverket och utnyttja det för kriminella ändamål, exempelvis stjäla information, avlyssna inloggningsuppgifter och ladda ned olagligt material.[138]

Under hösten 2008 lät KBM utföra en undersökning med syfte att få en närmare inblick i antalet trådlösa nätverk och förekomsten av kryptering. Mätresultaten visar att majoriteten privata nät är krypterade men många är fortfarande oskyddade. På de tre orter där mätningar gjordes[139] konstaterades att kryptering inte var påslagen i cirka 26 procent av de trådlösa näten. Att döma av nätens namn rör det sig i många fall av nät som ägs av hotell- och konferensanläggningar samt universitet. Precis som vid hemarbete kan man anta att trådlösa nät på hotell- och konferensanläggningar i betydande omfattning används för att hantera företags- eller myndighetsinformation som kan vara av känslig karaktär. Det finns olika lösningar för att via en bärbar klient sätta upp olika former av kommunikationskrypto, använder krypterad e-post etc. De flesta VPN-lösningar som finns tillgängliga på marknaden ger ett bra skydd för den typen av kommunikation. Säkerhetsmedvetandet är av stor vikt men det finns brister hos användarna.[140]

Som skydd mot avlyssning kan användning av krypteringsprotokollet WPA2 vara en förhållandevis bra lösning som torde vara tillräcklig för en genomsnittlig hemanvändare där användandet sker i ett privat syfte. Vid kryptering används dock fortfarande krypteringsprotokollet WEP i viss utsträckning. WEP kan inte idag anses ge ett sådant skydd och finns sedan ett par år inte med i ny utrustning. Det är viktigt att vara medveten om begränsningarna i krypteringsskyddet, användning av exempelvis WEP kan invagga användaren i en falsk tro att han eller hon är säker.

Bluetooth är en annan trådlös lösning som även den belastas av säkerhetsbrister. Tekniken är billig och implementeringen komplex vilket ger gott om utrymme för angripare att experimentera sig fram till olika typer av

[136] Även här brukar företagen tillhandahålla lösningar (olika VPN-lösningar) med tillfredställande säkerhet

[137] PTS har tagit fram en rapport om säkerhet i lokala trådlösa nätverk med råd till användare (PTS-ER-2007:16) Se även PTS rapport Säkrare trådlös kommunikation (utkommer i april 2009)

[138] Den förändrade lagstiftningen när det gäller utredning av misstänkt olaglig nedladdning av upphovsrättsskyddat material kan förändra hotbilden och skapa ett ökat incitament att använda någon annans oskyddade nätverk för att ladda ned material. Se kapitel 4.8

[139] Stockholm, Göteborg och Malmö

[140] PTS-ER-2007:16 s 29

attacker. Eftersom bluetooth-tekniken nu börjar användas i allt mer känslig utrustning, exempelvis inom hälso- och sjukvården, får sårbarheterna allt större betydelse. Trådlösa nätverk är jämfört med bluetooth något säkrare men eftersom WLAN generellt sett används i en mer kritisk miljö är det allvarligare. Både när det gäller bluetooth och WLAN finns det sätt att skydda kommunikationen men det krävs erfarenhet och kunskap för att göra det på rätt sätt.

6.3.3 Radio Frequency Identification (RFID)

Tekniken används inom allt fler områden som exempelvis svenska passhandlingar, lagervaror, medicinska förpackningar, inpasseringssystem, kollektivtrafik med mera.

Under 2008 redovisade flera forskarlag nedslående säkerhetsbrister i den Mifare-krets som RFID stöder. Kretsen används i en stor mängd kort och nycklar runt om i världen. Det visade sig bland annat att det var möjligt att med hjälp av trådlösa avläsare kopiera korten utan att ha tillgång dessa rent fysiskt. En stor satsning på ett nytt nationellt biljettsystem inom kollektivtrafiken i Nederländerna sköts på framtiden i väntan på att dessa svagheter skulle kunna hanteras.

Med hjälp av RFID går det att hämta information om en specifik produkt och spåra var den befinner sig geografiskt. Ur integritetssynpunkt och samhällsperspektiv finns det därför många aspekter som bör uppmärksammas. Tekniken är relativt billig och det finns en mängd användningsmöjligheter. Som ovan nämnts finns brister i tekniken och det är ytterst viktigt att säkerhetsfrågan på detta område lyfts.

6.3.4 Webbplatser

Sårbarheter i webbapplikationer utnyttjas allt oftare av angripare med olika syften och attackerna har fått stor uppmärksamhet de senaste åren. SQL-injektioner började uppmärksammas i slutet av 2007 och under 2008 noterades ett stort antal attacker av detta slag. SQL-injektioner riktar sig vanligtvis mot databaser eller databasservrar och möjliggörs oftast genom att webbutvecklaren har slarvat med att kontrollera vilka data som användaren kan skicka via formulär eller webbadressfält. Det bakomliggande problemet bottnar många gånger i att det finns en brist på processer och styrning. Många webbplatser har börjat i liten skala och sedan expanderat snabbt med fler användare och nya funktioner. I och med att webbplatsen från början inte byggts för ett sådant bruk, hamnar säkerhetsfrågorna lätt i andra hand. I flera fall är det troligen också okunskap om hot, sårbarheter och tillgängliga säkerhetsåtgärder som ligger bakom blottorna. Det görs inga säkerhetstester och säkerhetsanalyser utan fokus riktas istället mot användarvänlighet och funktion.

Om de som bygger och förvaltar webbplatsen är för få till antalet i förhållande till antalet användare, exempelvis för att webbplatsen snabbt ökat i popularitet, kan säkerhetsarbetet bli eftersatt. Genom angreppssätt som exempelvis drive by *downloads, remote file inclusion* och *cross-site-scripting* kan angripare orsaka skada, som exempelvis stjäla lösenord eller ändra innehåll. Det är av

särskilt intresse att utnyttja säkerhetsbrister i populära webbplatser med många besökare.

Det är viktigt att användare kan lita på webbinnehåll samt att känslig information, exempelvis lösenord, skyddas. I de fall som uppmärksammats under 2008 där användarnamn och lösenord har stulits har konsekvenserna förvärrats genom att många använt samma lösenord på flera olika webbplatser.[141] Genom ett enda stulet användarnamn och tillhörande lösenord har angriparen kunnat komma åt flera personliga webbplatser. Det finns lösningar för att motverka detta, som till exempel OpenID, men fortfarande en viss tveksamhet vad gäller säkerhet vilket påverkar förtroendet för dessa lösningar.

Det är också vanligt att skadlig programvara utformas för att likna antivirusprogram. De skadliga programmens webbsidor är då uppbyggda så att de påminner om antivirusföretagens webbsidor. Genom att ge intryck av att det handlar om ett säkerhetsprogram kan det många gånger vara enklare för en angripare att få offret att själv installera skadliga program, än för angriparen att försöka utnyttja webbplatsernas sårbarheter. I vissa bloggar och sociala nätverk är det tillåtet att lägga in kod. Detta skapar möjlighet att sprida skadlig kod som virus och trojaner till andra användare vilket i sin tur kan minska förtroendet för den här typen av tjänster.

6.3.5 Tid

Utöver organisationer som tillhandahåller kommunikationsnät- och kommunikationstjänster är en rad samhällsviktiga verksamheter och tjänster beroende av tillgång till spårbar tid. Nämnas kan Riksbanken, Banverket, Rakelsystemet, Luftfartsverket, Transportstyrelsen med flera. I dag finns flera alternativ att hämta tid, till exempel genom satellitnätverket Global Positioning System (GPS) och Network Time Protocol (NTP)- servrar som är tillgängliga via Internet och TV.

I ett kommunikationssamhälle där hundratusentals system kommunicerar med varandra är det väsentligt att tidsskalan är entydigt definierad och graden av korrekthet och robusthet bestämd. Om inte dessa frågor hanterats kommer man till exempel vid incidentutredningar att behöva ägna orimligt mycket tid och kostnader för att rekonstruera händelsekedjor. En av de allvarligaste bristerna med osynkroniserade system är att loggdata kan bli missvisande. Detta kan exempelvis leda till att dataintrång blir svåra att följa upp samt att banktransaktioner förlorar i spårbarhet.

Inom ramen för lägesbedömningen studerades hur korrekt och spårbar tid används inom organisationer som bedriver samhällskritisk verksamhet. Medvetenheten om vilken källa för tid som används varierar i organisationerna, men hos de organisationer vars verksamhet har påverkan på

[141] Så var fallet vid exempelvis dataintrånget hos Dataföreningen i februari 2008 då inloggningsuppgifter stals för 26 000 medlemmar.

kritiska samhällsfunktioner har goda kunskaper om detta. Det finns en hög tilltro till GPS-baserad teknik som källa för tid. Vissa organisationer använder GPS som enda tidskälla vilket kan anses vara olämpligt då denna källa är relativt störningskänslig samt kontrolleras av annan stat än Sverige. Generellt sett ökar sårbarheten när tid endast hämtas från en enda källa oavsett om det är GPS eller NTP.

En allvarlig brist hos flera av organisationerna är att man inte vet var de NTP servrar som används som primärkälla för den egna tiden är lokaliserade. Medvetenheten om att det finns nationella NTP servrar som garanterar hög kvalitet på tidsdata hos exempelvis Sveriges Tekniska Forskningsinstitut (SP)[142] borde vara högre än vad den är idag. En NTP-server som tillhandahålls av en okänd operatör någonstans på Internet kan brista i robusthet, korrekthet och tillgänglighet. Det är upp till var och en av tidsserveroperatörerna att svara för dessa egenskaper, vilket kan innebära att tillgänglighet och kvalitet kan variera. Om de samhällsviktiga verksamheterna i Sverige däremot nyttjar flera kända och stabila nationella källor ökar sannolikheten att kvaliteten, framförallt gentemot samverkande verksamheter, bibehålls eller ökas. Nyare versioner av NTP-protokollet erbjuder dessutom kryptografiska funktioner som skulle kunna tillföra verksamheten tidsdata med betydligt högre riktighet och spårbarhet än den som oftast används idag.[143]

Det finns en brist i hur uttalade policies och riktlinjer för tid ska hanteras men uppfattningen är ändå att dessa frågor ofta ingår i organisationens policy/regelverk för det övriga IT-säkerhetsarbetet. Revisioner av vilken loggdata som är mest betydelsefull att samla in samt återkommande analyser av hur verksamheten bäst säkerställer sin tillgång på tid samt synkronisering av tid mellan olika system görs i dag endast av de mest tidskritiska organisationerna. När det gäller tid bör både beroendet av störningskänsliga tidskällor och bristen på signerade tidskällor i form av signerade NTP-servrar beaktas av de aktörer som bedriver samhällsviktig verksamhet.

