Nationell hanterandeplan för allvarliga IT-incidenter

Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap

(Fö2010/701/SSK, Regeringsbeslut 12, 2010-04-14)

Förord

Regeringen gav den 14 april 2010 Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att senast den 1 mars 2011 ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras (Fö2010/701/SSK).

MSB redovisar i denna rapport den hanterandeplan som tagits fram. Planen är baserad på fyra huvudkomponenter: nationell lägesbild, informationssamordning, samlad konsekvens- och hanterandebedömning samt teknisk operativ samverkan. Hanterandeplanen aktiveras efter beslut av MSB, men ställer inte några uttalade krav på hanterande vid andra myndigheter. Däremot preciseras i planen vad som förväntas av andra aktörer i form av informationsdelning och samverkan.

Utöver hanterandeplanen har uppdraget även inbegripit att skapa tekniska kompetensnätverk som kan stödja samhället vid allvarliga IT-incidenter för att skapa en ökad förmåga till respons. I rapporten redovisar MSB konkreta förslag till stöd för skapande och upprätthållande av för samhället viktiga tekniska kompetensnätverk.

Stockholm 1 mars 2011

Helena Lindberg

Generaldirektör

Richard Oehme

Chef för Enheten för samhällets informationssäkerhet

Sammanfattning

I föreliggande rapport beskriver Myndigheten för samhällsskydd och beredskap (MSB) den nationella planen för hantering av allvarliga IT-incidenter (hanterandeplanen). Syftet med planen är att, genom samverkan och ett koordinerat beslutsfattande, förbättra förutsättningarna för att begränsa och avvärja de direkta konsekvenserna av en allvarlig IT-incident i samhället. För att lösa den uppgiften kommer det att krävas ett brett samarbete mellan olika aktörer.

Mål

Hanterandeplanen ska säkerställa möjligheterna till att

- upprätthålla en gemensam, kvalificerad lägesbild
- ge samordnade budskap till allmänheten
- snabbt och effektivt använda samhällets samlade resurser
- stödja effektiv teknisk hantering
- fatta kvalificerade, koordinerade beslut
- agera koordinerat på internationell nivå
- systematiskt utvärdera och återkoppla erfarenheterna.

Några utgångspunkter

En allvarlig IT-incident definieras som en IT-relaterad händelse som

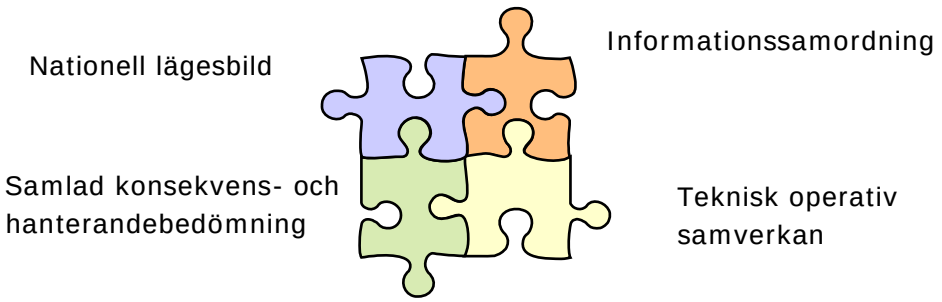
- avviker från det normala
- innebär en allvarlig störning i samhällsviktig verksamhet
- kräver snabba insatser på nationell nivå
- kräver samordnade insatser på nationell nivå.

Definitionen utgår från lagstiftningen kring extraordinära händelser i fredstid och höjd beredskap, och från definitioner av samhällsviktig verksamhet.

Hanterandeplanen fokuserar uteslutande på *hanteringen* av allvarliga IT-incidenter. Den utgår från de grundförutsättningar som finns inom det svenska krishanteringssystemet, det vill säga styrande principer och de enskilda aktörernas ansvar.

Samverkansprocesser i fokus

Hanterandeplanen består av fyra centrala samverkansprocesser: nationell lägesbild, informationssamordning, samlad konsekvens- och hanterandebedömning samt teknisk operativ samverkan.



Planen aktiveras efter beslut av MSB. Detta sker antingen när det föreligger ett påtagligt hot om (eller överhängande risk för) en allvarlig IT-incident eller när en sådan incident redan inträffat. Att planen aktiveras innebär inte att MSB ställer krav på hur incidenten hanteras vid andra myndigheter. Det hör till dessa myndigheters verksamhetsansvar. Däremot preciseras i planen vad berörda aktörer förväntas göra när det gäller informationsdelning och samverkan.

MSB beskriver nedan översiktligt de fyra huvudkomponenterna i hanterandeplanen.

Översiktlig beskrivning av de fyra huvudkomponenterna i hanterandeplanen

	Nationell lägesbild	**Informations-samordning**	**Samlad konsekvens- och hanterande-bedömning**	**Teknisk operativ samverkan**
Mål	Skapandet av en gemensam lägesbild för att ge möjlighet till koordinerat agerande och därmed ändamålsenlig användning av samhällets resurser i hanteringen av allvarliga IT-incidenter	Samordnad och kvalitativ information till allmänheten	En fördjupad och kompletterad konsekvensbaserad lägesbild ur ett samhälleligt perspektiv	Återställning till godtagbar funktionalitet
Uppnås genom	Samverkans-konferenser, aktörsspecifika aktiviteter	Informations-samordnings-konferenser, kommunikativa aktiviteter	Analys genomförd av MSB (med stöd av den nationella operativa samverkansfunktion-en för informations-säkerhet – NOS) som utgår från aktörernas lägesrapportering	Samverkan mellan berörda parter inom nationella och internationella nätverk
Ansvarig	MSB	MSB	MSB	Ansvariga aktörer
Berörda parter	SAMFI, centrala myndigheter, länsstyrelser, kommuner, samverkans-forum, näringsliv, övriga	Informatörs-nätverk och andra relevanta parter	SAMFI-myndigheterna, relevanta nätverk nationellt och internationellt, aktörer med ansvar för samhällsviktig verksamhet	SAMFI-myndigheterna, berörda aktörer
Exempel på verktyg	WIS, RAKEL, SOS-Alarm, Stödsystem för obligatorisk incidentrapport-ering, system för omvärldsbevak-ning	Krisinforma-tion.se, informations-tjänst, presskonferens text-tv, radio, RAKEL, SGSI, VMA, myndighets-meddelande	Beroendesimulering, RSA-db, övriga	Tillgängliga kommunika-tionskanaler, säkra kryptografiska funktioner

Planen är interimistisk tills dess att den övats och reviderats i linje med resultaten. Senast 2012 ska den första övningen vara genomförd och planen fastställd. MSB och enheten för informationssäkerhet ansvarar för att planera och genomföra övningen i samverkan med SAMFI-myndigheterna.

Stöd till framväxten av tekniska kompetensnätverk

När en allvarlig IT-incident inträffar är det de olika verksamheternas ordinarie personal som utgör basresursen för att praktiskt tekniskt hantera det inträffade. Denna basresurs riskerar att bli hårt ansträngd under en allvarlig IT-incident. Det kan därför uppstå behov av extra stöd i form av expert-kompetens. Det är ur detta perspektiv viktigt att *stödja framväxten av tekniska kompetensnätverk* som kan bidra till att öka samhällets förmåga att hantera konsekvenserna av allvarliga IT-incidenter.

De myndigheter som har ett särskilt ansvar inom informationssäkerhets-området har en viktig roll när det gäller nationell expertresurs, men tekniska kompetensnätverk behöver finnas på alla nivåer i samhället. Det förslag som läggs fram innebär följande:

- MSB avser att i samråd med myndigheterna i SAMFI undersöka möjligheten att organisera ett tekniskt kompetensnätverk bestående av tekniskt operativa SAMFI-experter.
- MSB avser att tillsammans med andra berörda aktörer genomföra en pilotstudie för att utveckla metoder och verktyg som kan stödja arbetet med tekniska kompetensnätverk på kommunal, regional och nationell nivå.
- MSB avser att aktivt arbeta för en utvecklad privat–offentlig samverkan mellan dels experter, dels experter och mottagare av experthjälpen i syfte att öka samhällets förmåga att hantera allvarliga IT-incidenter. Detta ska MSB göra genom att arrangera seminarier, konferenser och övningar.

Innehåll

1. Inledning 1
1.1 Bakgrund och utgångspunkter 1
1.2 Uppdragets genomförande 2
1.3 Varför behövs en plan för allvarliga IT-incidenter? 2
1.4 Konceptuell struktur – vision, mål och plan 3
1.5 Avgränsningar 4
1.6 Centrala begrepp 5
1.7 Läsanvisningar 6
2. Vad är en allvarlig IT-incident? 7
2.1 Definition av allvarlig IT-incident 7
2.2 Exempel på en allvarlig IT-incident 9
2.2.1 IT-attacker mot Estland 9
3. Grundförutsättningar för hanterandeplanen 11
3.1 Det svenska krishanteringssystemet 11
3.2 Styrande principer 11
3.2.1 Ansvarsprincipen 11
3.2.2 Närhetsprincipen 12
3.2.3 Likhetsprincipen 12
3.3 Ansvar och roller 12
3.3.1 Grundkrav på alla aktörer avseende krisberedskap 13
3.3.2 Särskilt ansvar inom krisberedskap 15
3.3.3 Särskilt ansvar för informationssäkerhet 17
3.3.4 Privata aktörer med ansvar för samhällsviktig verksamhet 25
4. Nationell hanterandeplan för allvarliga IT-incidenter 26
4.1 Samverkansprocesser i fokus 26
4.2 Hanterandeplanens ram 28
4.2.1 Aktivering av hanterandeplanen 29
4.2.2 Avaktivering av planen 30
4.2.3 Utvärdering av planen 30
4.2.4 Rutiner som är kopplade till hanterandeplanens ram 30
4.3 Nationell lägesbild 31
4.4 Informationssamordning 33
4.5 Samlad konsekvens- och hanterandebedömning 35
4.6 Teknisk operativ samverkan 36
5. Förvaltning av hanterandeplanen för allvarliga IT-incidenter 39
5.1 Ägarskap 39
5.2 Giltighet 39
5.3 Revidering, utvärdering och erfarenhetsåterkoppling 39
5.4 Kontaktperson 39
6. Finansiering 40

Bilaga A: Regeringsuppdraget
Bilaga B: Uppdragets organisation
Bilaga C: Förkortningar och vissa begrepp
Bilaga D: Förteckning över stödjande rutiner
Bilaga E: Tekniska kompetensnätverk
Bilaga F: Internationell utblick

1. Inledning

Det svenska samhället lutar sig i stor utsträckning mot att det finns en fungerande IT-infrastruktur och allt fler verksamheter är kritiskt beroende av IT och kommunikationsteknologi i det dagliga arbetet. Sårbarheter i systemen kan få stora konsekvenser – för såväl den enskilda som för samhället i stort.

Den nationella planen för hantering av allvarliga IT-incidenter syftar till att, genom samverkan och ett koordinerat beslutsfattande, förbättra förutsättningarna för att begränsa och avvärja de direkta konsekvenserna av en allvarlig IT-incident i samhället. En allvarlig IT-incident definieras som en IT-relaterad händelse som

- avviker från det normala
- innebär en allvarlig störning i samhällsviktig verksamhet
- kräver snabba insatser på nationell nivå
- kräver samordnade insatser på nationell nivå.

För att kunna säkerställa samhällets förmåga att hantera allvarliga IT-incidenter krävs en samlad insats och ett brett samarbete mellan olika aktörer. En koordinerad nationell hantering av IT-incidenter förutsätter ett ändamålsenligt ramverk. Den nationella planen för hantering av allvarliga IT-incidenter ska utgöra ett sådant ramverk.

1.1 Bakgrund och utgångspunkter

Myndigheten för samhällsskydd och beredskap (MSB) fick i april 2010 i uppdrag av regeringen att i samråd med övriga myndigheter inom samverkansgruppen för informationssäkerhet (SAMFI) ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras. I uppdraget ingick också att skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter.

Uppdraget var formulerat enligt följande:

> *Myndigheten för samhällsskydd och beredskap ska ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras samt skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter för att skapa en ökad förmåga till respons. Myndigheten för samhällsskydd och beredskap ska genomföra uppdraget i samråd med de myndigheter som ingår i samverkansgruppen för informationssäkerhet, SAMFI. (Regeringsuppdrag 2010-04-14, Fö2010/701/SSK)*

MSB har tolkat uppdraget som att hanterandeplanen ska utgå från det svenska krishanteringssystemets grundprinciper ansvars-, närhets- och likhetsprincipen. Dessutom ska planen

- ta hänsyn till att allvarliga IT-incidenter kan ha flera olika orsaker
- klargöra roller och ansvar på nationell nivå samt kopplingar till den internationella nivån
- ange processer och rutiner för den nationella hanteringen av allvarliga IT-incidenter.