6.3.6 Domain Name System (DNS) och Border Gateway Protocol (BGP)

Domain Name System (DNS) är en distribuerad databas som är tillgänglig med hjälp av ett globalt hierarkiskt nätverk av DNS-servrar. DNS används till att hitta information om tilldelade domännamn på Internet. Den översätter IP-nummer till domännamn och vice versa. Internet är idag beroende av fungerande DNS. Det finns ett antal säkerhetsrisker med DNS, exempelvis finns möjlighet för en angripare att manipulera svar på DNS-frågor för att på så sätt styra över trafik från en webbplats till sin egen.[144] Säkerheten kan ökas

[142] http://www.sp.se/

[143] NTP autokey, för mer info se exempelvis http://www.ntp.org

[144] Detta kan ske i avsikt att lura besökare att tro att de har kommit till sin Internetbank medan de i själva verket är omdirigerade till en falsk sida. Lämnar besökaren uppgift om användarnamn och lösenord kan på den falska sidan kan dessa uppgifter under vissa

genom att webbplatsinnehavaren använder sig av tjänsten DNS Security Extensions (DNSSEC). Detta innebär att webbplatsinnehavaren med hjälp av en elektronisk signatur ger besökare möjlighet att kontrollera att de verkligen nått rätt webbplats. Med hjälp av tjänsten går det att upptäcka om adresshänvisningen till exempelvis en viss webbplats har förfalskats.

Border Gateway Protocol (BGP) är ett routingprotokoll som binder samman Internet. Det har visat sig att BGP har allvarliga säkerhetsbrister vilka medför att en angripare utan upptäckt kan övervaka okrypterad Internettrafik var som helst i världen och även modifiera trafiken innan den når sin destination. En så kallad man-in-the-middle-attack demonstrerades av två forskare i augusti 2008. Attacken innebär att den utnyttjar BGP för att lura routrar att vidarebefordra data till en avlyssnares nätverk. Metoden kan användas för företagsspionage, statsspionage eller av underrättelsetjänster som vill avlyssna eller övervaka Internetdata utan samarbete från data- och teleoperatörer.

En händelse som fick stor uppmärksamhet under 2008 var när Pakistan Telecom skulle hindra användare i Pakistan från att komma åt YouTube för att på så sätt undvika att invånarna skulle få tillgång till innehåll som bedömdes som olämpligt av Pakistans regering. Av misstag pekade företaget om trafiken i BGP-routrarna. Detta medförde att många runt om i världen under två timmar inte kom åt YouTube och i stället kom till en sida i Pakistan som var tänkt för medborgarna.

6.3.7 Arkivering

Att data och information lagras på ett sätt som säkerställer behov av konfidentialitet, riktighet och tillgänglighet är av stor vikt. Det finns flera olika bestämmelser som styr hur arkivering ska ske. Riksarkivet har under många år arbetat med säkerhetsfrågorna rörande arkivering och på nationell nivå har arbetet bedrivits via SIS, Swedish Standards Institute.

Lagringen av digital information har under de senaste åren ökat explosionsartat. Som ett exempel kan nämnas att volymen på digitalt lagrad information 2007 var hela 36 gånger större än 1998. Lagringen slukar alltmer av organisationens budget.

Vid digital arkivering bör enhetliga och leverantörsoberoende format och standarder väljas. Ofta saknas en policy för hur information i digital form ska sparas. I stället har man konsekvent investerat i mer lagringsutrymme. Har inte säkerhetskopiorna strukturerats på ett väl genomtänkt sätt kan dock informationen förlora sin sökbarhet vilket gör att den tappar en stor del av sitt värde. Det finns system för e-postarkivering och dokumenthantering, men de uppfattas ofta som krångliga och används inte av användarna. Det är viktigt för

omständigheter användas av angriparen för att skaffa sig åtkomst till besökarens bankkonton.

en organisation att ta fram en policy för vad som ska sparas, varför och hur länge samt ett därtill hörande regelverk.

Vid sidan av de tekniska utmaningarna som arkivering innebär bör även brister när det gäller den rättsliga regleringen uppmärksammas. Tillämplig reglering beskrivs av experter på området som svårtillgänglig, överlappande, ofta föråldrad och dåligt anpassad till ”IT-eran”.[145] Av de två generella lagarna som gäller på området, bokföringslagen[146] och personuppgiftslagen,[147] är det den senare som ger upphov till flest frågor. Bristen på vägledning i form av rättsliga avgöranden gör att det fortfarande finns många oklarheter vad gäller tillämpningen.

6.3.8 Extern tjänstehantering (Outsourcing)

Outsourcingföretagen hanterar allt mer av samhällets informationsmängd och säkerhetsfrågorna som följer med det. De fördelar som nämns är kostnadsbesparingar samt att sårbarheten vid drift och förvaltning i många fall minskar då den tekniska kapaciteten och kompetensen hos leverantörerna är ofta högre än hos beställaren. Till nackdelarna hör beställarens kompetensförsvagning samt att ett beroendeförhållande skapas mellan beställare och leverantör, framförallt på längre sikt. Beroendeförhållandet gör att det är svårt att ta hem en verksamhet som en gång outsourcats. Det är även av grundläggande betydelse att informationen kan skyddas. Leverantören måste få möjlighet att kunna säkerställa kontinuitet i kundens verksamhet såväl som sin egen organisation.

Kundernas kravställning avseende säkerhet i allmänhet och kontinuitetsplanering i synnerhet är mycket varierande. Ett fåtal kunder har väl utvecklade kravspecifikationer med både omfattande och djupa krav. Spridningen är dock mycket stor och generellt är kravställandet svagt. Vissa kunder ställer knappt några krav alls, utan nöjer sig med den grundnivå som leverantörerna tillhandahåller som standard. Kraven på tillgänglighet är det klart viktigaste för de flesta kunderna. Att kravställandet är så pass svagt anses ha två förklaringar:

- Okunnighet eller aningslöshet. Många kunder förefaller ha begränsade kunskaper om kontinuitetsplanering och det saknas vana att göra riskanalyser och riskbedömningar.
- Återhållsamhet med kostnader. De flesta kunder förefaller vara beredda på att ta risker för att hålla nere kostnaderna.

Kunderna har i många fall en övertro på vilken säkerhet som ingår i bastjänsten och avstår därmed från att framföra egna ytterligare krav avseende kontinuitetsplanering. Detta kan också bero på leverantörernas agerande då de dels försöker sälja in mer säkerhet utöver grundutbudet och dels är mycket

[145] Se ex Computer Sweden, *Lagarna för lagring är orimliga,* 2009 01 30, s 10f

[146] Bokföringslag (1976:125)

[147] Personuppgiftslag (1998:204)

angelägna om att framhålla den säkerhet som finns redan i bastjänsten. Detta förfarande kan leda till att kunden avstår från att beställa ytterligare säkerhet.

Upphandling inom offentliga sektorn är lagreglerad och många myndigheter använder priset som enda kriterium vid utvärdering av inkomna offerter. Detta leder till ett dilemma för de leverantörer som ska utforma en offert till en inkommen anbudsförfrågan. Man offererar då ett tjänstepaket som precis uppfyller de minimikrav på säkerhet som angivits i anbudsunderlaget. Detta gör leverantören även om denne anar eller till och med är övertygad om att kunden behöver en bättre säkerhet. Lagen om offentlig upphandling (LOU)[148] kan i vissa fall vara kontraproduktiv vad gäller att gynna säkerhetstänkandet och kvalitetsaspekter hos myndigheterna.

Kontinuitetsplaneringens främsta syfte är att säkerställa att en verksamhet kan bedrivas även om incidenter och störningar inträffar. Här finns stora brister när det gäller outsourcing. De kontinuitetsplaner som trots allt finns fokuserar i allt för hög grad på tekniska lösningar. Samspelet mellan leverantören och verksamheten är oftast bristfällig eller obefintlig. Det är kontakten med denna verksamhet som avgör hur smidigt och säkert kontinuitetsplaneringen kommer att fungera vid en störning. Men sådana kontakter finns sällan, oftast går leverantörens kontakter via kundens IT-personal.

Den allmänna pressen på kostnadseffektivitet gör att anläggningarna blir allt större och ingen leverantör kan hålla sig med en så stor överkapacitet att man klarar ett övertagande av hela driften från en utslagen större anläggning. I dessa lägen tvingas man till prioriteringar där det är avtalen med kunderna som styr. De kunder som köpt reservkapacitet på annan anläggning och de som har dubblerad drift går i första hand.

I samband med mer omfattande störningar av driften eller katastrofer, t ex utslagning av en hel driftanläggning agerar leverantörerna ofta situationsanpassat avseende kundernas inbördes behandlingsordning och prioriteringarna är inget som kunderna underrättas om. Enligt de tumregler som finns är den absolut viktigaste åtgärden att så snabbt som möjligt återställa den egna infrastrukturen, eftersom den utgör basen för återgången till normaldrift. Längst ner på prioritetslistan kommer samhällsviktiga verksamheter såvida dessa inte har betalt för högre service. De flesta leverantörer känner sina kunder och vet vilka verksamheter som är de mest kritiska för dem. Detta innebär att leverantörerna gör prioriteringarna själva, utan egentlig kontakt med kunderna.

[148] Lag (1992:1528) om offentlig upphandling

7 Insatser för ökad säkerhet

7.1 Inledning

För att kunna ge en rättvisande bild av informationssäkerheten i samhället samt analysera utvecklingen är det centralt att ge en redogörelse för det arbete som pågår för att öka säkerheten. Under rubriken insatser för ökad säkerhet har vi samlat en rad exempel på olika åtgärder som vi bedömt främjar eller på annat sätt har påverkat samhällets informationssäkerhetsarbete under 2008 eller början av 2009.[149] Särskild fokus har riktats mot myndighetsinitiativ, reglering, standardisering, internationella initiativ och övning/utbildning. Vi bedömer handlingsplanerna och de internationella initiativen vara av särskild vikt.

7.2 Myndighetsinitiativ

År 2008 kännetecknades av en förhållandevis omfattande aktivitet från myndighetshåll där flera insatser och åtgärder har direkt bäring på informationssäkerhetsområdet. Det är av särskilt intresse att notera att vi under året har fått tre handlingsplaner som behandlar informationssäkerhet ur olika perspektiv, två helt nya samt en som uppdaterats under början av år 2009. Vidare går utvecklingen mot att stärka infrastrukturen framåt genom insatser på både nationell och internationell nivå.

7.2.1 Handlingsplan för samhällets informationssäkerhet

Regeringen har givit MSB i uppdrag att förvalta den nationella handlingsplanen för informationssäkerhet som togs fram 2008. Planen utgår från den nationella strategin för informationssäkerhet och har arbetats fram i samverkan med en rad andra myndigheter och organisationer med centrala uppgifter inom området[150]. MSB ska i slutet av året redovisa vilka åtgärder som myndigheten och andra berörda myndigheter har genomfört utifrån handlingsplanen.[151]

Handlingsplanen består sammantaget av 47 åtgärdsförslag för att höja nivån av informationssäkerhet i samhället, både med ett mer omfattande respektive snävt fokus. Särskilt fyra områden har identifierats som prioriterade.

---

[149] Fokus riktas mot insatser av mer generell karaktär. Vid sidan av detta kan det finnas centrala åtgärder inom olika sakområden, exempelvis energisektorn. Av utrymmesskäl har vi valt att inte redogöra för sådana i denna lägesbedömning.

[150] För närvarande pågår ett arbete inom MSB att lämna förslag på uppdatering av den nationella strategin utifrån den rådande samhällsutvecklingen. Förslaget skall lämnas till regeringen under 2009. Se mer om strategin i kap 2.1

[151] Regleringsbrev för budgetåret 2009 avseende Myndigheten för samhällsskydd och beredskap

- Det behövs ett *förbättrat sektorsövergripande och tvärsektoriellt arbete* för samhällets informationssäkerhet. Heltäckande föreskrifter på informationssäkerhetsområdet bör kunna utformas för att gälla samtliga myndigheter under regeringen. Samtidigt behöver det sektorsvisa ansvaret förtydligas. Vidare behöver det finnas möjligheter att ge ändamålsenliga rekommendationer till övriga delar av samhället.
- Det behöver fastställas en *grundläggande säkerhetsnivå* för samhällets informationssäkerhet. En sådan basnivå är en förutsättning för att kunna säkra de informationstillgångar som blivit alltmer fundamentala för såväl näringsliv som offentlig sektor.
- Samhället måste kunna hantera omfattande IT-relaterade störningar och kriser. En *operativ nationell samordningsfunktion* bör därför inrättas.
- Det finns kompetensbrister inom informationssäkerhetsområdet på alla nivåer i samhället. Den snabba utvecklingen medför också att kompetensbrister hos den enskilde användaren får allt större konsekvenser. Därför läggs flera förslag som tillsammans utgör en bred satsning för att *höja kompetensen* inom området.

Under 2008 påbörjades arbete med en rad åtgärdspunkter. Bland annat inleddes arbetet med att stödja myndigheternas tillämpning av LIS (Ledningssystem för Informationssäkerhet – SS-ISO/IEC 27001 och SS-ISO/IEC 27002) inom projektet grundläggande informationssäkerhet[152] och utbildningssektorn kartlades i syfte att bygga en grund för kompetenshöjande åtgärder. Ytterligare en rad åtgärder är planerade under 2009.

De förslag som lämnas i handlingsplanen avser åtgärder inom informationssäkerhetsområdet och omfattar hela samhället från normaltillstånd till kris. Det handlar om en rad konkreta åtgärder där ett flertal syftar till att minska sårbarheten i hos verksamheter, exempelvis genom att ta fram information och rekommendationer om hur informationssäkerhet bör beaktas i upphandlingar och att ställa krav på att myndigheter redovisar i sin årsredovisning på vilket sätt gällande krav på informationssäkerhet uppfylls. Många åtgärder syftar till att generellt öka kompetens och medvetande om informationssäkerhet och andra på att öka kunskap och samverkan inom ett specifikt utpekat område, exempelvis digitala kontrollsystem. Dessa och övriga åtgärdsförslag har i princip samtliga en direkt inverkan, kort- eller långsiktigt, på hot och sårbarheter/risker som har lyfts fram i lägesbedömningen.

När samtliga 47 åtgärdsförslag är genomförda kommer informationssäkerheten i samhället att vara betydligt bättre än vad förhållandet är idag. Handlingsplanen har ett brett stöd hos centrala aktörer på informationssäkerhetsområdet och stödjer flertalet mål för informationssäkerhetsarbetet som satts upp i den nuvarande strategin för samhällets säkerhetsarbete.

[152] Se nedan avsnitt 7.2.4

7.2.2 Handlingsplan för E-förvaltning

Den vid årsskiftet 2008-2009 nedlagda myndigheten Verva, Verket för förvaltningsutveckling, hade bland annat regeringens uppdrag att leda och samordna statsförvaltningens utvecklingsarbete med säkert informationsutbyte och säker hantering av elektroniska handlingar. Enligt regeringens handlingsplan för e-förvaltning[153] är elektronisk identifiering en viktig faktor för tilliten och dialogen mellan myndigheter, medborgare och företag. Skälet för detta är att det i många ärenden finns ett behov av säker identifiering, krav på underskrift och skydd för den personliga integriteten.

Säkerhetsfrågorna inom den offentliga sektorn har haft en stark koppling till utvecklingen av elektroniska tjänster (e-tjänster) som pågått sedan mitten av 1990-talet. Det har hela tiden funnits ett starkt tryck att utveckla säkra lösningar för elektronisk identifiering och underskrifter. Sedan början av 2000-talet är väl spridda lösningar tillgängliga för identifiering och signering elektroniskt genom Statskontorets och Vervas ramavtalsupphandlingar. Ett antal banker samt TeliaSonera är utgivare och idag använder mer än 1,5 miljoner personer i Sverige sina e-legitimationer för offentliga och privata e-tjänster varje månad.

Användningen av dagens e-legitimationer har på många sätt varit framgångsrik men ändå inte helt problemfri. Upplevda problem har främst varit inriktade på försörjningsmodellen och användningen. Utgivarnas koncept har medfört vissa svårigheter på grund av teknisk komplexitet och tillämpade prismodeller har upplevts som problematiska.[154] Användningen av e-legitimationer har av vissa upplevts som inflexibla. Alla som behöver har inte kunnat få en e-legitimation, t ex personer under 16 år, inte heller flyktingar utan identitetshandlingar och utan banktillgodohavanden.[155] Under åren har också lösningarnas säkerhet ifrågasatts. Kritik har riktats mot användningen av sk mjuka certifikat (certifikat och krypteringsnycklar lagrade i en datafil) som inte ansetts tillgodose rimliga säkerhetskrav. Säkerheten med de ”mjuka” certifikaten har dock successivt förbättrats av leverantörerna och några incidenter kopplat till sårbarhet med ”mjuka” certifikat är inte kända i detta sammanhang. Det finns dock en brett förankrad uppfattning om att utvecklingen bör gå emot en ökad användning av smarta kort eller lösningar med motsvarande säkerhetsnivå.

I Vervas rapport Elektronisk identifiering och underskrift i Sverige[156] bedömer Verva att en generell och gemensam infrastruktur för e-legitimationer

[153] Handlingsplan för eFörvaltning – Nya grunder för IT-baserad verksamhetsutveckling i offentlig förvaltning, Fi2008/491, regeringsbeslut 2008-01-17

[154] VERVA, *Slutrapport om säkert informationsutbyte och säker hantering av elektroniska handlingar*, 2008:12

[155] Nedmonteringen av svensk kassaservice har inneburit att enskilda nu är hänvisade till att söka identitetshandlingar hos bankerna. Utan några tillgodohavanden och identitetshandlingar har det dock visat sig svårt att få elektronisk legitimation.

[156] Särtryck ur Vervas rapport 2008:12

underlättar för organisationer som erbjuder e-tjänster att tillhandahålla enkla och användbara lösningar. En generell lösning skapar förutsägbarhet för användaren. Förutsägbarhet skapar i sin tur trygghet och tillit. Verva föreslog att regeringen säkerställer att det finns en för Sverige reglerad ordning för e-legitimationer som ger stöd för såväl kvalificerade som avancerade elektroniska signaturer, bland annat ska det nationella ID-kortet kunna användas som bärare av Svensk e-legitimation.

7.2.3 Handlingsplan för internetsäkerhet

PTS är sektorsmyndighet för elektroniska kommunikationer vilket även inbegriper Internet. 2006 fick myndigheten i uppdrag att lämna förslag på en strategi för ett säkrare Internet i Sverige som beslutades av regeringen samma år.

Strategin är inriktad mot de delar av infrastrukturen som är unika för Internet och innehåller förutom strategiska överväganden även en handlingsplan för att nå målen.[157] Visionen är att Internet om tio år är säkert, snabbt och har hög tillgänglighet för alla i Sverige. Handlingsplanen uppdaterades i början av 2009.

Målet för en strategi för ett säkrare Internet i Sverige är att säkra kritiska funktioner i Internets infrastruktur som, om de inte upprätthålls, ger omfattande störningar eller avbrott och på så sätt försvårar eller förhindrar användning av Internet för stora grupper av enskilda användare eller för samhällsviktiga företag, myndigheter och organisationer. Stora delar av infrastrukturen tillhandahålls av privata aktörer. Utgångspunkten för säkerhet i Internets infrastruktur är därför tillhandahållarnas ansvar för nät och tjänster utifrån marknadens krav. Det offentliga åtagandet bygger på att det finns krav som marknaden inte kan tillgodose.