En central utgångspunkt har varit att planen ska nära ansluta till de principer för krishantering som tillämpas i samhället.

MSB har påbörjat arbetet med att ta fram tekniska kompetensnätverk och ger i bilaga E tre konkreta förslag till hur myndigheten, i samverkan och samråd med andra aktörer, kan verka för att skapa en ökad förmåga till att hantera allvarliga IT-incidenter.

1.2 Uppdragets genomförande

Arbetet med att ta fram den nationella hanterandeplanen för allvarliga IT-incidenter har i huvudsak bedrivits av en arbetsgrupp vid MSB bestående av representanter från flera avdelningar och enheter. Enheten för samhällets informationssäkerhet har varit sammanhållande.

För att säkerställa att relevanta externa aktörer deltog i arbetet bjöd MSB in till en extern referensgrupp. I denna har representanter från statliga myndigheter, kommuner, universitet och privat näringsliv ingått. I bilaga B framgår hur arbetet med uppdraget har organiserats och hur sammansättningen av referensgruppen sett ut.

I uppdragsbeskrivningen framgår att uppdraget ska genomföras i samråd med myndigheterna i SAMFI. Därför infördes en stående punkt på SAMFI:s ordinarie möten där eventuella frågor om uppdraget kunde lyftas för avdömning. Samtliga myndigheter i SAMFI har också varit representerade i referensgruppen.

1.3 Varför behövs en plan för allvarliga IT-incidenter?

I samhället i dag finns strukturer och regelverk för att hantera olika typer av olyckor och kriser på både lokal, regional och nationell nivå. Den nationella hanterandeplanen för allvarliga IT-incidenter kompletterar dessa strukturer och regelverk när det gäller att hantera konsekvenserna av allvarliga IT-incidenter. Det är särskilt fem förhållanden som gör att det behövs en särskild nationell plan:

1. Korta tidsförhållanden
    a. Händelseförloppet är ofta snabbt vid en IT-incident, vilket gör att det måste vara tydligt vilken aktör som ska agera när.
    b. Möjligheterna till förvarning är ofta små, till skillnad från exempelvis väderrelaterade händelser, vilket gör att berörda aktörer snabbt måste koordinera arbetet.
    c. Det är nödvändigt att ha tillgång till väl etablerade samverkans- och informationskanaler.
2. Sektorsövergripande konsekvenser och beroendeförhållanden mellan samhällets sektorer
    a. Störningar kan snabbt komma att påverka många aktörer. Internet och andra centrala informationsinfrastrukturer är av grundläggande betydelse för ett stort antal sektorer i samhället.
    b. Beroendet mellan sektorer när det gäller el, tele och IT ställer särskilda krav på samverkan under en kris.
3. Geografisk obundenhet
    a. Hot, risker och sårbarheter på IT-området är ofta geografiskt obundna. Nationell och internationell samverkan måste formas på ett ändamålsenligt sätt för att möta detta.
4. Förtroendefrågor
    a. Samhällets grundläggande funktioner är beroende av, och dimensionerade för, ett fungerande IT-stöd. IT-störningar kan snabbt påverka allmänhetens förtroende negativt för tjänster eller för centrala aktörer, vilket skapar ett behov av ett koordinerat budskap för att mildra effekterna.
5. Kompetensbehov
    a. Hanteringen av IT-incidenter ställer i vissa skeden stora krav på specialistkompetens för att berörda aktörer ska kunna avvärja eller mildra effekterna av en störning. Att tillgängliggöra kompetens – på olika nivåer i samhället – är viktigt.

1.4 Konceptuell struktur – vision, mål och plan

Visionen för hanterandeplanen har definierats som att skapa förutsättningar för att minimera konsekvenserna av en allvarlig IT-incident genom samverkan och ett koordinerat beslutsfattande.

MSB har, tillsammans med de aktörer som deltagit i uppdragets genomförande, brutit ned denna vision i ett antal konkreta mål. Genom ändamåls-

enliga processer samt tydliga roll- och ansvarsbeskrivningar ska planen säkerställa möjligheten till att

- ta fram en gemensam och kvalificerad lägesbild med hänsyn taget till informationsteknologins centrala roll för samhällets funktionalitet
- formulera och kommunicera ett samordnat budskap till allmänheten
- effektivt och snabbt använda samhällets samlade resurser
- stödja effektiv teknisk hantering av IT-incidenten
- fatta kvalificerade och koordinerade beslut
- svenskt agerande på internationell nivå sker koordinerat
- systematisk utvärdering och erfarenhetsåterkoppling sker.

Med utgångspunkt i visionen och målen har MSB tagit fram den nationella hanterandeplanen för allvarliga IT-incidenter.

1.5 Avgränsningar

Huvudsyftet med planen är att skapa förutsättningar för att kunna säkerställa samhällets förmåga att hantera allvarliga IT-incidenter. Uppgiften kräver som tidigare nämnts en samlad insats och ett brett samarbete mellan olika aktörer. För att kunna uppnå detta är det viktigt att olika aktörers ansvar och roller kopplade till arbetet med att hantera allvarliga IT-incidenter är tydliggjorda. Grunden för hanterandeplanen är de legala förutsättningarna tillsammans med centrala principer som exempelvis ansvarsprincipen. Eftersom hanterande-planen tar fasta på behovet av samverkan och koordinering mellan aktörer, är det ansvar och roller i förhållande till det som behandlas i planen. Exempelvis påverkar hanterandeplanen inte det stöd till insatser i samband med nationella kriser med IT-inslag som underrättelse- och säkerhetstjänster särskilt ska svara för.

Planen innehåller en genomgång av aktörernas ansvar inom krishantering och informationssäkerhet som finns utpekat i författningstexter, men går inte in i detalj på hur enskilda aktörer väljer att lösa sina uppgifter.

Hanterandeplanen fokuserar uteslutande på *hantering* av allvarliga IT-incidenter. Detta innebär att det förebyggande arbetet inom informations-säkerhetsområdet inte inkluderas trots att det är av avgörande betydelse för förmågan att kunna hantera allvarliga IT-incidenter. I delar av planen finns dock hänvisningar till viktiga rutiner inom det förebyggande arbetet som stöd för att till exempel etablera en gemensam lägesbild.

Planen har vidare tagits fram för hantering av allvarliga IT-incidenter i fredstid och gäller inte vid höjd beredskap.

1.6 Centrala begrepp

I hanterandeplanen används olika begrepp. En del är välkända, andra behöver förklaras närmare.

Begreppet *allvarlig IT-incident* är centralt och beskrivs utförligt i kapitel 2. I samma kapitel presenteras den definition av *samhällsviktig verksamhet* som MSB tidigare tagit fram. Regeringen har gett MSB i uppdrag att ta fram en samlad nationell strategi för skydd av samhällsviktig verksamhet (Regeringsuppdrag Fö2010/698/SSK). I detta ingår att förtydliga begreppet samhällsviktig verksamhet. Uppdraget ska redovisas till regeringen 1 mars 2011.

Med ett *koordinerat* beslutsfattande avses att aktörerna delar samma lägesbild och utifrån denna fattar sina respektive beslut.

Informationssäkerhet används i en vid bemärkelse. Begreppet avser både administrativa och tekniska aspekter med avseende på konfidentialitet, riktighet och tillgänglighet av information och de resurser som används för att hantera informationen. Men informationssäkerhet handlar om mer än att säkra informationssystem. Även resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

Nationell operativ samverkansfunktion (NOS) är en samverkansform som genom

- ändamålsenliga arbetsformer
- deltagande av aktörer med god insikt i IT-incidentfrågor
- goda fysiska förutsättningar (lokaler, kommunikationsutrustning, med mera)

skapar möjlighet att starkt öka förutsättningarna för en samlad nationell hantering av allvarliga IT-incidenter.

NOS ska säkerställa att samhällets samlade resurser på bästa möjliga sätt används vid hanteringen av allvarliga IT-incidenter samt att internationell hjälp vid behov kan tas emot säkert och effektivt. Arbetet inom NOS vilar på ansvarsprincipen, det vill säga varken MSB eller någon annan i NOS-samarbetet tar över någon annan aktörs ansvar att praktiskt hantera en IT-incident.

CERT står för Computer Emergency Response Team och är benämningen på en verksamhet med huvudsaklig uppgift att bevaka och hantera IT-incidenter. En *nationell* CERT är en kontaktpunkt för informationsdelning och koordinering inom landet och internationellt. I Sverige drivs den nationella CERT:en, CERT-SE, sedan 1 januari 2011 av MSB.

Begreppet *krisberedskap* definieras på samma sätt som i 4 § förordning (2006:942) om krisberedskap och höjd beredskap (KBF), det vill säga förmågan att genom utbildning, övning och andra åtgärder samt genom den

organisation och de strukturer som skapas före, under och efter en kris förebygga, motstå och hantera krissituationer.

1.7 Läsanvisningar

Efter beskrivningen av bakgrund och avgränsningar i kapitel 1 följer i kapitel 2 ett resonemang om vad som avses med allvarliga IT-incidenter. Såväl en definition av en allvarlig IT-incident som ett faktiskt exempel presenteras för att läsaren ska förstå vad det är som skiljer allvarliga IT-incidenter från andra, mer ”vardagliga”, IT-incidenter.

I kapitel 3 finns en genomgång av såväl styrande principer i krishanterings-systemet som olika aktörers formella ansvar och roller. I kapitel 4 följer en genomgång av de samverkansprocesser som är centrala i den nationella hanterandeplanen för allvarliga IT-incidenter.

Kapitel 5 beskriver hanterandeplanens förvaltning och i kapitel 6 beskrivs de finansiella förutsättningarna.

Det finns även ett antal bilagor:

Bilaga A Regeringsuppdraget

Bilaga B Uppdragets organisation

Bilaga C Begrepp och vissa förkortningar

Bilaga D Förteckning över stödjande rutiner

Bilaga E Tekniska kompetensnätverk

Bilaga F Internationell utblick

2. Vad är en allvarlig IT-incident?

Utgångspunkten för uppdraget är hanteringen av konsekvenserna av *allvarliga IT-incidenter*. Eftersom det saknas en vedertagen definition av detta begrepp har MSB, tillsammans med referensgruppen för uppdraget, tagit fram en sådan som grund för hanterandeplanen. Stöd i detta arbete har hämtats i andra länders ansatser vad gäller hantering av IT-incidenter som faller utanför det ”normala bruset”. I USA:s responsplan benämns exempelvis dessa i termer av cyberhändelser av nationell signifikans (Homeland Security, *National Cyber Incident Response Plan*, Interim Version 2010, s. 1). MSB har dock hämtat mest underlag från lagstiftningen inom krisberedskapsområdet och från definitioner av samhällsviktig verksamhet.

2.1 Definition av allvarlig IT-incident

En allvarlig IT-incident definieras inom ramen för den nationella hanterande-planen som en IT-relaterad händelse som

1. avviker från det normala
2. innebär en allvarlig störning i samhällsviktig verksamhet
3. kräver snabba insatser på nationell nivå
4. kräver samordnade insatser på nationell nivå.

Det finns alltså *fyra separata villkor som samtliga måste uppfyllas* för att incidenten ska kunna definieras som allvarlig.

Definitionen anknyter till hur en extraordinär händelse definieras i 4 § 1 kap. lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH), det vill säga en

> *[...] händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller ett landsting.*

Definitionen har även sin grund i hur begreppet samhällsviktig verksamhet definieras. *Samhällsviktig verksamhet* ur ett krisberedskapsperspektiv är verksamhet som uppfyller det ena eller båda av följande villkor (Proposition 2007/98:92 *Stärkt krisberedskap – för säkerhets skull*):

1. *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.*

2. *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.*

Exempel på sektorer där det finns verksamheter som alltid måste fungera är: Energiförsörjning, vattenförsörjning, information och kommunikation, finansiella tjänster, socialförsäkringar, hälso- och sjukvård, social omsorg, skydd och säkerhet, transporter, kommunalteknisk försörjning, livsmedel, handel och industri och offentlig förvaltning.