När det gäller Internet identifierade PTS 2006 en rad trender och hotbilder. Årets lägesbedömning ger vid handen att flertalet av dessa kvarstår även idag, två år senare. De strategiska ställningstaganden som trenderna och hoten föranledde 2006 har följaktligen i samband med uppdateringen 2009 endast förändrats marginellt. De utgörs idag av:

- Internets fysiska infrastruktur bör skyddas mot olyckor, störningar, avlyssning och manipulation av information under överföring.
- Motståndskraften mot störningar i domännamnssystemet bör ökas.
- Motståndskraften mot störningar i trafikutbyte mellan Internetoperatörer bör ökas.
- Användare och beställare bör utbildas och informeras för ökat säkerhetsmedvetande.
- Ansvarstagandet för användares säkerhet bör öka hos Internetoperatörer samt tillhandahållare av programvaror och utrustning.

[157] Strategi för ett säkrare Internet i Sverige PTS-ER-2006:12

- Den nationella kunskapsutvecklingen avseende Internets infrastruktur bör främjas. Det bör ske i ett bredare sammanhang rörande informationssäkerhet.
- Det svenska deltagandet i internationella forum bör fördjupas. Detta bör ske i samverkan mellan privat och offentlig sektor.
- Förmågan att hantera kriser relaterade till Internets infrastruktur bör utvecklas.

Handlingsplanen består av ett antal åtgärder som syftar till att uppfylla de strategiska ställningstagandena. Enligt den uppdaterade handlingsplanen avser PTS under den kommande tvåårsperioden att bland annat:

- främja användningen av DNSSEC,
- ta fram rekommendationer om säkrare trafikutbyte mellan Internetoperatörer,
- förbereda införandet av IPv6,
- minska beroendet av störningskänsliga tidskällor,
- arbeta med kompetenshöjning,
- studera förekomsten av botnät i Sverige,
- öka sitt deltagande i internationella organisationer och
- verka för att en europeisk strategi för informationssamhället även innefattar området säkrare Internet.

Ett fungerande och säkert Internet är en avgörande förutsättning för informationshantering inom en rad olika sektorer varför både strategin och handlingsplanen utgör centrala verktyg för samhällets informationssäkerhet, inte minst när det gäller samhällsviktig verksamhet och effektivt utnyttjande av IT.

7.2.4 Grundläggande informationssäkerhet

Ett mål för handlingsplanen för samhällets informationssäkerhet är, liksom strategin för ett säkrare Internet, att bidra till arbetet för att åstadkomma en robust informationsinfrastruktur i samhället och grundläggande nivå för informationssäkerhet.

För närvarande pågår arbete inom MSB och med stöd från andra myndigheter och intressenter med att skapa en rad stöddokument för tillämpningen av ledningssystem för informationssäkerhet. Som ett första steg i syfte att underlätta det interna säkerhetsarbetet har en modell för informationsklassning tagits fram.[158] Ett annat steg är att tillgängliggöra de föreskrifter som Verva tog fram för informationssäkerhet på MSB:s hemsida

[158] Klassningsmodellen kommer att publiceras under våren 2009.

samt påbörja ett internt arbete med att ta fram och ersätta dessa med föreskrifter utfärdade av MSB.

7.2.5 Nationell samverkansfunktion

Erfarenheter från bland annat attackerna mot Estland under våren 2007 visar att IT-baserade störningar och angrepp inte sällan sprider sig över organisationsgränser med hög hastighet. Att ha en förberedd organisation för detta, inte minst vad gäller ansvarsfördelning, är därför av stor vikt. Ett viktigt åtgärdsförslag i handlingsplanen är därför att, utifrån befintliga resurser, skapa en operativ nationell samordningsfunktion med god operativ förmåga under allvarliga störningar och kriser. En sådan funktion skulle även kunna bedriva övningsverksamhet under normaltillstånd. Samövning innebär ett lärande för flera aktörer och kan dessutom ha mycket stor betydelse om normaltillståndet övergår till en krissituation.

Storskaliga IT-relaterade angrepp har som regel ett mycket snabbt händelseförlopp och det ställs därför särskilda krav på att kunna detektera och presentera ett sådant händelseförlopp. Motåtgärderna startar dessutom omedelbart på stor bredd och då av naturliga skäl mindre koordinerade. Det gäller således att snabbt kunna klarlägga läget och att koordinera åtgärderna som vidtas.

Denna lägesbild är dock bara en del av all den information som förekommer i en viss situation. Därför är det viktigt att kunna utväxla information mellan ett flertal berörda aktörer. Det är också viktigt att förstå att information i lägesbilden är olika tidskritiska beroende på vilken typ av angrepp eller företeelse som skall hanteras men kanske den allra viktigaste faktorn är att den eller de som har uppgift och resurser att kunna hantera situationen blir delgiven all relevant information.

Målet med att inrätta en operativ nationell samverkansfunktion är att det ska finnas en effektiv informationsdelning inom informationssäkerhet i samhället i stort, genom vilken berörda parter ska kunna nå en samlad kunskapsnivå och lägesbedömning och nå en operativ förmåga att kunna kommunicera och agera i samband med incidenter och kriser. Detta innebär även att kompetent och övad personal ska finnas tillgänglig i händelse av kris.

Med hänsyn till MSB:s uppdrag är det naturligt att myndigheten har en central roll att upprätthålla en del av en nationell lägesbild. För närvarande pågår arbete att skapa en administrativ och teknisk infrastruktur för informationsdelning och respons i vid mening inom informationssäkerhet i det svenska samhället. Utgångspunkten är att utgå från och ta tillvara nuvarande verksamhet, såsom CERT-verksamheten hos Sitic och befintlig underrättelseverksamhet inom polisen, säkerhetspolisen, försvarsmakten och FRA.

7.2.6 Swedish Government Secure Intranet (SGSI)

Flera av de hot som vi redogjort för i kapitel 5 är kopplade till osäker nätverksmiljö. SGSI är ett krypterat och skyddat myndighetsnät med anslutning till EU:s säkra nät S-TESTA dit enbart en anslutning per

medlemsstat tillåts. Sedan nätet driftsattes 2004 har säkerheten utvecklats vidare. Detta har skett genom en kontinuerlig analys av förekommande hot och risker som sedan ligger till grund för att utveckla säkerhetsprocessen.

SGSI-nätet är utformat för att klara höga krav på tillgänglighet och kan idag erbjuda mycket högre driftsäkerhet och tillgänglighet än t ex internet. Drift och underhåll sköts av personal från Rikspolisstyrelsen, Försvarsmakten och TeliaSonera tillsammans med ackrediterade myndigheternas lokala tekniker. SGSI består i dagsläget av ett tjugotal myndigheter. Samtliga myndigheter uppfyller de säkerhetskrav som gäller för anslutning till nätet. Kommunicerar myndigheter med varandra inom landet bör man överväga anslutning till SGSI för att inte utsätta sig för de risker oskyddade nät kan ge upphov till. Detta gäller exempelvis i den framtida e-förvaltningen då en medborgare ska kunna kontakta en enda myndighet via Internet och där få hela ärendet utfört även om myndigheten måste inhämta en del av informationen från andra myndigheter.

7.2.7 Kryptografiska funktioner

Idag finns nationellt godkända kryptosystem för skydd av elektronisk kommunikation i form av system för kryptering av telefoni i fasta och mobila telenät, telefax och videokonferens samt för att skydda datakommunikation och datafiler. Dessa ska möjliggöra tvärsektoriell samverkan mellan Regeringskansliet, myndigheter och vissa företag finns. De nationellt godkända systemen har säkerhetsgranskats av Försvarsmakten som garanterar att det inte finns inplanterade eller oavsiktliga svagheter i den kryptografiska funktionen. Vissa system granskas även av Försvarets materielverk (CSEC) enligt standarden Common Criteria. Det finns idag nationellt godkända kryptosystem för skydd av sådan information som rör rikets säkerhet och omfattas av sekretess enligt sekretesslagen[159]. Det finns även system som kan nyttjas för att skydda information som omfattas av sekretess som ej rör rikets säkerhet samt för annan känslig myndighetsinformation. Flertalet system kan användas nationellt men även internationellt vid resor eller för informationsutbyte med personal från andra stater, för det senare krävs godkännande av Regeringen samt att erforderliga avtal sluts mellan parterna.

MSB beslutar om vilka civila myndigheter eller andra organisationer som skall tilldelas nationellt godkända kryptosystem. Försvarets radioanstalt, FRA, anskaffar efter samråd med MSB den kryptomateriel som krävs för samhällets skydd och beredskap. FRA stödjer därefter de myndigheter som använder nationellt godkända kryptosystem samt ger den utbildning som behövs för att vara behörig att hantera sådana system.

Den lokala nivån har idag ej tillgång till nationellt godkända kryptosystem. Under år 2009 påbörjas ett arbete med att erbjuda kommunerna nationellt

[159] Sekretesslag (1980:100)

godkända kryptografiska funktioner inom sin verksamhet samt för säkert informationsutbyte med statliga myndigheter.

7.2.8 DNSSEC

Brister i domännamnssystemets uppbyggnad gör det möjligt att felaktigt utge sig för att tillhandahålla en viss webbplats. Detta gör det möjligt att få användare att tro att de nått sin bank och då lura av dem inloggningsuppgifter och koder.

För att skydda sig mot den här typen av attacker är det möjligt att använda DNSSEC, dvs med hjälp av en elektronisk signatur ge användare möjlighet att på ett säkert sätt kontrollera att de verkligen nått rätt webbplats. Med hjälp av tjänsten går det att upptäcka om adresshänvisningen till exempelvis en viss webbplats har förfalskats.

Under 2008 har intresset för den DNSSEC tjänst som .SE erbjuder ökat kraftigt och i november hade 1000 st domäner under .SE signerats. För att ytterligare markera fördelarna med tekniken har PTS som första statliga myndighet signerat sin webbplats.

7.3 Reglering

Skydd av information är en central juridisk uppgift och under det senaste åren har en rad åtgärder och initiativ vidtagits med bäring på informationssäkerhetsområdet. Nedanstående genomgång har inte någon ambition att vara heltäckande utan fokus riktas mot regleringsinsatser som bedömts vara av betydelse för samhällets informationssäkerhet. I år har lagstiftaren ägnat särskild uppmärksamhet mot myndigheter och andra organisationers informationshantering, arbetet att bekämpa brottslighet och terrorism samt skyddet av den personliga integriteten inom hälso- och sjukvård.

7.3.1 Säkrare informationshantering

Den 1 januari 2008 trädde *Vervas föreskrifter om statliga myndigheters arbete med säkert elektroniskt informationsutbyte* i kraft.[160] Syftet med föreskriften är enligt 2 § att skapa förutsättningar för ett säkert och förtroendefullt elektroniskt informationsutbyte genom att myndigheterna bedriver sin verksamhet med den säkerhet som är nödvändig med hänsyn till den enskilda myndighetens förutsättningar. Föreskriften är central för myndigheternas informationssäkerhet på så sätt att den ställer krav på ett metodiskt informationssäkerhetsarbete. Varje myndighet ska tillämpa ett ledningssystem för informationssäkerhet och mot bakgrund av risk- och sårbarhetsanalyser avgöra vilka risker som ska elimineras, reduceras eller accepteras. Föreskriften är en viktig koppling mellan reglering och standardisering då den uttryckligt ställer krav på att arbetet ska bedrivas i former enligt informationssäkerhetsstandarden ISO/IEC 27000. Vid årsskiftet

[160] VERVAFS 2007:2

2008/2009 lades Verva ned. Föreskrifterna är fortfarande i kraft och en undersökning som Verva genomförde visar att majoriteten av de undersökta myndigheterna har infört eller börjat följa föreskrifterna.[161]

Eftersom det finns ett behov av tydliga regelverk och riktlinjer på informationssäkerhetsområdet fick MSB bemyndigande i krisberedskapsförordningen[162] att meddela föreskrifter om informationssäkerhet med beaktande av nationell och internationell standard. Arbetet med föreskrifterna pågår inom myndigheten, när de är klara kommer de att ersätta Vervas föreskrifter om informationssäkerhet.

En viktig förutsättning för att uppnå önskad nivå av informationssäkerhet är att ha ordning och kontroll över sin informationshantering. En viktig del i detta arbete är ett tydligt utpekat ansvar. Riksrevisionen pekade i ett flertal rapporter mellan 2005 och 2007[163] på brister när det gällde myndigheternas interna styrning och kontroll av informationssäkerhet. Detta gällde inte minst ledningens förståelse och arbete med att leda och ta ansvar för informationssäkerhetsarbetet. Sedan den 1 januari 2008 har ledningens ansvar förtydligats i *myndighetsförordningen*.[164] *Förordningen om intern styrning och kontroll*[165] förtydligar ledningens uppgifter samt ställer krav på riskanalys, kontrollåtgärder, uppföljning och dokumentation.[166]

Samtliga ovan nämna regelverk bidrar till effektiv och säker informationshantering hos myndigheter. Det är dock viktigt att se till att arbetet med regelverken samordnas, exempelvis när det gäller krav på riskanalyser.

När det gäller större företag har informationshantering reglerats i allt större utsträckning. Där utgångspunkten har varit att försvåra ekonomisk brottslighet, peka ut ansvar och öka insyn. Ett grundläggande regelverk är det amerikanska lagen *Sarbanes-Oxley, SoX*.[167] Inom EU har motsvarande arbete företrädesvis skett genom de 4:e, 7:e och 8:e bolagsdirektiven[168]. Det

---

[161] VERVA, *69 myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltningen,* 2008:14, s 24

[162] 30a och 34 §§ Förordning (2006:942) om krisberedskap och höjd beredskap

[163] Se exempelvis RiR 2005:26 Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten och RiR 2006:24 Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten

[164] Myndighetsförordning (2007:603)

[165] Förordning (2007:603) om intern styrning och kontroll

[166] Ekonomistyrningsverket får meddela de föreskrifter som behövs för verkställigheten av förordningen.

[167] Sarbanes-Oxley Act of 2002

[168] Rådets fjärde direktiv 78/660/EEG av den 25 juli 1978 om årsbokslut i vissa typer av Bolag, Rådets sjunde direktiv 83/349/EEG av den 13 juni 1983 om sammanställd redovisning, Rådets åttonde direktiv 84/253/EEG av den 10 april 1984 om godkännande av personer som har ansvar för lagstadgad revision av räkenskaper. Det åttonde bolagsdirektivet ersattes av Europaparlamentets och rådets direktiv 2006/43/EG av den 26

sistnämnda har föranlett ändringar i den svenska koden för bolagsstyrning[169], ändringarna trädde ikraft den 1 juli 2008.

En utredning som kan få stor betydelse för säkerhet och informationshantering är Säkerhetskopiors rättsliga ställning (2009:5). Utredningen föreslår att säkerhetskopior ska undantas från grundlagens regler om allmänna handlingar[170].

7.3.2 Förebygga och bekämpa brott

När det gäller möjligheterna till informationsinhämtning för att förebygga och bekämpa brottslighet har en rad förändringar genomförts respektive utretts under 2008. En av de mest omskrivna och omdebatterade lagarna är *lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet*[171]som trädde ikraft den 1 januari 2009. Lagen ger Försvarets radioanstalt (FRA) under vissa villkor möjligheter till spaning i kabel, en utökning jämfört med tidigare begränsning till spaning i etern. Enligt lagens 1 § får FRA inhämta signaler i elektronisk form för underrättelseverksamhet inom ramen för de inriktningar som anges av regeringen eller de myndigheter som regeringen bestämmer. Exempel på sådana myndigheter är Säkerhetspolisen (SÄPO), Rikskriminalpolisen och MSB. Debatten kring lagen rörde främst integritetsfrågor och ledde till att regeringen la fram ett förslag på förändring av lagen där inriktning av signalspaning endast får göras av regeringen, Regeringskansliet och Försvarsmakten, tillståndskravet skärps, särskilt integritetskänslig information som uppfångas ska förstöras och den enskildes tillgång till effektiva rättsmedel förstärks.[172]

Integritetsdebatten spås av en del bedömare åter tillta i samband med att direktivet om lagring av trafikdata för brottsbekämpning[173] ska implementeras i svensk lagstiftning. Lagen ålägger teleoperatörer att lagra trafikuppgifter i ett år. Syftet är att underlätta tillgång till elektronisk bevisning.

Integritetsdebatten har även aktualiserats när det gäller förändringarna i upphovsrättslagen som träder ikraft den 1 april 2009.[174] Den ger upphovsrättsinnehavare som skivbolag, bokförlag och filmbolag under vissa

---

april 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG

[169] http://www.bolagsstyrning.se/files/docs/Svenskkodforbolagsstyrning.pdf

[170] Tryckfrihetsförordning (1949:105) 2 kap 3 §

[171] I media benämndes den ofta ”FRA-lagen”

[172] Ds 2009:1 Förstärkt integritetsskydd vid signalspaning

[173] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG

[174] Se prop 2008/09:67 och Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter.

omständigheter rätt att få ut uppgifter om IP-adresser hos teleoperatörer via domstol. En kritik som riktats mot regelförändringen är att den ger upphovsrättsinnehavarna större möjligheter att få ut den här typen av uppgifter från teleoperatörerna än polisen som i dagsläget är begränsade av regeln i lagen om elektronisk kommunikation[175] att det bland annat skall gälla ett brott för vilket det inte är föreskrivet lindrigare straff än två års fängelse.[176] Begränsningarna vad gäller polisernas möjligheter att få tillgång till den här typen av information har varit föremål för en utredning.[177] En debatt har även inletts rörande det sk IPRED2 direktivet och Anti-Counterfeiting Trade Agreement (ACTA).[178]

7.3.3 Skydd av personlig integritet

Förra året ägnades förändringar i personuppgiftslagen[179] stor uppmärksamhet i media. I år är det av särskilt intresse att lyfta fram den nya patientdatalagen[180] som trädde ikraft 29 maj 2008. Lagen kompletterar personuppgiftslagen och tydliggör vad som gäller för hantering av personuppgifter inom hälso- och sjukvårdsområdet. Det huvudsakliga syftet är att stärka integritetsskyddet. Reglering ska möjliggöra både en ökad patientsäkerhet och ett starkt integritetsskydd. Det blir med den nya lagen möjligt att ha en sammanhållen journalföring vilket betyder att vårdgivare har möjlighet att bygga system där olika vårdgivare kan få åtkomst till patientens information oavsett var han eller hon söker vård. Patienten får också större möjligheter att påverka genom att exempelvis kunna spärra en potentiell elektronisk åtkomst till sin journal för andra enheter inom samma vårdgivare såväl som för andra vårdgivare. Patienten kan också få ökad åtkomst till logguppgifter. Socialstyrelsen har rätt att meddela närmare föreskrifter om säkerhetsåtgärder vid hantering och förvaring av journaler.

---

[175] 6 kap. 22 § första stycket 3 lag (2003:389) om elektronisk kommunikation

[176] Enligt 7 kap 53 § lag (1960:729) om upphovsrätt till litterära och konstnärliga verk ska den som gör sig skyldig till upphovsrättsintrång dömas, om det sker uppsåtligen eller av grov oaktsamhet, till böter eller fängelse i högst två år.

[177] SOU 2009:1 En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen (polismetodutredningen)

[178] IPRED2 direktivet: *Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights* (COM/2006/0168 final - COD 2005/0127) och det internationella avtalet Anti-Counterfeiting Trade Agreement (ACTA), vilket i syfte att bekämpa immaterialrättsintrång kan ge utökade möjligheter att få ut information från nätoperatörer och ge rätt till utökad kontroll vid gränsöverskridning av bärbara medier som datorer.

[179] Personuppgiftslag (1998:204). Förändringarna innebar att lagen i stort gick från att ange vad som är tillåtet till att istället uppge vad som utgör missbruk (handlingsmodell till en missbruksmodell).

[180] Patientdatalag (2008:355)

7.4 Standardisering

Standardisering är vid sidan av reglering ett kraftfullt styrmedel när det gäller säkerhetsarbete. Antalet standarder som har bäring på informationssäkerhetsområdet är stort men vi har valt att belysa utvecklingen inom tre standarder med särskilt central roll. Inom särskilt de två första har Sverige varit en aktiv deltagare i det internationella standardiseringsarbetet.