Inspiration har också hämtats från den förklaring till begreppet som MSB ger inom projektet *Styrning av el till prioriterade elanvändare i en elbrist-situation* (Styrel) (MSB *Styrel – inriktning för prioritering av elanvändare,* svar på regeringsuppdrag nr 13 i regleringsbrevet för 2010, d-nr 2009-3054 s. 7). Där används för identifiering av samhällsviktig verksamhet, som ett komplement till definitionen nedanstående begreppsförklaring:

- *Verksamheten är av sådan betydelse för befolkningens liv och hälsa, samhällets funktionalitet samt våra grundläggande värden att den måste kunna bedrivas även vid allvarliga händelser eller kriser.*
- *Verksamheten är av särskild betydelse för att en pågående allvarlig händelse eller kris ska kunna hanteras med så små skadeverkningar som möjligt.*

MSB arbetar för närvarande med att förtydliga begreppet samhällsviktig verksamhet på uppdrag av regeringen, inom ramen för framtagandet av en samlad nationell strategi för skydd av sådan verksamhet (Regeringsuppdrag Fö2010/698/SSK). Förslag kommer att ges till regeringen den 1 mars 2011. Eftersom detta förslag i nuläget inte är färdigarbetat har hanterandeplanens definition av allvarlig IT-incident baserats på de definitioner som gäller i dagsläget.

Definitionen av en allvarlig IT-incident utgår också från Statskontorets riktlinjer *Hantering av IT-incidenter – Vem gör vad och hur?* (IT-kommissionen, 2001) där en IT-incident definieras som en ”oönskad och oplanerad störning [som] drabbar eller påverkar ett IT-system”. IT ges i hanterandeplanen en vid betydelse och definieras som teknik för insamling, lagring, bearbetning, produktion, återfinnande samt kommunikation och presentation av information (data, text, ljud, bild). En IT-relaterad incident kan därmed vara en händelse som påverkar eller stör olika typer av hårdvara, data- eller telekommunikation, styr- och övervakningssystem med mera.

En allvarlig IT-relaterad incident behöver inte vara ett resultat av brottsligt uppsåt. Orsaken kan vara bristande kompetens, misstag eller tekniska sammanbrott och naturhändelser (MSB *Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter*, Uppdragsredovisning, 2009-14471, s.4).

Sammanfattningsvis kan definitionen av en allvarlig IT-incident sägas bestå av fem beståndsdelar, vilka presenteras i Tabell 1 nedan.

Tabell 1. Komponenter i definitionen av en allvarlig IT-incident

Komponenter
En IT-relaterad incident där IT ges en vid bemärkelse
En situation som avviker från det normala
En situation som innebär en allvarlig störning i samhällsviktig verksamhet
En situation som kräver snabba insatser på nationell nivå
En situation som kräver samordnade insatser på nationell nivå

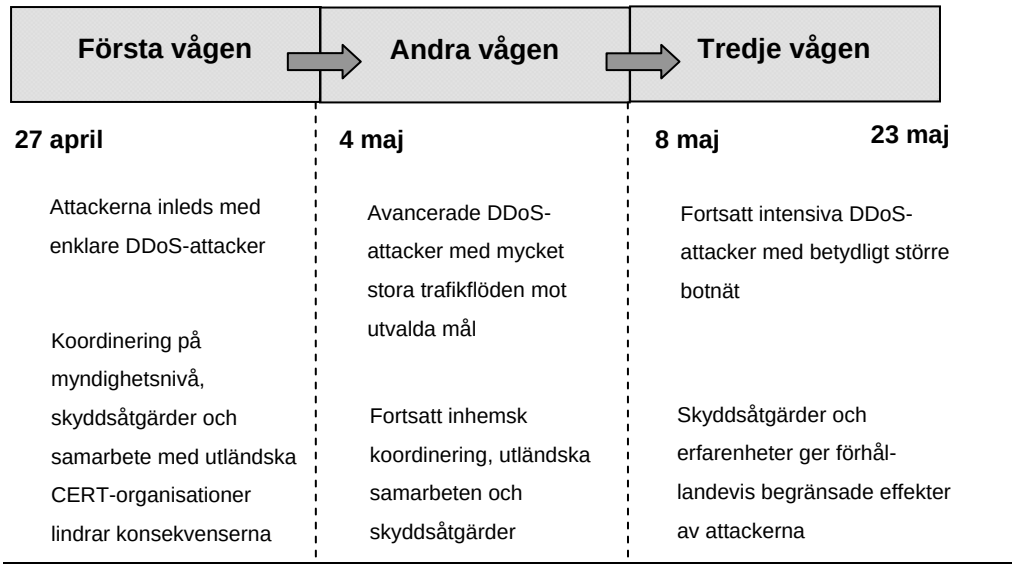
2.2 Exempel på en allvarlig IT-incident

För att visa vad som menas med en allvarlig IT-incident inom ramen för den nationella hanterandeplanen har MSB studerat och analyserat ett antal faktiska IT-incidenter. Ett exempel på en IT-relaterad händelse som anses uppfylla kriterierna för en allvarlig IT-incident är IT-attackerna mot Estland 2007, som var en omfattande tillgänglighetsattack. En IT-incident kan vara mycket mer än så. IT-incidenter kan vara både ”logiska” och ”fysiska” till sin natur. Nedan finns en kort genomgång av IT-attackerna mot Estland. (KBM 2008 *Sveriges beredskap mot nätangrepp* d-nr 1104-2007)

2.2.1 IT-attacker mot Estland

Under april 2007 drabbades Estland av politisk oro och demonstrationer med anledning av att en sovjetisk minnesstaty flyttades. Händelsen resulterade även i en serie omfattande DDoS-attacker (Distributed Denial of Service-attack, en typ av tillgänglighetsattack). Dessa attacker drabbade Estland i tre vågor och pågick totalt under ungefär tre veckor. Händelsen inleddes med enkla åtkomstattacker som efter hand övergick i välkoordinerade attacker.

Organisationer som drabbades var bland annat det estniska parlamentet, ministerier, centrala myndigheter, banker och media. Händelsens förlopp beskrivs i Figur 1, nedan.



Figur 1. Händelseförlopp under IT-attackerna i Estland 2007

I samband med DDoS-attackerna genomfördes misslyckade angreppsförsök mot det estniska telenätet och det system som används av den estniska räddningstjänsten.

Attackerna fick flera direkta konsekvenser. En rad estniska webbplatser drabbades av åtkomstproblem. Politiska partier, parlamentet, presidenten, polisen, skolor, kommuner och flera centrala myndigheter var drabbade.

Hackare placerade falsk information på regeringspartiets webbsida undertecknad av premiärministern. Parlamentet tvingades dessutom att stänga sin e-post under 12 timmar.

Bankers verksamhet på Internet slogs ut och deras kontakt med utlandet blockerades. Internetoperatörer tvingades att släppa samtliga kundkoppel under 20 sekunder för att starta om sin verksamhet.

Sammanfattningsvis fick dessa attacker flera effekter i samhället och flera samhällsviktiga verksamheter påverkades eller riskerade att påverkas av attackerna. Det handlar om information och kommunikation som Internet och teletjänster, betalningsförmedling, räddningstjänstens IT-system och offentlig förvaltning på nationell, regional och lokal nivå.

Denna händelse kan klassas som en allvarlig IT-incident eftersom den

- var IT-relaterad
- avvek från det normala
- innebar en allvarlig störning i samhällsviktig verksamhet
- krävde snabba insatser på nationell nivå
- krävde samordnade insatser på nationell nivå.

3. Grundförutsättningar för hanterandeplanen

Planen för att hantera allvarliga IT-incidenter utgår från de grundförutsättningar som finns inom det svenska krishanteringssystemet, det vill säga förutsättningarna för samverkan och koordinering knutet till enskilda aktörers ansvar och roller samt styrande principer.

3.1 Det svenska krishanteringssystemet

Svensk krishantering bygger på samverkan. Alla aktörer måste vid händelse av en kris kunna agera tillsammans och samverka kring beslut och insatser. Det gäller oavsett region eller affärsområde: privat näringsliv, polis, räddningstjänst, beslutsfattare inom kommun, länsstyrelse eller statsledning.

Krishanteringssystemet inkluderar sektorsansvar, områdesansvar och verksamhetsansvar, indelat på kommunal nivå (lokalt), på länsstyrelse- och landstingsnivå (regionalt) och på central myndighets- och regeringsnivå (nationell nivå).

En kris hanteras till en början i dess omedelbara närhet, samtidigt som det finns resurser beredda på regional och nationell nivå om händelserna blir för omfattande för att hantera på lokal nivå. Detta innebär att kommunernas verksamhet är grunden för i stort sett all hanteringen av kriser. Under en kris ska länsstyrelsen i egenskap av geografiskt områdesansvarig på regional nivå stödja kommunen när det gäller samverkan mellan myndigheter, kommuner och andra aktörer. Länsstyrelsens stöd innebär inte någon förändring av övriga aktörers ansvar för att hantera krisen.

Krishanteringen på nationell nivå är regeringens ansvar. Regeringen hanterar strategiska frågor. Statsrådsberedningen leder och samordnar arbetet och regeringen får stöd under en kris genom att kansliet för krishantering tar fram en samlad lägesbild om hur enskilda händelser påverkar samhället i stort. Ansvaret för ledning och samordning av det praktiska arbetet ligger på berörda myndigheter.

3.2 Styrande principer

Svensk krishantering styrs av tre principer: *ansvarsprincipen*, *närhetsprincipen* och *likhetsprincipen*.

3.2.1 Ansvarsprincipen

Ansvarsprincipen är av grundläggande betydelse. I korthet innebär principen att den som har ansvar för en viss verksamhet under normala förhållanden även har samma ansvar under en kris. Någon krisledande aktör som tar över berörda aktörers ansvar finns inte.

Ansvarsprincipen har förstärkts under senare år, bland annat som ett resultat av ett antal händelser under 2000-talet, och inkluderar nu ett uttalat krav på samverkan. Berörda aktörer är skyldiga att stödja varandra vid en kris och därmed ta en aktivare roll i samhällets krisberedskap.

> *Varje myndighet, vars ansvarsområde berörs av en krissituation, skall vidta de åtgärder som behövs för att hantera konsekvenserna av denna. Myndigheterna skall samverka och stödja varandra vid en sådan krissituation (5 § KBF).*

I propositionen 2005/06:133 Samverkan vid kris – för ett säkrare samhälle formuleras även ett försiktighetskrav som inkluderar skyldigheten att agera utifrån ansvarsprincipen även vid osäkerhet:

> *Alla aktörer som berörs av en kris, direkt eller indirekt, och som kan bidra till att hantera konsekvenserna har ett ansvar att agera även i osäkra lägen (prop. 2005/06:133, s. 51).*

Detta innebär att en aktör inte ska kunna undvika att agera, eller inte behöva vidta förebyggande åtgärder bara för att någon annan aktör står som huvudansvarig (prop. 2005/06:133, s. 51).

För att ansvarsprincipen ska ge effekt även vid en kris, måste åtgärderna inom krisberedskap och skydd mot olyckor och kriser vara en del av en organisations verksamhet under normala förhållanden.

3.2.2 Närhetsprincipen

Närhetsprincipen innebär att en kris ska hanteras där den inträffar och ledas av dem som är närmast berörda och ansvariga. Krishanteringen bör endast lyftas till högre beslutsnivåer om det bedöms som nödvändigt.

> *En grund för enkla, tydliga och lättförståeliga kontaktvägar och strukturer skapas genom att den operativa hanteringen sker geografiskt och organisatoriskt så nära krisen som möjligt, […] (prop. 2005/06:133, s. 51)*

3.2.3 Likhetsprincipen

Likhetsprincipen innebär att en verksamhets organisation och lokalisering så långt som möjligt ska behållas vid en kris. Förändringar i organisationen ska inte vara större än vad som krävs för att hantera krisen.

> *[…] och att organisatoriska förändringar inte görs större än vad krisen kräver (prop. 2005/06:133 s. 51).*

3.3 Ansvar och roller

Myndigheter, landsting och kommuner har i författning ett utpekat ansvar inom krisberedskapsområdet och inom informationssäkerhetsarbetet.

3.3.1 Grundkrav på alla aktörer avseende krisberedskap

Det ställs krav på såväl statliga myndigheter som på kommuner och landsting att vidta åtgärder i samband med en krissituation som har koppling till aktörens ansvarsområde eller geografiska områdesansvar (5 § KBF, 7 § 5 kap. LEH). Dessutom finns det ett antal utpekade myndigheter med särskilt ansvar inom krisberedskapsområdet (11 § KBF). Vad gäller de privata aktörerna utgörs det främsta verktyget av privat–offentlig samverkan eftersom det saknas motsvarande lagstadgade krav på krisberedskap för denna typ av aktörer.