Den största delen av organiserat standardiseringsarbete sker inom tre olika organisationer, ISO, IEC och ITU. När det gäller IT samarbetar ISO och IEC. Standarder som utvecklas gemensamt benämns alltid med beteckningen ISO/IEC och ett nummer. För att hantera den gemensamma utvecklingen har ISO och IEC bildat en gemensam kommitté kallat Joint Technical Committee 1, JTC 1. Under denna kommitté organiseras sedan subkommittéer med ansvarig för olika områden. SC 27 har ansvaret för all utveckling av standarder inom informationssäkerhetsområdet.[181]

Standardiseringsverksamheten inom informationssäkerhetsområdet kännetecknas av en hög aktivitet med ett stort antal standarder under utveckling. Sverige har under många år deltagit aktivt i arbetet inom SC 27. Standardiseringsverksamheten inom SIS rörande informationssäkerhet är idag samlad i en kommitté, TK 318.

Internationellt inom JTC1/SC 27 finns totalt cirka ett 80-tal standarder utgivna eller under utveckling inom området.

Allt standardiseringsarbete av intresse för informationssäkerhetsområdet sker dock inte inom ISO och IEC. Det finns en stor mängd branschstandarder och de facto standarder som även de är av betydelse.[182]

7.4.1 ISO/IEC 27000 Ledningssystem för informationssäkerhet (LIS)

Standardserien SS-ISO/IEC 27000 Ledningssystem för informationssäkerhet intar en central roll på informationssäkerhetsområdet. Den sätter upp en ram för och stödjer en organisations framtagning av policy och mål samt arbetet med att nå målen. SS-ISO/IEC 27000-serien bildar nu en naturlig mittpunkt för all standardisering inom informationssäkerhetsområdet och där övriga standarder försöker förhålla sig till nämnda serie. Samtidigt kan konstateras att SS-ISO/IEC 27000-serien får allt större genomslag internationellt och nationellt i Sverige.

Under 2008 har 27000-serien utökats med en standard för riskhantering inom informationssäkerhet, SS-ISO/IEC 27005. Arbetet med att revidera de ursprungliga standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 27002 som innehåller uttryckliga krav respektive rekommendationer hur kraven

[181] Det är främst 5 olika working groups som arbetar med standarder.

[182] Som exempel kan nämnas den nedan beskrivna branschstandarden för korthantering PCI DSS och operativsystemet Windows dominerande ställning på marknaden.

implementeras har också påbörjats. Under 2009 planeras 27000-serien utvidgas ytterligare när ISO/IEC 27003 rörande införande av ledningssystem för informationssäkerhet och ISO/IEC 27004 mätning av informationssäkerhet blir färdiga och ges ut.

Under 2009 kommer också en övergripande standard med terminologi och översikt över 27000-serien att ges ut. Denna kommer att heta SS-ISO/IEC 27000 och är historisk i det avseendet att det är den första ISO-standarden någonsin som kommer att kunna publiceras fritt.[183] SS-ISO/IEC 27000 kommer att innehålla definitioner, beskrivningar över processen i LIS samt utgöra en beskrivning av både 27000-serien samt 27030-serien[184].

Inom den svenska offentliga förvaltningen får standardiseringen en allt större roll. Sammanslagningen av KBM, SRV och SPF innebär att den nya myndigheten för samhällsskydd och beredskap, MSB får en allt viktigare och tydligare roll som samordningsansvarig myndighet inom informationssäkerhetsområdet. Krisberedskapsförordningen[185] pekar på att det föreskriftsansvar som åtföljer den nya myndighetens ansvar ska baseras på standarder i området. Vervas föreskrift inom området pekar redan på att statliga myndigheter måste införa ett ledningssystem för informationssäkerhet, LIS, i enlighet med SS-ISO/IEC 27001 och SS-ISO/IEC 27002. För att underlätta arbetet har MSB köpt ut och kommer att distribuera nämnda standarder till myndigheter som omfattas av Vervas föreskrift inom området (statliga myndigheter).

7.4.2 Common Criteria

Common Criteria (CC) är en standard för hur man ställer krav, deklarerar och evaluerar säkerhet i IT-produkter och system i deras användningsmiljöer. CC är ett ramverk för hur man beskriver de funktionella kraven på IT-säkerhet i en produkt eller ett system, inte en samling krav i sig. Inom ramverket klarläggs först kravbilden så att produkten eller systemet sedan ska kunna evalueras i förhållande till denna. CC fokuserar på det behov av informationssäkerhet (konfidentialitet, tillförlitlighet och tillgänglighet) som uppstår på grund av avsiktliga eller oavsiktliga hot.

Inom ramen för Common Criteria Recognition Arrangement (CCRA) bedrivs ett internationellt samarbete för att utveckla CC standarden[186]. För närvarande finns 25 deltagarländer där det senast tillkomna är Pakistan som accepterades som medlem under 2008. Standarden är ett viktigt verktyg i arbetet med säkra produkter. I Sverige är till dags dato 2 produkter certifierade och 4 är under

[183] Kostnaden för standarder varierar. Inköpskostnaden av ett paket med ISO/IEC 27001 och ISO/IEC 27002 brukar ligga på runt 3000 kr.

[184] Den sistnämnda innehåller bl.a. multipartstandarden network security som är under revision. Även andra standarder som bl.a. berör kontinuitetsplanering, incidenthantering, insamling av bevis och cybersecurity återfinns i ISO/IEC 27030-familjen.

[185] 34 § Förordning (2006:942) om krisberedskap och höjd beredskap

[186] http://www.commoncriteriaportal.org

evaluering. Detta kan jämföras med situationen i USA där ett mycket målmedvetet arbete pågår att endast använda CC-certifierade produkter hos statliga myndigheter som hanterar känsligt material.[187]

7.4.3 Payment Card Industry Standard Data Security Standard (PCI DSS)

Stulen kortinformation och kortbedrägerier har utgjort ett problem i många delar av världen och ett bekymmer för kortindustrin. Årets lägesbedömning visar också på att olaglig hantering av personuppgifter snarare ökar än minskar.

I syfte att öka säkerheten kring hantering av kortinformation minimera riskerna för stöld av kortdata har de internationella kortnätverken MasterCard och Visa tagit fram standarden PCI DSS som ursprungligen lanserades 2004 men uppdaterades 2008 till version 1.2. Ett syfte med standarden är att upprätthålla och stärka förtroendet för kort som betalningsmedel.

Alla säljföretag, inlösare och tredje parter som hanterar, lagrar och/eller överför kortinformation måste uppfylla PCI DSS kraven. Säkerhetskraven varierar något beroende på företagets volymer (korttransaktioner), bransch och riskklassificering men rör exempelvis krav på brandvägg, hantering av lösenord, fysisk säkerhet, loggning och säkerhetspolicy. Uppfyller inte ett säljföretag eller inlösare kraven risker denne finansiella förluster och i yttersta fall att förlora rätten att ta emot kort som betalningsmedel.

Standarden med sina säkerhetskrav anses komma att generellt öka säkerheten hos de berörda parterna och i förlängningen öka förtroendet hos kunderna för kortbetalningssystemet.

7.5 Internationella initiativ

Inom informationssäkerhetsarbetet pågår en rad insatser på internationell nivå, vissa av teknisk natur och andra med mer administrativ fokus. Fungerande informationshanteringen är av grundläggande betydelse för det egna samhällets funktioner samtidigt som infrastrukturen informationshanteringen utnyttjar, exempelvis Internet, är internationell. Internationell samverkan är här en nödvändighet för att uppnå tillräcklig säkerhet. I lägesbedömningen har vi valt att särskilt belysa några av insatserna som vidtagits inom EU och FN. Utöver dessa organisationer sker viktigt arbete, särskilt när det gäller Internet i en rad internationella organisationer som ICANN och IETF.

[187] Relevanta regelverk är här FISMA, Federal Information Security Management Act och Policy 11 (National Information Assurance Acquisition Policy (NSTISSP 11)) För mer information se https://buildsecurityin.us-cert.gov/swa/acqart.html

7.5.1 ENISA

Enisa[188] är en EU-myndighet som har till uppgift att stödja medlemsstater, EU-organ och företag i arbetet att hålla en hög och effektiv nivå när det gäller informationssäkerhet. ENISA fungerar även som ett expertcentrum för medlemsstaterna och EU-institutionerna som underlättar informationsutbyte och samarbete. Organisationen samlar och analyserar data om säkerhetsincidenter och risker samt arbetar aktivt med medvetandehöjande åtgärder.

Målen för 2009 är:

- Förbättra robusthet och förmåga till återhämtning i europeiska elektroniska kommunikationsnät
- Utveckla och upprätthålla samarbetet mellan medlemsstater
- Identifiera nya risker inom ny teknik och tjänster

7.5.2 Organisation for economic co-operation and development, OECD

OECD har under flera år ägnat uppmärksamhet åt informationssäkerhetsfrågan. Ett grundläggande dokument i detta sammanhang är organisationens riktlinjer för säkerheten i informationssystem och nät, på väg mot en säkerhetskultur från 2002.[189] Under 2008 har organisationen vid sitt ministermöte i juni 2008 bland annat riktat fokus mot RFID[190] och digitalt material[191]. Organisationen har även givit ut rekommendationer för skyddet av kritiska informationsinfrastrukturer.[192]

7.5.3 Internet Governance Forum, IGF

IGF har som syfte att stödja FN:s generalsekreterare att förverkliga uppgiften från the World Summit on the Information Society (WSIS) att skapa ett nytt forum för policydiskussioner för alla berörda parter när det gäller styrning och utveckling av Internet. Vid det senaste mötet i december 2008 stod arbete med att främja säkerhet och förtroende högt på agendan. Till skillnad från föregående års möte tillägnades frågan en hel dag. Vid mötet konstaterades att säkerhet var nyckeln till att skapa förtroende för e-handel, e-förvaltning och andra onlineaktiviteter samt att säkerhet kan vara den svåraste utmaningen för alla inblandade. För att kunna hantera hot som virus, phising, spionage och botnät betonades vikten av samarbete mellan en rad olika aktörer. En viktig

---

[188] Se http://www.enisa.europa.eu

[189] Se http://www.oecd.org/dataoecd/42/57/32494705.PDF

[190] 3 Rapporter från OECD om RFID har samlats i ett dokument: *OECD Policy Guidance on Radio Frequency Identification, Radio-Frequency Identification: A Focus on Security and Privacy och RFID Applications, Impacts and Country Initiatives* 2008 http://www.oecd.org/dataoecd/19/42/40892347.pdf

[191] OECD, *Policy Guidance for digital content*, 2008

http://www.oecd.org/dataoecd/20/54/40895797.pdf

[192] OECD, OECD recommendation of the council on the Protection of Critical Information Infrastructures [C(2008)35] se http://www.oecd.org/dataoecd/1/13/40825404.pdf

förutsättning för ett sådant samarbete är enligt IGF att skapa förtroende mellan de inblandade.