Alla myndigheter har genom 30 § förordning (2006:942) om krisberedskap och höjd beredskap ett ansvar för att arbeta med informationssäkerhet:

> *Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. (30 § KBF)*

Tabell 2 nedan visar kraven inom krisberedskapen som berör kommuner såväl som myndigheter, på central och regional nivå.

Tabell 2. Grundkrav inom krisberedskap

GRUNDKRAV INOM KRISBEREDSKAP	
Aktörer	***Ansvar***
Centrala myndigheter	Varje myndighet, vars ansvarsområde berörs av en krissituation, skall vidta de åtgärder som behövs för att hantera konsekvenserna av denna. Myndigheterna skall samverka och stödja varandra vid en sådan krissituation. (5 § KBF)
Kommuner och landsting	Kommuner och landsting skall analysera vilka extraordinära händelser i fredstid som kan inträffa i kommunen respektive landstinget och hur dessa händelser kan påverka den egna verksamheten. Resultatet av arbetet skall värderas och sammanställas i en risk- och sårbarhetsanalys. (1 st. 1 § 2 kap. LEH)
	Kommuner och landsting skall vidare, med beaktande av risk- och sårbarhetsanalysen, för varje ny mandatperiod fastställa en plan för hur de skall hantera extraordinära händelser. (2 st. 1 § 2 kap. LEH)
	I kommuner och landsting skall det finnas en nämnd för att fullgöra uppgifter under extraordinära händelser i fredstid (krisledningsnämnd). […] (2 § 2 kap. LEH)

	Kommuner skall inom sitt geografiska område i fråga om extraordinära händelser i fredstid verka för att 1. olika aktörer i kommunen samverkar och uppnår samordning i planerings- och förberedelsearbetet, 2. de krishanteringsåtgärder som vidtas av olika aktörer under en sådan händelse samordnas, och 3. informationen till allmänheten under sådana förhållanden samordnas. (7 § 2 kap. LEH)
	Kommuner och landsting skall ansvara för att förtroendevalda och anställd personal får den utbildning och övning som behövs för att de skall kunna lösa sina uppgifter vid extraordinära händelser i fredstid. (8 § 2 kap. LEH)
	Kommuner och landsting skall hålla den myndighet som regeringen bestämmer informerad om vilka åtgärder som vidtagits enligt detta kapitel och hur åtgärderna påverkat krisberedskapsläget. Kommunen och landstinget skall vid en extraordinär händelse i fredstid ge den myndighet som regeringen bestämmer lägesrapporter och information om händelseutvecklingen, tillståndet och den förväntade utvecklingen samt om vidtagna och planerade åtgärder. (9 § 2 kap. LEH)
Länsstyrelser	Länsstyrelsen skall inom sitt geografiska område i fråga om sådana situationer som avses i 9 § vara en sammanhållande funktion mellan lokala aktörer, som exempelvis kommuner, landsting och näringsliv, och den nationella nivån, samt verka för att: • regionala risk- och sårbarhetsanalyser sammanställs, • nödvändig samverkan inom länet och med närliggande län sker kontinuerligt, • under en kris samordna verksamhet mellan kommuner, landsting och myndigheter, • informationen till allmänheten och företrädare för massmedia under sådana förhållanden samordnas, och • efter beslut av regeringen prioritera och inrikta statliga och internationella resurser som ställs till förfogande. (7 § KBF)

3.3.2 Särskilt ansvar inom krisberedskap

För att möta olika behov på krisberedskapsområdet har vissa myndigheter utöver grundkravet ett särskilt ansvar. Detta ansvar innebär att myndigheterna ska planera och vidta förberedelser för att skapa förmåga att hantera en kris, förebygga sårbarheter och motstå hot och risker (11 § KBF). För att främja en helhetssyn ska krisberedskapsplaneringen för dessa myndigheter bedrivas inom samverkansområden. Syftet är att i samverkan med berörda aktörer komma fram till hur krisberedskapen inom ett område och mellan områden bör stärkas. Vilka myndigheter som är utpekade i förordningen, samt vilket samverkansområde de hör till, framgår av nedanstående Tabell 3. Av Tabell 4 framgår vad det särskilda ansvaret består i.

Tabell 3. Myndigheter med särskilt ansvar enligt 11 § KBF

UTPEKADE MYNDIGHETER ENLIGT 11 § KBF	
Samverkansområden	***Myndigheter med särskilda uppgifter inom samverkansområdena***
Teknisk infrastruktur	Affärsverket svenska kraftnät
	Elsäkerhetsverket
	Myndigheten för samhällsskydd och beredskap
	Post- och telestyrelsen
	Statens energimyndighet
	Livsmedelsverket
Transporter	Sjöfartsverket
	Statens energimyndighet
	Trafikverket
	Transportstyrelsen
Farliga ämnen	Kustbevakningen
	Livsmedelsverket
	Myndigheten för samhällsskydd och beredskap
	Rikspolisstyrelsen
	Smittskyddsinstitutet
	Socialstyrelsen
	Statens jordbruksverk
	Statens veterinärmedicinska anstalt
	Strålsäkerhetsmyndigheten
	Tullverket
Ekonomisk säkerhet	Finansinspektionen
	Försäkringskassan
	Pensionsmyndigheten
	Riksgäldskontoret
	Skatteverket
Geografiskt områdesansvar	Länsstyrelserna
	Myndigheten för samhällsskydd och beredskap
Skydd, undsättning och vård	Kustbevakningen
	Myndigheten för samhällsskydd och beredskap

	Rikspolisstyrelsen
	Sjöfartsverket
	Socialstyrelsen
	Transportstyrelsen
	Tullverket

I samverkansområdena deltar fler myndigheter än de som av regeringen har ett särskilt utpekat ansvar enligt krisberedskapsförordningen. För närvarande deltar Försvarsmakten, FRA, Fortifikationsverket, Lantmäteriet, SMHI och FOI.

Tabell 4. De utpekade myndigheternas särskilda ansvar enligt bilaga till KBF

SÄRSKILT ANSVAR FÖR UTPEKADE MYNDIGHETER ENLIGT 11 § KBF	
Aktörer	***Ansvar***
Utpekade myndigheter, centrala och regionala	Myndigheterna ska särskilt 1. samverka med länsstyrelserna i deras roll som områdesansvarig myndighet, 2. samverka med övriga statliga myndigheter, kommuner, landsting, sammanslutningar och näringsidkare som är berörda, 3. beakta det samarbete som sker inom Europeiska Unionen och internationella forum i frågor som rör samhällets krisberedskap, 4. beakta behovet av forsknings- och utvecklingsinsatser och annan kunskapsinhämtning såsom erfarenhetsåterföring av inträffade händelser, 5. beakta behovet av säkerhet och kompatibilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete, 6. beakta behovet av deltagande i det samhällsgemensamma radiokommunikationssystemet för skydd och säkerhet (Rakel) som förvaltas av Myndigheten för samhällsskydd och beredskap, och 7. informera Myndigheten för samhällsskydd och beredskap om sin övningsverksamhet för att den ska kunna samordnas med den övningsverksamhet som Myndigheten för samhällsskydd och beredskap planerar. Myndigheterna ska vidare delta i den övningsverksamhet som berör deras ansvarsområde. (11 § KBF)
	Myndigheten för samhällsskydd och beredskap ska vid behov till Regeringskansliet lämna förslag på förändringar av vilka myndigheter som ska ha en tjänsteman i beredskap med uppgift att initiera och samordna det inledande arbetet för att upptäcka,

	verifiera, larma och informera vid allvarliga kriser. (12 § KBF) 19 centrala myndigheter har inrättat TiB och ledningsfunktioner enligt regeringsbeslut (Tjänsteman i beredskap och ledningsfunktion enligt förordningen (2006:942) om krisberedskap och höjd beredskap, Fö2007/436/CIV, 2007-06-07), samt ytterligare åtta efter ett kompletterande beslut (Fö2008/552/SSK, 2008-10-09). Även länsstyrelserna har TiB och ledningsfunktion (enligt regeringsbeslut den 29 mars 2007 om Förordning (2007:130) om ändring i förordningen (2002:864) med länsstyrelseinstruktion).
	Myndigheter med ansvar enligt 11 § skall, när en situation som avses i 9 § andra stycket uppstår, hålla regeringen informerad om händelseutvecklingen, tillståndet, den förväntade utvecklingen och tillgängliga resurser inom respektive ansvarsområde samt om vidtagna och planerade åtgärder. 15 § Varje myndighet ska efter förfrågan från Regeringskansliet eller Myndigheten för samhällsskydd och beredskap lämna den information som behövs för samlade lägesbilder. (14-15 § KBF)

3.3.3 Särskilt ansvar för informationssäkerhet

Några statliga myndigheter har ett särskilt ansvar för olika delar av arbetet med samhällets informationssäkerhet. De flesta av dessa statliga myndigheter ingår i Samverkansgruppen för informationssäkerhet (SAMFI). I SAMFI ingår

- Myndigheten för samhällsskydd och beredskap (MSB)
- Post- och telestyrelsen (PTS)
- Försvarets radioanstalt (FRA)
- Försvarets materielverk (FMV)
- Försvarsmakten (FM)
- Rikspolisstyrelsen (RPS) som representeras genom Rikskriminalpolisen (RKP) och Säkerhetspolisen (Säpo).

SAMFI ska genom att samverka och utbyta information stödja de aktuella myndigheternas uppdrag inom informationssäkerhetområdet. Visionen är att *verka för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.* SAMFI-

myndigheternas och Datainspektionens uppdrag beskrivs i tabell 5 nedan. Informationen kommer från instruktioner och annan relevant författning.

Tabell 5. Myndigheter med särskilt ansvar för informationssäkerhet

MYNDIGHETER MED SÄRSKILT ANSVAR FÖR INFORMATIONSSÄKERHET	
Aktörer	***Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning***
Myndigheten för samhällsskydd och beredskap (MSB)	**Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap** 1 § Myndigheten för samhällsskydd och beredskap har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris. 7 § Myndigheten ska ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att 1. samordna krishanteringsåtgärderna, 2. samordna information till allmänhet och media, 3. effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och 4. samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder. Myndigheten ska ha förmågan att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser. 11 a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället. Myndigheten ska vidare svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. Myndigheten ska i detta arbete: 1. agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs

	för att avhjälpa eller lindra effekter av det inträffade, 2. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och 3. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa. Förordning (2010:1901). **Förordning (2006:942) om krisberedskap och höjd beredskap** 31 § Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut, Fortifikationsverket, Totalförsvarets rekryteringsmyndighet, Myndigheten för samhällsskydd och beredskap och Regeringskansliet ska ha säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap beslutar vilka övriga myndigheter som ska ha säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap beslutar även vilka företag som efter överenskommelse ska få tillgång till säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap får därutöver ingå avtal om tilldelning med kommuner och organisationer som har behov av säkra kryptografiska funktioner. 34 § Myndigheten för samhällsskydd och beredskap får 1. meddela de ytterligare föreskrifter som behövs för verkställigheten av 9 § om risk- och sårbarhetsanalyser, 2. meddela föreskrifter om sådana säkerhetskrav som avses i 30 a § med beaktande av nationell och internationell standard, samt 3. meddela de ytterligare föreskrifter som behövs för verkställigheten av 16-20 samt 33 §§, utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket.
Post och telestyrelsen (PTS)	**Förordning (2007:951) med instruktion för Post- och telestyrelsen** 1 § Post- och telestyrelsen är förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. 4 § Post- och telestyrelsen har till uppgift att 1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att tillse att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska

	kommunikationstjänster, 7. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker, 10. meddela föreskrifter enligt förordningen (2003:396) om elektronisk kommunikation, 14. utöva tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer samt meddela föreskrifter enligt förordningen (2000:833) om kvalificerade elektroniska signaturer, 15. utöva tillsyn enligt lagen (2006:24) om nationella toppdomäner för Sverige på Internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på Internet, och 16. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, samt verka för ökad krishanteringsförmåga. 17. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer, och 18. lämna råd och stöd till myndigheter, kommuner och landsting samt företag, organisationer och andra enskilda i frågor om nätsäkerhet. Förordning (2010:1913). 7 § Post och telestyrelsen ska 3. vara det behöriga organ som får begära råd och stöd enligt Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet. 5. delta i arbetet i internationella organ i frågor som rör Internets förvaltning genom att vid behov företräda Sverige i dessa organ och genom att bereda ärenden med intressenter på nationell nivå. 8 § Post- och telestyrelsen får genom upphandling 4. stärka samhällets beredskap mot allvarliga störningar av elektronisk kommunikation och posttjänster i fred.
Rikspolisstyrelsen (RPS) och Säkerhetspolisen (Säpo)	**Förordning (1989:773) med instruktion för Rikspolisstyrelsen** 3 § Rikspolisstyrelsen svarar för samordningen av 5. Polisens beredskap för åtgärder vid incidenter i

	informationstekniska system (IT-incidenter) **Förordning (2002:1050) med instruktion för Säkerhetspolisen** 2 § Säkerhetspolisen har till uppgift att inom Rikspolisstyrelsen leda och bedriva polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet. Säkerhetspolisen skall även, utöver vad som anges i första stycket, inom Rikspolisstyrelsen leda och bedriva polisverksamhet när det gäller 1. terrorismbekämpning **Polislag (1984:387)** 2 § Till polisens uppgifter hör att 1. förebygga brott och andra störningar av den allmänna ordningen eller säkerheten, 3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal, 4. lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen, Andra myndigheter ska ge polisen stöd i dess arbete. **Säkerhetsskyddslag (1996:627)** 5 § I verksamhet där lagen gäller skall det säkerhetsskydd finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Säkerhetsskyddet skall utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar. 6 § Med säkerhetsskydd avses 1. skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet, 2. skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, och 3. skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet. Lag (2009:464). 7 § Säkerhetsskyddet skall förebygga

	1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet), Säkerhetsskyddet skall även i övrigt förebygga terrorism. 9 § Vid utformningen av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt. 33 § Regeringen eller den myndighet som regeringen utser meddelar de närmare föreskrifter som behövs för lagens tillämpning. **Säkerhetsskyddsförordning (1996:633)** 43 § Rikspolisstyrelsen får meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om förfarandet vid registerkontroll. Sådana föreskrifter som avser kontroll av personal vid Försvarsmakten skall beslutas efter samråd med Försvarsmakten. 44 § Rikspolisstyrelsen och Försvarsmakten får meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) för sina respektive tillsynsområden enligt 39 §. Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket. 44 a § Rikspolisstyrelsen får, utöver vad som sägs i 43 §, meddela föreskrifter om verkställighet av säkerhetsskyddslagen (1996:627) för sitt tillsynsområde enligt 40 a §. Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket. 45 § Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Om det behövs skall myndigheterna innan dess samråda med den myndighet som enligt 43 och 44 §§ meddelar föreskrifter för myndighetens område. Myndigheternas föreskrifter får avvika från föreskrifterna enligt 43 och 44 §§ endast om detta har medgivits av den myndighet som har meddelat dessa föreskrifter.
Försvarets radioanstalt (FRA)	**Förordning (2007:937) med instruktion för Försvarets radioanstalt** 4 § Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet. Försvarets radioanstalt får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från

	sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt ska särskilt kunna 1. stödja insatser vid nationella kriser med IT-inslag, 2. medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system, 3. genomföra IT-säkerhetsanalyser, och 4. ge annat tekniskt stöd. Försvarets radioanstalt ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. **Förordning (2006:942) om krisberedskap och höjd beredskap** 32 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 31 § ska ha säkra kryptografiska funktioner tilldelas sådana.
Försvarets materielverk (FMV)	**Förordning (2007:854) med instruktion för Försvarets materielverk** 5 § Vid Försvarets materielverk finns ett certifieringsorgan som ska upprätta och driva en certifieringsordning för säkerhet i IT-produkter och system. Försvarets materielverk ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat.
Försvarsmakten (FM)	**Förordning (2007:1266) med instruktion för Försvarsmakten** 3 b § Försvarsmakten ska särskilt 3. leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information, 4. biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet, 33 § Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret, förutom i fråga om verkställigheten av 33 § förordningen (2006:942) om krisberedskap och höjd beredskap. **Säkerhetsskyddslag (1996:627)** 33 § Regeringen eller den myndighet som regeringen

	utser meddelar de närmare föreskrifter som behövs för lagens tillämpning. (1996:627) **Säkerhetsskyddsförordning (1996:633)** 44 § Rikspolisstyrelsen och Försvarsmakten får meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) för sina respektive tillsynsområden enligt 39 §. Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket. 45 § Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Om det behövs skall myndigheterna innan dess samråda med den myndighet som enligt 43 och 44 §§ meddelar föreskrifter för myndighetens område. Myndigheternas föreskrifter får avvika från föreskrifterna enligt 43 och 44 §§ endast om detta har medgivits av den myndighet som har meddelat dessa föreskrifter. **Förordning (2006:942) om krisberedskap och höjd beredskap** 32 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 31 § ska ha säkra kryptografiska funktioner tilldelas sådana.
Datainspektionen (DI), inte med i SAMFI	**Förordning (2007:975) med instruktion för Datainspektionen** 1 § Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Myndigheten ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen (1998:204). Myndigheten ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.

	Personuppgiftsförordning (1998:1191) 2 § Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen (1998:204). Datainspektionens föreskriftsrätt enligt personuppgiftslagen (1998:204) framgår av personuppgiftsförordningen (1998:1191).

3.3.4 Privata aktörer med ansvar för samhällsviktig verksamhet

I dag ägs och drivs större delen av samhällsviktig verksamhet och infrastruktur av privata aktörer. Ibland befinner sig dessa aktörer utanför Sveriges gränser. Även om denna typ av aktörer inte omfattas av det formella ansvaret för krisberedskap och informationssäkerhet innebär det inte att de är utan ansvar. Det finns i många fall specifik lagstiftning som styr aktörernas ansvar, inte minst gentemot slutkonsumenterna. Ett exempel som kan nämnas i detta sammanhang är ellagen (1997:857) som bland annat fastställer i 9 a § 3 kap. att ett elavbrott inte får vara längre än 24 timmar.

4. Nationell hanterandeplan för allvarliga IT-incidenter

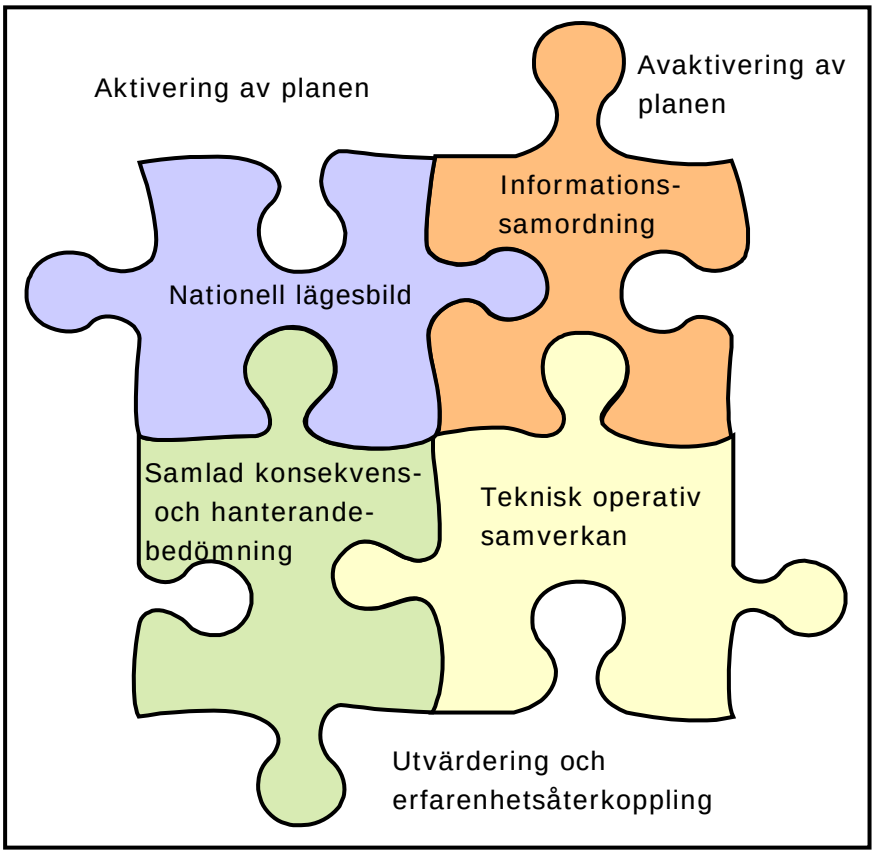
Sverige behöver ett ramverk som *tillförsäkrar en koordinerad hantering* av allvarliga IT-incidenter. Det är angeläget att skapa goda möjligheter för att myndigheter och andra aktörer ska kunna samordna åtgärder och insatser. Enligt de styrande principerna inom krisberedskap ligger ansvaret för att hantera en incident på varje enskild aktör. Planen är till för att underlätta för varje aktör att skapa sig en bild av vad som har hänt och vilka förutsättningar som den aktuella incidenten medför. Detta uppnås genom att tillsammans med andra aktörer ta fram en gemensam lägesbild. Andra aktiviteter som aktörerna med fördel kan göra tillsammans är att utåt informera om händelsen och sinsemellan dela information om hur man rent tekniskt kan avhjälpa incidenten. Samhället och enskilda har mycket att vinna på att aktörer och sektorer samverkar, vilket MSB har i uppdrag att stödja. Hanterandeplanens huvuddel består därför av fyra samverkansprocesser. De syftar till att skapa bästa möjliga förutsättningar inom de områden där samverkan bedömts vara av störst betydelse vid hanteringen av en allvarlig IT-incident. Samverkansprocesserna är

- nationell lägesbild
- informationssamordning
- samlad konsekvens- och hanterandebedömning
- teknisk operativ samverkan.

4.1 Samverkansprocesser i fokus

Samverkansprocesserna har utformats med tidigare nämnda grundförutsättningar i åtanke. Processerna är separata men kopplade komponenter, vilket illustreras av Figur 2 nedan. Ramen som omsluter de olika processerna i illustrationen består av rutiner för aktivering och avslut av hanterandeplanen samt utvärdering och erfarenhetsåterkoppling.

Under hanteringen av en allvarlig IT-incident kommer till större delen av tiden dessa processer att fortgå parallellt. En djupare beskrivning av processerna följer i kapitel 4.3–4.6.



Figur 2. Hanterandeplanens samverkansprocesser

Nationell lägesbild

Under en krissituation som påverkar hela nationen finns det många informationskällor och informationsmottagare. Lägesinformation utgör en nödvändig förutsättning för att alla inblandade aktörer ska förstå situationen och kunna hantera den. För att aktörerna samordnat ska kunna planera åtgärder och diskutera resursbehov och resursfördelning måste aktörernas separata lägesinformation också sammanställas i en gemensam lägesbild. Den nationella lägesbilden av allvarliga IT-incidenter tas fram inom ramen för den redan nu tillämpade samverkansprocessen för hantering av kriser vid MSB. Målet för denna process är att underlätta för berörda aktörer att få en gemensam lägesbild.

Informationssamordning

En allvarlig IT-incident leder oundvikligen till ett stort intresse från media och allmänheten, och ett tydligt behov av information. I syfte att minimera skadeverkningarna av IT-incidenten och i största möjliga mån begränsa felaktiga och potentiellt skadliga spekulationer är det viktigt att samordna informationen till allmänhet och media. Skadan kan till exempel minskas genom att aktörerna går ut med råd och rekommendationer till allmänheten. Informationssamordningen är tänkt att ske inom ramen för den informations-samordningsprocess som MSB ansvarar för och som i nuläget involverar ett antal tematiskt formerade informatörsnätverk. Informatörsnätverken består av

informatörer hos centrala myndigheter och kan utökas vid behov. Målet för denna process är att nå ut till allmänheten med ett samlat budskap i rätt tid.

Samlad konsekvens- och hanterandebedömning

Det finns ett behov av att sammanföra den IT-relaterade lägesbilden med den övergripande och samhällsinriktade nationella lägesbilden som MSB enligt instruktionen har ett utpekat ansvar för att upprätthålla och rapportera till regeringen (7 § Förordning (2008:1002)). Den IT-relaterade lägesbilden tas i huvudsak fram genom samarbetet mellan berörda aktörer inom den nationella operativa samverkansfunktionen för informationssäkerhet (NOS) vid MSB.