Då Internet, och följaktligen alla säkerhetsfrågor som är kopplade till Internetanvändande, är av internationellt intresse är det av betydelse att IGF så tydligt trycker på behovet av internationella insatser och samverkan samt erbjuder en plattform för sådant arbete.

7.5.4 European Program for Critical Infrastructure Protection, EPCIP

General Direktoratet för rättvisa, frihet och säkerhet finansierar en studie som belyser beroendet av ICT (Information and Communication Technology) i energi, finans och transportsektorn. Syftet med studien är att skapa en bättre förståelse för hotet mot kritisk infrastruktur samt vilka säkerhetsrisker som bör hanteras. Studien ska även se på vilka konsekvenser på samhällsnivå detta kan leda till. Målet med studien är att visa på:

- Metoder för bedömning av kritisk infrastrukturs beroende av ICT
- Avtal samt definitioner av vad som räknas som kritiskt
- Riktlinjer för att reducera IT-hotet mot kritisk infrastruktur
- Rekommendationer avseende säkerhetsåtgärder som kan ligga till grund för beslut, både för ägare av kritisk infrastruktur samt beslutsfattare på EU - nivå

Studien initierades i början av september 2008 och drivs i projektform. Projektet ska leverera sin rapport i slutet av juli 2009. Som en naturlig del i detta arbete kommer projektgruppen att arbeta nära tillsammans med kommissionen, ägare av kritisk infrastruktur, myndigheter, organisationer och forskningsinstanser.[193]

7.5.5 Internationell samverkan

Utvecklingen inom området cybersäkerhet har gett upphov till ett behov för internationell samverkan. Flera nationella initiativ har tagits för att stärka den nationella säkerheten mot cyberhot i samverkan med andra länder. Det amerikanska Cyber Security Initiativ som initierades 2008 är exempel på ett mycket omfattande sådant.

Nästan ett år efter de storskaliga nätverksattackerna mot Estland enades försvarsministrarna inom NATO om en cyberförsvarspolicy som antogs i början av 2008. I policyn ingår utvecklingen av en responsmekanism i händelse av en cyberattack.[194] Det har inom NATO även utvecklats ett koncept för cybersäkerhetsfrågor. [195] Medlemsländerna uppmanas till att stärka sina nyckelinfrastrukturer, dela med sig av erfarenheter och kunnande - så kallad best practices, samt se till att kunna tillhandahålla stöd i händelse av att något

[193] http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm

[194] Nina Wilhelmson FHS

[195] http://www.NATO.int/docu/update/2008/05-may/e0514a.html

av medlemsländerna skulle begära detta vid en attack.[196] Vidare betonas internt samarbete vid en attack, såsom personliga nätverk av (politiska) ledare och experter, samverkan mellan den privata och offentliga sektorn, samt ett förebyggande försvar.[197] I april 2008 bestämdes vidare om inrättandet av ett nytt Centre of Excellence i Estland för cybersäkerhet - Cooperative Cyber Defence Centre of Exellence (CCDCOE), som nu har kommit igång med sin verksamhet.[198]

Tidigare har man inom NATO uppgett att man endast ska använda organisationens resurser till att skydda dess egna nätverk. I den policy som nu har utvecklats innefattas även medlemsländerna och under attackerna i Georgien 2008 sändes personal ut från NATO för att ge stöd vilket möjligen tyder på ett ännu bredare upptagningsområde med tanke på att Georgien inte är NATO medlem. Även inom EU pågår ett arbete där man nu ser på området cybersäkerhet och diskussioner pågår kring hur man skall förhålla sig till detta.

7.6 Övning och utbildning

IT används idag inom hela samhället och av i stort sett varje medborgare. Det gör att kunskaper om informationssäkerhet är nödvändiga för att den enskilde ska kunna skydda sin information och de transaktioner denne utför. Till detta ska föras aspekten att var och en med sina handlingar bidrar till samhällets gemensamma säkerhet och robusthet.

Det är väsentligt att utbildning om informationssäkerhet når alla grupper i samhället. Kunskaper om risker med hantering av IT och Internet måste därför tidigt tillföras medborgarna och utgöra en integrerad och naturlig del av hela skolgången samt finnas med i högre utbildningar.

Utbildning och förståelse för informationssäkerhet är grundläggande för att kunna nå de mål som satts ut på informationssäkerhetsområdet. Vi har därför valt att redogöra för två nya satsningar på utbildning och två större övningar som har genomförts.

7.6.1 Chief Information Assurance Officer (CIAO)

Försvarshögskolan har i samarbete med MSB startat en kvalitetssäkrad CIAO-kurs. Kursen, som är etablerad sedan lång tid och genomförs på det amerikanska National Defense University (NDU) och deras Information Resources Managment College (IRMC), har nu modifierats för en svensk/europisk målgrupp. CIAO-kursen syftar till att sätta informationen i fokus och öka förmågan av balanserad riskhantering mellan personal, processer och teknik för att uppnå verksamhetens mål. Den vänder sig främst till dem som har en central roll i verksamheters informationssäkerhetsarbete.

[196] Bucharest Summit Declaration (art. 47)

[197] Nina Wilhelmsson, FHS

[198] http://www.ccdcoe.org

7.6.2 SIS Informationssäkerhetsakademi

Under 2008 lanserade SIS sin Informationssäkerhetsakademi som vänder sig till dem som ansvarar för, påverkar eller medverkar till verksamhetens informationssäkerhet. Kursen är uppbyggt kring standardsviten 27000.

Med hänsyn till att standarderna i 27000-serien lyfts fram i allt fler sammanhang, inte minst i rättsliga regelverk, är det av betydelse att det finns utbildningsmöjligheter.

7.6.3 Samverkansövning 2008 (SAMÖ 08)

En viktig del i det kompetenshöjande arbetet är övning. Detta gäller särskilt för situationer där flera olika organisationer ska samverka och samarbeta kring en gemensam fråga.

Den 22-24 april 2008 genomförde 3 000 deltagare från Regeringskansliet, centrala myndigheter, länsstyrelser, kommuner, organisationer och företag samt ett stort allmänhetsnätverk samverkansövningen SAMÖ 2008. KBM hade ansvar för att planera, genomföra och utvärdera övningen.

Scenariot i övningen handlade om omfattande logiska IT-attacker mot det finansiella systemet. Den finansiella sektorn, bland annat myndigheter inom samverkansområdet Ekonomisk säkerhet, liksom polisen och geografiskt områdesansvariga aktörer på nationell och regional nivå, påverkades. Händelser som får allvarliga konsekvenser för flera samhällsviktiga funktioner krävde samordnade insatser.

Nyckelordet i övningen var förtroende och syftet med övningen var att alla aktörer efter övningen skulle kunna säga att de utvecklat sin förmåga att i samverkan behålla förtroendet för samhällets institutioner vid en kris.

Utifrån syftet fanns två delmål; Att aktörerna samordnar sina beslut och åtgärder och på så sätt skapar en gemensam lägesuppfattning och att informationen från de övade till media och allmänhet var trovärdig, relevant och lättillgänglig.

Utvärderarna av SAMÖ[199] drog tre slutsatser;

- Aktörerna prioriterade inte samverkan eller samordning utanför befintliga nätverk.
- Aktörerna hade inte tillräcklig kunskap om andra aktörers ansvar och mandat.
- Det skapades aldrig en gemensam lägesuppfattning.

Ur slutsatserna kan tre utvecklingsbehov dras;

[199] KBM, *Utvärdering av Samverkansövning 2008*

- En bättre samverkan i kris nås enklast genom ett tydliggörande av roller och ansvar. Varje aktör måste förstå hur övriga aktörer berörs av de beslut och åtgärder som man själv tar och ha en bättre kunskap om andra aktörers mandat och ansvar i kris.
- Relevanta kontaktytor måste skapas redan i vardagen.
- Rutiner och metoder för att skapa en gemensam lägesuppfattning måste klargöras.

Sammanfattningsvis kan man säga att det viktigaste att fokusera på för MSB är att;

- Fördjupa diskussionen om begreppen lägesbild och lägesuppfattning.
- Klargöra rapporteringsrutiner och hur återkoppling av information ska ske till berörda aktörer.
- Genom övning och utbildning bidra till ökad kunskap om aktörers olika roller och mandat.

7.6.4 FHS Övning

Efter de cyberattacker som drabbade Estland under 2007 påbörjades samverkan mellan Sverige och Estland med syfte dels att följa utvecklingen i Estland samt upprätthålla kontakterna med SIVAK och skapa ett nätverk för forskningsutbyte. Detta utbyte har bland annat resulterat i en övning som ägde rum den 6 december 2008. Denna övning sponsrades av KBM och genomfördes i FHS regi tillsammans med experter från Estland samt med stöd av FOI, FMV och FRA. Övningen omfattade främst intrångsattacker och huvuddelen av de försvarande lagen bestod av magisterstudenter från Linköpings universitet och Mastersstuderande på Informationssäkerhetsprogrammet vid Tallinns tekniska högskola.

Ett antal möjliga förbättringar identifierades och en fortsättning på en något högre nivå planeras för 2009 i syfte att Sverige ska vara väl rustat och en kompetent partner inför den internationella övningen Cyberstorm III hösten 2010.

Källor och vidare läsning

Offentligt tryck

Prop 2005/06:133 *Samverkan vid kris - för ett säkrare samhälle*
http://www.regeringen.se/download/49d6475a.pdf?major=1&minor=60468&cn=attachmentPublDuplicator_0_attachment

Prop 2001/02:158 *Samhällets säkerhet och beredskap*
http://www.regeringen.se/download/03c0eac6.pdf?major=1&minor=3260&cn=attachmentPublDuplicator_0_attachment

Prop 2008/09:67 *Civilrättsliga sanktioner på immaterialrättens område - genomförande av direktiv 2004/48/EG*
http://www.regeringen.se/download/c18e5f5a.pdf?major=1&minor=116938&cn=attachmentPublDuplicator_0_attachment

Skr. 2005/06:139 *Nationell IT-strategi för vård och omsorg*
http://www.regeringen.se/content/1/c6/06/03/73/9959f31e.pdf

Handlingsplan för eFörvaltning (2008)
http://www.regeringen.se/content/1/c6/07/49/95/2c28b30b.pdf

Regeringens strategi för ökad säkerhet i Internets infrastruktur N2006/5335/ITFoU
http://www.regeringen.se/content/1/c6/01/83/13/1c50c06e.pdf

SOU 2004:32 *Informationssäkerhet i Sverige och internationellt - en översikt (Delrapport från InfoSäkutredningen)*
http://www.regeringen.se/download/24f80e10.pdf?major=1&minor=23350&cn=attachmentPublDuplicator_0_attachment

SOU 2005:42 *Säker information*
http://www.regeringen.se/download/84506b80.pdf?major=1&minor=44381&cn=attachmentPublDuplicator_0_attachment

SOU 2007:39 *Framtidens polis*
http://www.regeringen.se/download/85343fad.pdf?major=1&minor=83590&cn=attachmentPublDuplicator_0_attachment

SOU 2007:76 *Lagring av trafikuppgifter för brottsbekämpning*
http://www.regeringen.se/download/2f8c7424.pdf?major=1&minor=91521&cn=attachmentPublDuplicator_0_attachment

SOU 2009:1 *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen*
http://www.regeringen.se/download/bca06dc6.pdf?major=1&minor=119163&cn=attachmentPublDuplicator_0_attachment

SOU 2009:5 *Säkerhetskopiors rättsliga status*
http://www.regeringen.se/download/f72be402.pdf?major=1&minor=119810&cn=attachmentPublDuplicator_0_attachment

Verket för förvaltningsutveckling, *Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte*, VERVAFS 2007:2
http://www.regeringen.se/content/1/c6/11/82/47/da357c5e.pdf

Europaparlamentets och rådets direktiv 2004/48/EG om säkerställande av skyddet för immateriella rättigheter
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:SV:PDF

Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:SV:HTML

Europeiska gemenskapernas kommission KOM(2007) 267 Meddelande från kommissionen till Europaparlamentet, rådet och Europeiska unionens regionkommitté: Att införa en allmän politik för kampen mot IT-relaterad brottslighet
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:SV:HTML

Europarådet, *Convention on Cybercrime* CETS No.: 185, 2001
http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Myndighetsrapporter

Domstolsverket, *Specialisering - En förstudie i samarbete med Sveriges Domareförbund*, DV-rapport 2003:3
http://www.dom.se/Publikationer/Rapporter/DV-rapport_2003_3.pdf

Finansinspektionen, *Ansvaret för betalningssystemet* (2008:10)
http://www.fi.se/upload/20_Publicerat/30_Rapporter/2008/Rapport2008_10.pdf

Krisberedskapsmyndigheten, *Klarar vi krisen? Samhällets krisberedskapsförmåga 2007*, KBM:s temaserie 2008:2
http://www.krisberedskapsmyndigheten.se/upload/17065/klarar_vi_krisen_temaserien2008-2.pdf

Krisberedskapsmyndigheten, *Samhällets informationssäkerhet, Handlingsplan 2008*, 2008
http://www.krisberedskapsmyndigheten.se/upload/17005/handlingsplan_samhallets_informationssakerhet_20080401.pdf

Krisberedskapsmyndigheten, *Samhällsviktigt! Förslag till definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv*, 2007
http://www.krisberedskapsmyndigheten.se/upload/11351/faktablad_samhallsviktigt_022007.pdf

Krisberedskapsmyndigheten, *Utvärdering av Samverkansövning 2008*
http://www.krisberedskapsmyndigheten.se/upload/17866/Samo_2008_utvardering.pdf

Krisberedskapsmyndigheten, *Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter*, 2008
http://www.krisberedskapsmyndigheten.se/upload/17913/SCADA_sv_2008.pdf

Post- och telestyrelsen, *Botnät - Kapade datorer i Sverige*, PTS-ER-2009:11
http://www.pts.se/upload/Rapporter/Internet/2009/botnat-i-sverige-2009-11.pdf

Post- och telestyrelsen, *God funktion och teknisk säkerhet i elektroniska kommunikationer*, PTS-ER-2008:13
http://www.pts.se/upload/Rapporter/Internet/2008/Tillsyn-god-funktion-och-teknisk-sakerhet-PTS-ER-2008-13.pdf

Post- och telestyrelsen, *Strategi för ett säkrare Internet i Sverige*, PTS-ER-2006:12
http://www.pts.se/upload/Documents/SE/strategi_sakrare_internet_2006_12.pdf

Post- och telestyrelsen, *Säkerhet i lokala trådlösa nät*, PTS-ER-2007:16
http://www.pts.se/upload/Documents/SE/Sakerhet_lokala_tradlosa_nat.pdf

Riksrevisionen, *Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten*, RiR 2006:24
http://www.riksrevisionen.se/templib/pages/OpenDocument____556.aspx?documentid=6442

Riksrevisionen, *Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten*, RiR 2005:26
http://www.riksrevisionen.se/templib/pages/OpenDocument____556.aspx?documentid=5948

Riksrevisionen, *Krisberedskap i betalningssystemet*, RiR 2007:28
http://www.riksrevisionen.se/templib/pages/OpenDocument____556.aspx?documentid=6787

Styrelsen för psykologiskt försvar, *Risk- och sårbarhetsanalys av mediesektorn 2008*

Verket för förvaltningsutveckling, *Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar*, 2008:12

Verket för förvaltningsutveckling, *69 myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltningen*, 2008:14

Övrigt

Brottsförebyggande rådet/Krisberedskapsmyndigheten, *IT-relaterade brott och incidenter – Ett hot mot samhällsviktiga verksamheter?*, 2008

CERT-FI, *Information security review*, 2008
https://www.cert.fi/en/reports.html

Codenomicon white paper, *Wireless security: Past, present and future*, 2008
http://www.codenomicon.com/resources/whitepapers/Codenomicon_Wireless_WP_v1_0.pdf

Cyveillance, white paper, *Online financial fraud and identity theft report*, 2008
http://www.cyveillance.com/web/knowcenter/white-papers.asp

Deloitte, *Treading Water, the 2007 technology, media & telecommunications security survey*, 2007
http://www.deloitte.com/dtt/cda/doc/content/se_treading_water_120208.pdf

Department for business enterprise & regulatory reform (BERR), *2008 information security breaches survey – executive summary*, 2008
http://www.berr.gov.uk/files/file45713.pdf

European Network and Information Security Agency, *ENISA Position paper, Security issues in the context of authentication using mobile devices (Mobile eID)*, 2008
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf

Försvarshögskolan CATS, Nina Wilhelmsson, *Folkrättsliga aspekter på cyberhot och skydd mot informationsoperationer, en studie baserad på erfarenheter från cyberattackerna mot Estland 2007*, 2008

Georgia Tech Information Security Center, *Emerging Cyber Threats Report for 2009*, 2008
http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

Google, *2008 annual Google communications intelligence report a google white paper February 2008*, 2008
http://www.google.com/a/help/intl/en/security/pdf/cir_08.pdf

Halon, *Q4 2008 Internet Threats Trend Report*, 2009
http://www.halonsecurity.ch/press/documents/2008_q4_email_threats_trend_report.pdf

McAfee, *Virtual Criminology Report - Cybercrime Versus Cyberlaw*, 2008
http://resources.mcafee.com/content/NAMcAfeeCriminologyReport

Microsoft, *Security Intelligence Report, January through June 2008*, 2008,
http://download.microsoft.com/download/b/2/9/b29bee13-ceca-48f0-b4ad-53cf85f325e8/Microsoft_Security_Intelligence_Report_v5.pdf

Nohlberg, Marcus, *Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks*, Stockholms Universitet, 2009

OECD, *OECD Policy Guidance for digital content*, 2008
http://www.oecd.org/dataoecd/20/54/40895797.pdf

OECD, *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures* [C(2008)35], 2008
http://www.oecd.org/dataoecd/1/13/40825404.pdf

OECD, *RFID Radio Frequency Identification: OECD Policy Guidance - A Focus on Information Security and Privacy - Applications, Impacts and Country Initiatives*, 2008
http://www.oecd.org/dataoecd/19/42/40892347.pdf

Reporting and Analysis Centre for Information Assurance MELANI, *Information assurance – Situation in Switzerland and internationally*, 2008
http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=en

SECODE, *Security threats and trends December 2008*, 2008
http://www.secode.se/be/__xs_attachments/Threats_and_Trends_December_2008.pdf

SECODE, *Security threats and trends February 2008*, 2008
http://www.secode.se/be/__xs_attachments/2008-02%20-%20IDS%20-%20Trusler%20og%20Trender-ENG.pdf

Sofaer, Abraham D. & Goodman, Seymor E. et al., *A proposal for International Convention on Cyber Crime and Terrorism*, CISAC Report, 2000
http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm

Srejber, Eva, Sveriges Riksbank, *Sårbarheter i det moderna betalningsväsendet*, anförande Sveriges säkerhetsting i Eskilstuna 2006-10-18

Symantec, *Symantec global Internet security threat report, trends for July- December 07*, 2008
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

United States government accountability office (GAO), *Information security – Although progress reported, federal agencies need to resolve significant deficiencies*, GAO-08-496T, 2008
http://www.gao.gov/new.items/d08496t.pdf

Verizon business, *2008 data breach investigations report*, 2008
http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Åhlfeldt, Rose-Mharie, *Information Security in Distributed Healthcare, Exploring the Needs for Achieving Patient Safety and Patient Privacy*, Stockholm University, 2008

MSB Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msbmyndigheten.se
Publ.nr MSB 0023-09 ISBN 978-91-7383-009-6