MSB löser genom NOS regeringens inriktning som uttrycks i proposition 2010/11:1 utgiftsområde 6 (s. 83):

> *För att förbättra samhällets förmåga att förebygga och hantera allvarliga IT-incidenter anser regeringen att det krävs en mer sammanhållen struktur på området. Ett viktigt medel för att uppnå detta mål är inrättandet av en nationell samverkansfunktion för informationssäkerhet. Regeringen anser därför att Myndigheten för samhällsskydd och beredskap i samverkan med berörda myndigheter bör verka för en sådan funktion.*

Samarbetet inom NOS stödjer det arbete som sker vid MSB med att tillsammans med aktörerna som berörts av krisen ta fram en kvalitativ och samlad konsekvens- och hanterandebedömning med IT-kompetens. Detta resulterar i möjligheten att få fram en bedömning som tar hänsyn till såväl de IT-relaterade aspekterna som samhället i stort. Konsekvens- och hanterande-bedömningen kan ligga till grund för regeringens beslutsfattande och kontakter med omvärlden. Den kan också ligga till grund för aktörerna som ska fatta beslut inom sitt respektive verksamhetsansvar. Målet för denna process är att skapa en fördjupad och kompletterad konsekvensbaserad lägesbild ur ett samhälleligt perspektiv.

Teknisk operativ samverkan

Samverkan är ofta en förutsättning för att kunna hantera de tekniska aspekterna av allvarliga IT-incidenter på ett effektivt sätt. Att dela information om bland annat identifierade sårbarheter, skadlig kod samt strategier för avhjälpande nationellt och internationellt kan i många fall förkorta krisförloppet. När det gäller internationell samverkan är olika CERT-organisationer en viktig resurs. CERT står för Computer Emergency Response Team. Det är viktigt att påpeka att ansvaret för denna process ligger på samtliga aktörer som har ansvar för att rent tekniskt avhjälpa IT-relaterade incidenter. Målet för denna process är att på ett effektivt sätt nå godtagbar funktionalitet.

4.2 Hanterandeplanens ram

Det finns ett antal aktiviteter och stödjande rutiner som är relevanta för hanterandeplanen men som går utanför de samverkansprocesser som är själva

kärnan. Dessa är aktivering respektive avaktivering av planen samt utvärdering och erfarenhetsåterkoppling av hanteringen av en allvarlig IT-incident.

4.2.1 Aktivering av hanterandeplanen

Beslut om att aktivera den nationella hanterandeplanen för allvarliga IT-incidenter tas när det

- finns ett påtagligt hot om eller överhängande risk för en allvarlig IT-incident
- när en allvarlig IT-incident inträffat (och denna inte redan föranlett att hanterandeplanen aktiverats).

Beslutet fattas av ansvarig person vid MSB:s avdelning för samordning och insats, inom ramen för befintligt mandat. För att ett sådant beslut ska tas krävs att information inkommit till MSB. Informationen kan exempelvis komma från tjänsteman i beredskap (TiB) eller genom att MSB i sin ordinarie omvärlds-bevakning själva har identifierat något som påkallar detta beslut. För tydlighetens skull är det viktigt att klargöra att behovet av att aktivera hanterandeplanen givetvis kan påkallas av samtliga aktörer. Den inter-nationella dimensionen är viktig och information kan även inkomma via Regeringskansliets TiB till MSB, eller via en europeisk eller internationell CERT-organisation till CERT-SE.

Att MSB aktiverar hanterandeplanen innebär, beroende på händelsens art, att MSB som minst höjer bevakningen och informerar berörda aktörer[1] om detta. Om planen aktiverats innan en allvarlig IT-incident inträffat ökar MSB bevakningen genom bland annat ökad aktivitet i samarbetet inom NOS. MSB hämtar också information från relevanta parter för att skapa en uppfattning om den pågående IT-incidenten. Syftet med denna fas (som kan betraktas som en begränsad eskaleringsmekanism) är att skapa förutsättningar för att i största möjliga utsträckning agera proaktivt.

Om planen aktiverats som svar på en inträffad allvarlig IT-incident fattar MSB ett internt beslut om en så kallad samordningshändelse varvid den process som beskrivs under ”nationell lägesbild” (kapitel 4.3) tar vid (se vidare beskrivningen nedan).

Ett beslut om att planen aktiverats innebär inte några krav på att andra myndigheter eller aktörer ska aktivera sina respektive krishanteringsfunktioner. Beslut om detta fattas av respektive aktör inom ramen för deras verksamhetsansvar. Däremot preciseras i planen det som förväntas av berörda aktörer när det gäller informationsdelning och samverkan inom planens olika processer.

[1] Informationen går till berörda myndigheter via deras TiB-funktion.

4.2.2 Avaktivering av planen

Då parametrarna för en allvarlig IT-incident (se avsnitt 2.1) inte längre är uppfyllda tar ansvarig person på MSB beslut om att avaktivera hanterande-planen. Trots att planen är avaktiverad kan delprocesser fortgå. Efter en incident finns det exempelvis ett allmänt informationsbehov även långt efter det att konsekvenserna av incidenten klingat av.

4.2.3 Utvärdering av planen

En viktig del i planen är att skapa goda förutsättningar för en systematisk utvärdering.

Utvärderingsinsatsen ska vara proportionerlig till det som ska utvärderas. Därför kan den vara mer eller mindre omfattande.

För att säkerställa fortlöpande och systematisk utvärdering har en särskild utvärderingsrutin skapats. När MSB fattar beslut om att aktivera den nationella hanterandeplanen för allvarliga IT-incidenter fattar de samtidigt beslut om att sätta igång en utvärdering.

Det är viktigt att slutsatser och erfarenheter återkopplas till berörda aktörer i systemet efter en utvärdering. Men det är också viktigt att informationen sammanställs så att den kan användas vid en revidering av den nationella hanterandeplanen.

4.2.4 Rutiner som är kopplade till hanterandeplanens ram

Tabell 6. Rutiner som är kopplade till hanterandeplanens ramprocesser

Stödjande rutiner	Aktivering av den nationella hanterandeplanen för allvarliga IT-incidenter Informering om aktivering av plan till berörda aktörer (via TiB) Avaktivering av hanterandeplanen Beslut om utvärdering Utvärdering och erfarenhetsåterkoppling till berörda aktörer

De uppgifter som är kopplade till planens ram samt olika aktörers roller beskrivs i tabellen nedan.

Tabell 7. Uppgifter kopplade till hanterandeplanens ram

Aktör	Uppgifter kopplade till hanterandeplanens ram
Myndigheten för samhällsskydd och beredskap	Beslut om aktivering av hanterandeplanen för allvarliga IT-incidenter Utvärdering av samordningshändelsen och erfarenhetsåterkoppling till berörda aktörer Beslut om avaktivering av den nationella hanterandeplanen för allvarliga IT-incidenter Informering om aktivering av plan till berörda aktörer (via TiB)

Övriga	Incidentrapportering[2] Påkalla behovet, när sådant föreligger, av att aktivera hanterandeplanen Stöd i utvärderingen av hanteringen

Nationell lägesbild

Nationell lägesbild är en av de mest grundläggande av samverkansprocesserna i hanterandeplanen eftersom den i många fall är en förutsättning för att aktörerna ska kunna fatta samordnade och välgrundade beslut. Nedan följer en schematisk uppställning av syfte samt de olika komponenter som ingår i processen.

Tabell 8. Sammanfattande tabell för processen *nationell lägesbild*

Överordnat mål	Skapa en gemensam lägesbild för att ge möjlighet till koordinerat agerande och därmed ändamålsenlig användning av samhällets resurser i hanteringen av allvarliga IT-incidenter
Uppnås genom	Samverkanskonferenser Aktörsspecifika aktiviteter Övriga aktiviteter
Berörda parter	SAMFI-myndigheterna Centrala myndigheter Länsstyrelser Kommuner Befintliga samverkansforum Privat näringsliv Övriga
Sammankallande till samverkanskonferenser	MSB
Deltagande parter i samverkanskonferenser	SAMFI-myndigheterna Centrala myndigheter Länsstyrelser Eventuellt inbjudna experter Övriga
Exempel på stödjande verktyg	WIS RAKEL Kallelse via SOS-alarm

[2] I nuläget finns inget krav på obligatorisk incidentrapportering men det pågår ett regeringsuppdrag med syfte att utreda hur ett system för obligatorisk IT-incidentrapportering kan utformas. Mot bakgrund av detta återfinns denna skrivning i uppgiftsbeskrivningen. Notera även att en obligatorisk incidentrapportering inte ersätter brottsanmälan till polisen.

	Stödsystem för obligatorisk incidentrapportering (kommande) System för omvärldsbevakning m.m.
Stödjande rutiner	Informerande av tekniska kompetensnätverk Samverkanskonferens Incidentrapportering Rapportering till regeringen Rapportering till berörda aktörer (nationellt och internationellt)

Processen med att skapa en nationell lägesbild kopplas i hanterandeplanen till den redan etablerade samverkansprocessen för kriser i samhället som upprätthålls av MSB. Detta innebär att aktörerna kan använda rutiner som redan är upparbetade. Det som skiljer hanteringen av en allvarlig IT-incident från en annan typ av kris är framför allt *tidsaspekten,* både avseende möjligt händelseförlopp och de krav detta ställer på snabbt agerande från inblandade parter.

En annan aspekt som innebär en utmaning är kopplad till möjligheten att en allvarlig IT-incident *sprider sig över såväl flera sektorer som geografiska gränser* – något som också får följder för den nationella lägesbilden. Det är troligt att ett större antal aktörer behöver vara med i samverkanskonferenserna för att skapa en mer komplett lägesbild.

En viktig förutsättning för arbetet med att ta fram en nationell lägesbild är att tydliggöra aktörernas roller i denna process och vad de förväntas kunna bidra med. Tabell 9 nedan beskriver olika aktörers roller i samverkansprocessen nationell lägesbild.

Tabell 9. Uppgifter kopplade till samverkansprocessen nationell lägesbild

Aktör	**Uppgifter kopplade till samverkansprocessen nationell lägesbild**
Myndigheten för samhällsskydd och beredskap	Beslut om samordningshändelse Kallelse till och genomförande av samverkanskonferens(er) Sammanställande av nationell lägesbild Rapportering av nationell lägesbild till regeringen Rapportering av nationell lägesbild till aktörerna i systemet Beslut om att informera relevanta tekniska kompetensnätverk Beslut om avslut av samordningshändelsen
SAMFI-myndigheterna	Informationsdelning avseende lägesbild, konsekvenser, vidtagna åtgärder och behov av resurser Obligatorisk incidentrapportering av inträffade IT-

	incidenter till MSB Deltagande i samverkanskonferenser EV. resursförstärkning av den nationella samverkansfunktionen för informationssäkerhet
Centrala myndigheter	Informationsdelning avseende lägesbild, konsekvenser, vidtagna åtgärder och behov av resurser Obligatorisk inrapportering av inträffade IT-incidenter till MSB Deltagande i samverkanskonferenser
Länsstyrelser	Genomförande av regionala samverkanskonferenser Sammanställning av regional lägesbild Informationsdelning avseende lägesbild, konsekvenser, vidtagna åtgärder och behov av resurser Frivillig inrapportering av inträffade IT-incidenter till MSB Deltagande i samverkanskonferenser
Kommuner	Informationsdelning avseende lägesbild, konsekvenser, vidtagna åtgärder och behov av resurser Deltagande i regionala samverkanskonferenser
Befintliga samverkansforum	Informationsdelning
Privat näringsliv	Informationsdelning via sektorsansvarig myndighet och länsstyrelsen Frivillig inrapportering av inträffade IT-incidenter till MSB Ev. deltagande i samverkanskonferenser Ev. resursförstärkning av den nationella samverkansfunktionen för informationssäkerhet (avseende operatörer av samhällsviktiga funktioner och infrastrukturer)
Övriga	Informationsdelning

4.3 Informationssamordning

Information är ett viktigt redskap vid hanteringen av alla former av kriser. Det har visat sig vara av avgörande betydelse att kunna samordna informationen till allmänheten i syfte att ge en enhetlig bild av konsekvenser, berörda aktörer, behov av åtgärder och händelseförlopp. Det finns sedan tidigare väl upparbetade kontakter mellan olika tematiska informatörsnätverk bestående av informatörer på flera centrala myndigheter. I händelse av en kris kallar MSB samman dessa till en informationssamordningskonferens. Denna hålls vanligtvis i anslutning till de så kallade samverkanskonferenserna och

informatörerna sitter ofta med under dessa för att ta del av lägesrapporteringen.

Tabell 10. Informationssamordning

Överordnat mål	Samordnad och kvalitativ informationsspridning till allmänheten – ett samlat budskap i rätt tid!
Uppnås genom	Informationssamordningskonferenser och kommunikativa aktiviteter
Sammankallande	MSB
Kopplad process	Nationell lägesbild
Berörda parter	Informatörsnätverk och andra relevanta parter
Exempel på stödjande verktyg	www.krisinformation.se Myndighetsgemensam informationstjänst Presskonferens Text-tv Radio RAKEL SGSI VMA Myndighetsmeddelande m.m.
Stödjande rutiner	FAQ Underlag nationell lägesbild

En viktig aspekt kopplad till informationssamordningen är att det är informatörerna som ska svara på frågor – inte de som arbetar med att avhjälpa den pågående IT-relaterade krisen. Avlastas inte den tekniskt operativa personalen på detta sätt finns det risk för att arbetet med att informera olika aktörer inkräktar på det faktiska arbetet med att avhjälpa och begränsa konsekvenserna av incidenten.

Aktörernas ansvar och aktiviteter inom ramen för processen informationssamordning beskrivs i tabell 11.

Tabell 11. Uppgifter kopplade till samverkansprocessen informationssamordning

Aktör	**Uppgifter kopplade till samverkansprocessen informationssamordning**
Myndigheten för samhällsskydd och beredskap	Kallelse till och genomförande av informationssamordningskonferens(er) Publicering av överenskommet material via relevanta kanaler som exempelvis www.krisinformation.se Deltagande i diverse olika informationsrelaterade aktiviteter gemensamt med relevanta aktörer
Informatörsnätverk bestående av informatörer hos de centrala myndigheterna	Deltagande i informationssamordningskonferenser Deltagande i diverse olika informationsrelaterade aktiviteter gemensamt med relevanta aktörer Bidra med underlag till publicering via

och länsstyrelserna	www.krisinformation.se
Eventuellt andra relevanta parter (exempelvis berörda privata ägare eller operatörer av samhällskritisk infrastruktur)	Deltagande i informationssamordningskonferenser Deltagande i diverse olika informationsrelaterade aktiviteter gemensamt med relevanta aktörer

4.4 Samlad konsekvens- och hanterandebedömning

Förutom den nationella lägesbilden, som skapas av aktörerna i samverkanskonferenserna, behövs en fördjupad analys av konsekvenser och en bedömning av hanteringen (inklusive behov av specifika resurser). Processen samlad konsekvens- och hanterandebedömning utgår från den information som delats via samverkanskonferenserna. Analysen av situationen fördjupas genom att den IT-relaterade lägesbilden (som tas fram inom NOS) läggs samman med aktörernas sammanlagda lägesbild. För att analysera samhälleliga, mer långtgående konsekvenser av incidenten använder man också verktyg som MSB har, bland annat beroendesimuleringsverktyg. Sammantaget åstadkoms en mer kvalitativ analys och bedömning som ytterst tjänar såväl regeringen i dess beslutsfattande som övriga berörda aktörer.

En naturlig del i konsekvens- och hanterandebedömningen är att ge rekommendationer och varningar till representanter för samhällsviktiga verksamheter men även till allmänheten.

Tabell 12. Samlad konsekvens- och hanterandebedömning

Överordnat mål	En fördjupad och kompletterad konsekvensbaserad lägesbild ur ett samhälleligt perspektiv
Uppnås genom	Analys genomförd i regi av MSB med stöd av den nationella samverkansfunktionen för informationssäkerhet (NOS)
Kopplad process	Nationell lägesbild
Ansvarig	MSB
Berörda parter	SAMFI-myndigheterna CERT-SE Relevanta nätverk nationellt och internationellt Privata aktörer med ansvar för samhällsviktig verksamhets funktionalitet
Exempel på stödjande verktyg	Beroendesimuleringsverktyg RSA-db Övriga
Stödjande rutiner	Underlag enskilda konsekvensbedömningar

	Kontaktperson (liaison) med processen nationell lägesbild

Aktörernas uppgifter inom ramen för processen samlad konsekvens- och hanterandebedömning beskrivs i tabellen nedan.

Tabell 13. Uppgifter kopplade till processen *samlad konsekvens- och hanterandebedömning*

Aktör	Uppgifter kopplade till processen samlad konsekvens- och hanterandebedömning
Myndigheten för samhällsskydd och beredskap	Kontinuerlig uppdatering och analys av den nationella informationssäkerhetsrelaterade lägesbilden Samlad konsekvens- och hanterandebedömning Varna och informera samhällsviktiga aktörer och andra berörda Rapportering av den samlade konsekvens- och hanterandebedömningen till regeringen samt berörda aktörer Underlag till ansvarig för informationssamordningsprocessen för vidare diskussion och beslut
SAMFI-myndigheterna	Informationsdelning och analysstöd Ev. resursförstärkning av NOS
Relevanta nätverk nationellt och internationellt	Informationsdelning och analys Expertstöd inom ramen för existerande tekniska kompetensnätverk Ev. resursförstärkning av NOS
Privata aktörer med ansvar för samhällsviktig verksamhets funktionalitet	Informationsdelning Expertstöd inom ramen för existerande tekniska kompetensnätverk Ev. resursförstärkning av NOS

4.5 Teknisk operativ samverkan

När en allvarlig IT-incident inträffar är det de olika verksamheternas ordinarie personal som utgör basresursen för att praktiskt tekniskt hantera det inträffade. Basresursen utgörs exempelvis av tekniker, driftspersonal, systemutvecklare och IT-säkerhetsexperter. Denna basresurs riskerar att bli hårt ansträngd under en allvarlig IT-incident, vilket gör att det behövs olika nationella resurser som kan stödja hanteringen vid allvarligare IT-incidenter (exempelvis tekniska kompetensnätverk). En annan aspekt kopplad till det tekniska hanterandet av allvarliga IT-incidenter är behovet av samverkan och informationsdelning mellan aktörer som tekniskt operativt hanterar incidenten.

Den tekniskt operativa samverkan är av väsentlig betydelse för att avhjälpa allvarliga IT-incidenter. Även om respektive verksamhet ansvarar för den

tekniska hanteringen av det som äger rum inom dess verksamhetsansvar är det viktigt att dela information om exempelvis identifierade sårbarheter, hur den skadliga koden ser ut, möjliga patchar med mera. Det kan också uppstå ett behov av extra resurser (expertresurser). MSB verkar för att underlätta kontaktskapande mellan olika experter och mellan experter och mottagare av experthjälp. I bilaga E beskrivs MSB:s åtaganden för att stödja framväxten av tekniska kompetensnätverk som ett led i att förbättra samhällets förmåga att hantera allvarliga IT-incidenter. I det tekniska avhjälpandet är det viktigt att peka på betydelsen av internationell samverkan – inte minst mellan olika CERT-organisationer.

Tabell 14. Teknisk operativ samverkan

Överordnat mål	Återställning till godtagbar funktionalitet
Uppnås genom	Samverkan mellan berörda parter inom ramen för befintliga nationella och internationella nätverk
Kopplad process	Nationell lägesbild Samlad konsekvens- och hanterandebedömning
Ansvarig	Ansvariga aktörer inom ramen för respektive mandat
Berörda parter	SAMFI-myndigheterna CERT-SE Berörda aktörer (offentliga och privata) nationellt och internationellt
Exempel på stödjande verktyg	Tillgängliga kommunikationskanaler Säkra kryptografiska funktioner[3]
Stödjande rutiner	Informationsdelning (TLP) Operativt stöd Förmedling av kontakt med tekniska kompetensnätverk

Det som kan förväntas av olika berörda aktörer avseende teknisk operativ samverkan sammanfattas nedan.

Tabell 15. Uppgifter kopplade till samverkansprocessen *teknisk operativ samverkan*

Aktör	**Uppgifter kopplade till samverkansprocessen teknisk operativ samverkan**
Myndigheten för samhällsskydd och beredskap	Löpande lämna tekniska råd och stöd (CERT-SE) för avhjälpande av allvarliga IT-incidenter Vara Sveriges kontaktpunkt gentemot liknande europeiska och internationella organisationer (CERT-SE)

[3] Delning av känslig information mellan samverkande myndigheter bör skyddas med hjälp av säkra kryptografiska funktioner, både för att behålla konfidentialitet och riktighet men även, vilket kanske är särskilt viktigt i det här fallet, för att garantera att informationen kommer från en betrodd avsändare.

	Varna och informera samhällsviktiga verksamheter, kritisk infrastruktur och andra relevanta aktörer (NOS) Rekommendera vissa typer av insatser och resurser
SAMFI-myndigheter	Informationsdelning Operativt stöd i tekniskt hänseende (främst FRA, Säpo och FM. Bedömning från fall till fall)
Övriga ansvariga aktörer inom ramen för deras respektive mandat	Informationsdelning

5. Förvaltning av hanterandeplanen för allvarliga IT-incidenter

5.1 Ägarskap

Hanterandeplanen för allvarliga IT-incidenter ägs och förvaltas av MSB.

5.2 Giltighet

Planen är *interimistisk till dess att den övats* och reviderats i linje med resultaten. Senast 2012 ska den första övningen vara genomförd och planen fastställd. MSB och enheten för informationssäkerhet ansvarar för att planera och genomföra denna övning i samverkan med SAMFI-myndigheterna.

Planen föreslås efter fastställande gälla i tre år (eller till dess att behov finns av att se över denna).

Planen bör övas kontinuerligt för att vara adekvat och uppdaterad. Förslagsvis sker detta vart tredje år med start det år den fastställs.

5.3 Revidering, utvärdering och erfarenhetsåterkoppling

Planen ska efter det att den fastställts utvärderas vart tredje år eller när behov uppstår. Alla myndigheter i SAMFI kan ta initiativ till utvärdering som inte faller inom ramen för den ordinarie revisionstiden. Revidering av planens innehåll sker efter samråd med SAMFI-myndigheterna och beslut av MSB.

5.4 Kontaktperson

Kontaktperson för hanterandeplanen för allvarliga IT-incidenter är chefen för enheten för samhällets informationssäkerhet vid MSB.

6. Finansiering

MSB bedömer att den nationella hanterandeplanen för allvarliga IT-incidenter i nuläget till övervägande del[4] kan finansieras inom myndighetens ram. MSB återkommer i den ordinarie budgetprocessen ifall denna bedömning ändras.

De kostnader som kommer att bli aktuella är i huvudsak

- omkostnader för att tillgängliggöra och införa planen (tryck, föreläsningar med mera)
- kostnader i samband med föreslagen övning 2012 i syfte att utvärdera och fastställa planen
- kostnader för att förvalta planen.

När det gäller kostnaderna för de tekniska kompetensnätverken är det i nuläget svårt att uppskatta dessa. Utgångspunkten är att framtida tekniska kompetensnätverk ska finansieras av deltagarna själva – i huvudsak handlar det om egen tid. I vissa fall kan viss central finansiering komma att krävas, det rör sig då främst om punktinsatser. Ett systematiskt arbete med att tydliggöra kostnadsfrågan kommer att göras i nära anslutning till åtgärderna.

[4] En närmare genomgång av förutsättningarna för den föreslagna övningen 2012 behöver göras i syfte att klargöra kostnaderna.

7. Referenser

Lagar

Polislag (1984:387)

Säkerhetsskyddslag (1996:627)

Ellag (1997:857)

Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Förordningar

Förordning (1989:773) med instruktion för Rikspolisstyrelsen

Säkerhetsskyddsförordning (1996:633)

Personuppgiftsförordning (1998:1191)

Förordning (2002:864) med länsstyrelseinstruktion

Förordning (2002:1050) med instruktion för Säkerhetspolisen

Förordning (2006:942) om krisberedskap och höjd beredskap

Förordning (2007:854) med instruktion för Försvarets materielverk

Förordning (2007:937) med instruktion för Försvarets radioanstalt

Förordning (2007:951) med instruktion för Post- och telestyrelsen

Förordning (2007:975) med instruktion för Datainspektionen

Förordning (2007:1266) med instruktion för Försvarsmakten

Förordning (2008:1002) med instruktions för Myndigheten för samhällsskydd och beredskap

Propositioner

Proposition 2005/06:133 *Samverkan vid kris – för ett säkrare samhälle*

Proposition 2007/98:92 *Stärkt krisberedskap – för säkerhets skull*

Proposition 2010/11:1 *Budgetpropositionen för 2011*

Dokument från myndigheter

KBM (2008) *Sveriges beredskap mot nätangrepp* d-nr 1104-2007

MSB (2010) *Styrel – inriktning för prioritering av elanvändare,* svar på regeringsuppdrag nr 13 i regleringsbrevet för 2010, 2009-3054

MSB (2010) *Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter,* Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap, 2009-14471

Statskontoret (2001) *Hantering av IT-incidenter – Vem gör vad och hur?* IT-kommissionen

Övrigt

Regeringsbeslut *Tjänsteman i beredskap och ledningsfunktion enligt förordningen (2006:942) om krisberedskap och höjd beredskap,* (Fö2007/436/CIV, 2007-06-07)

Regeringsbeslut *Tjänsteman i beredskap och ledningsfunktion enligt förordningen (2006:942) om krisberedskap och höjd beredskap* (Fö2008/552/SSK, 2008-10-09)

Regeringsuppdrag 2010-04-14, Fö2010/701/SSK

Regeringsuppdrag 2010-04-14, Fö2010/698/SSK

USA: *National Cyber Incident Response Plan, Interim Version,* Homeland Security, September 2010

WARP Homepage: http://www.warp.gov.uk/index.html (2010-12-03)

Bilaga A: Regeringsuppdraget

REGERINGEN

Myndigheten för samhällsskydd o beredskap
2010 -04- 19
Ärendenummer
2010 - 4545 - 1

Regeringsbeslut 12

2010-04-14 Fö2010/701/SSK

Försvarsdepartementet

Myndigheten för samhällsskydd och beredskap
651 81 KARLSTAD

Uppdrag till Myndigheten för samhällsskydd och beredskap angående samhällets informationssäkerhet

Regeringens beslut

1. Myndigheten för samhällsskydd och beredskap ska lämna förslag på hur en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting kan skapas. Myndigheten för samhällsskydd och beredskap ska genomföra uppdraget i samråd med andra berörda aktörer bl.a. de som ingår i samverkansgruppen för informationssäkerhet, SAMFI (Försvarets radioanstalt, Försvarets materielverk, Post- och telestyrelsen, Försvarsmakten och Säkerhetspolisen), Totalförsvarets forskningsinstitut, Skatteverket samt Delegationen för e-förvaltning. Myndigheten ska i detta arbete beakta befintlig infrastruktur, även kommersiella system, samt presentera alternativa lösningar med kostnadsförslag. Erfarenheter från andra länder som gjort liknande etableringar ska inhämtas. Myndigheten ska också i samråd med Försvarsmakten och Försvarets radioanstalt analysera hur befintliga eller kommande kryptosystem i detta syfte kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.

2. Myndigheten för samhällsskydd och beredskap ska ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras samt skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter för att skapa en ökad förmåga till respons. Myndigheten för samhällsskydd och beredskap ska genomföra uppdraget i samråd med de myndigheter som ingår i samverkansgruppen för informationssäkerhet, SAMFI.

3. Myndigheten för samhällsskydd och beredskap ska utreda hur ett system för obligatorisk IT-incidentrapportering för statliga myndigheter kan utformas.

Postadress 103 33 Stockholm
Besöksadress Jakobsgatan 9
Telefonväxel 08-405 10 00
Telefax 08-723 11 89
E-post: registrator@defence.ministry.se

2

4. Myndigheten för samhällsskydd och beredskap ska, liksom tidigare Krisberedskapsmyndigheten, kontinuerligt analysera och bedöma omvärldsutvecklingen avseende hot, sårbarheter och risker inom informationssäkerhetsområdet samt konsekvenser för viktiga funktioner i samhället. Den samlade bedömningen ska tas fram i samverkan med berörda aktörer i samhället. Detta ska ses som ett komplement till den löpande rapportering och lägesbedömning som försvarsunderrättelse-myndigheterna och Säkerhetspolisen lämnar till regeringen inom ramen för sina respektive uppdrag.

5. Myndigheten för samhällsskydd och beredskap ska ha möjlighet att utifrån analyser av förmågebedömningar, genomförda risk- och sårbarhetsanalyser samt bedömningar av beroendeförhållanden föreslå enskilda myndigheter att anlita Försvarets radioanstalt för IT-säkerhetsanalyser. Detta ska ske i samråd med tillsynsmyndigheterna enligt säkerhetsskyddsförordningen (1996:633). Efter genomförda analyser ska Myndigheten för samhällsskydd och beredskap informera tillsynsmyndigheterna om påträffade förhållanden av betydelser för dessa myndigheters förebyggande och brottsbekämpande arbete.

Myndigheten för samhällsskydd och beredskap ska redovisa bedömda kostnader samt lämna förslag till finansiering. Myndigheten för samhällsskydd och beredskap ska hålla Regeringskansliet (Försvarsdepartementet) fortlöpande informerat under uppdragets genomförande.

Uppdragen ska redovisas senast 1 mars 2011 till Regeringskansliet (Försvarsdepartementet).

Ärendet

Att myndigheterna och andra offentliga aktörer kan kommunicera på ett säkert sätt är en förutsättning för god nationell informationssäkerhet och möjligheten att hantera allvarliga IT-incidenter eller andra allvarliga störningar. I det svenska samhället behövs en administrativ och teknisk infrastruktur vid kriser och olyckor för informationsdelning och respons i vid mening, där samtliga aktörer av betydelse för samhällets kritiska informationsinfrastruktur finns representerade. Infrastrukturen ska fungera under normala förhållanden men ska också innefatta en organisation och struktur som kan fungera som stöd under allvarliga störningar och kriser. En sådan stödorganisation och infrastruktur behöver ha en hög informationssäkerhet för att inte slås ut vid allvarliga störningar. För att bli kostnadseffektiv och för att på bästa sätt ta vara på befintlig kompetens och organisation ska det övervägas att låta infrastrukturen bygga på nuvarande teknisk struktur. En övergång från normalläge till krisläge ska inte innebära stora förändringar vad gäller aktörer och arbetssätt, eftersom det bedöms försvåra och fördröja arbetet.

En nationellt digital informations- och kommunikationsinfrastruktur består sannolikt inte av ett enskilt fysiskt nät utan av flera olika nät, där det finns en gemensam logisk tjänst, för säkert informationsutbyte med hög tillgänglighet som kan nyttjas av myndigheter och andra offentliga aktörer.

Myndigheten för samhällsskydd och beredskap har på regeringens uppdrag redovisat en rapport Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter (Fö2009/2162/SSK). Enligt rapporten är den rapportering av IT-incidenter som idag sker på frivillig basis otillräcklig för att kunna bidra till en löpande aktuell lägesbild av tillståndet vid samhällsviktig verksamhet och kritisk infrastruktur. Regeringen anger i budgetpropositionen för 2010 (prop. 2009/10:1, bet 2009/10:FöU1, rskr. 2009/10:104) att rapportering av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur behöver förbättras.

Hot mot verksamheter och tillgångar kan antingen vara antagonistiska eller oavsiktliga som exempelvis naturolyckor och tekniska fel. Sårbarheter, som fallerande skydd och bristande rutiner, bidrar till att hot realiseras. Regeringen ser därför ett behov av att ha en aktuell och relevant uppfattning om hot, sårbarheter och risker på samt trender och tendenser på informationssäkerhetsområdet.

På regeringens vägnar

Sten Tolgfors

Linda Ericson

Kopia till

Statsrådsberedningen/SAM
Justitiedepartementet/PO
Justitiedepartementet/Gransk
Justitiedepartementet/L4
Utrikesdepartementet/FIM
Finansdepartementet/BA
Finansdepartementet/SF
Finansdepartementet/SKA
Näringsdepartementet/ITP
Rikspolisstyrelsen

4

Säkerhetspolisen
Försvarsmakten
Försvarets materielverk
Försvarets radioanstalt
Totalförsvarets forskningsinstitut
Skatteverket
Post och telestyrelsen
Sveriges kommuner och landsting
Delegationen för e-förvaltning

Bilaga B: Uppdragets organisation

Arbetet med regeringsuppdraget har styrts av en styrgrupp inom MSB, bestående av

- Richard Oehme, ordförande
- Mikael Tofvesson
- Anna Nyman.

I projektgruppen som har arbetat med uppdraget har följande personer ingått:

- Malin Fylkner, projektledare
- Helena Andersson
- Åke Holmgren
- Sara Jegeman
- Svante Nygren
- Göran Pestana (CERT-SE)
- Ester Veibäck (direktstöd, FOI).

Till arbetet med regeringsuppdraget har en referensgrupp med representanter från följande organisationer knutits:

Organisation	Representant
Försvarets materielverk	**Anders Dahlberg**
Försvarets radioanstalt	**Arvid Kjell**
	Cecilia Laurén
Försvarsmakten	**Tobias Jonason**
FM/CERT	**Ulf Skoglund**
Försvarsmakten, Högkvarteret	**Tobias Rogell**
Göteborgs stad	**Jan A Svensson**
Länsstyrelsen i Västernorrlands län	**Torbjörn Westman**
Näringslivets säkerhetsdelegation	**Tommy Svensson**
Post- och telestyrelsen	**Peter Wallström**
Riksdagsförvaltningen	**Mikael Vos**
Rikspolisstyrelsen	**Kristin Granlund**
Skatteverket	**Teijo Mattila**
	Maria Emilsson
Sveriges kommuner och landsting	**Jörgen Sandström**
Socialstyrelsen	**Kerstin Risshytt**
Stockholms universitet, DSV	**Christer Magnusson**
	Love Ekenberg
Svenska kraftnät	**Alireza Hafezi**
Säkerhetspolisen	**Michael Nilsson**
Tele2	**Lars Michael Jogbäck**
Totalförsvarets forskningsinstitut	**Johan Allgurén**
	Anders Törne
Trafikverket	**Lars Nifwa**

Externa resurser har använts i två delstudier som FOI utfört:

- Internationell studie – Fredrik Lindgren
- Framtagande av typscenarier – Georg Fischer och Ann-Sofie Stenérus Dover.

Myndigheterna i SAMFI har fortlöpande informerats och fått möjlighet att lämna synpunkter på utvecklingen av hanterandeplanen.

Bilaga C: Förkortningar och vissa begrepp

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

CERT (Computer Emergency Response Team) – Funktion för incidenthantering.

CERT-SE – Den svenska nationella CERT-funktionen vid MSB.

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.

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

CSEC (Sveriges certifieringsorgan för IT-säkerhet) – Är placerad på FMV och ansvarar för uppbyggnad, drift och förvaltning av ett system för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med standarden Common Criteria.

DDoS-attacker (Distributed Denial of Service) – En typ av tillgänglighetsattack, 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.

FHS – Försvarshögskolan.

FOI – Totalförsvarets forskningsinstitut.

FORTV – Fortifikationsverket.

FM – Försvarsmakten.

FMV – Försvarets materielverk.

FRA – Försvarets radioanstalt.

KBF – Krisberedskapsförordningen: förordning (2006:942) om krisberedskap och höjd beredskap.

LAN (Local Area Network) – Lokalt sammankopplade datorer.

LEH – lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

MSB – Myndigheten för samhällsskydd och beredskap.

NOS (Nationell operativ samverkansfunktion för informationssäkerhet) – är en samverkansform som inrättats av MSB. NOS

syftar till att skapa en förbättrad förmåga i samhället att hantera allvarliga IT-incidenter.

NTSG – Nationella Telesamverkansgruppen.

PTS – Post- och telestyrelsen.

PUL – personuppgiftslagen.

Ping- och SYN-flodning – Olika typer av tillgänglighetsattacker.

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

RKP – Rikskriminalpolisen.

RPS – Rikspolisstyrelsen.

RSA – Risk- och sårbarhetsanalys.

SAMFI (Samverkansgruppen för informationssäkerhet) – SAMFI utgörs av representanter från Försvarets radioanstalt, Post- och telestyrelsen, Försvarsmakten, Rikspolisstyrelsen, Försvarets materielverk, Säkerhetspolisen och Myndigheten för samhällsskydd och beredskap.

S-BIT – Samordningsfunktion för brottsrelaterade IT-incidenter, gemensamt ägd av RKP och Säpo.

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

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

Sitic (Sveriges incidentcentrum) – Den svenska CERT-funktionen. Drivs av MSB från 1 januari 2011 under namnet CERT-SE.

Säkra kryptografiska funktioner – Kryptosystem som är nationellt godkända för att skydda både hemliga och skyddsvärda uppgifter. Kryptolösningar finns hos samtliga i kapitel 3 utpekade myndigheter för att skydda samtal, faxöverföring, datafiler, videokonferens eller hela nätverk.

Säpo – Säkerhetspolisen.

TiB – Tjänsteman i beredskap.

TLP (Traffic Light Protocol) – En modell för delning av känslig information mellan organisationer. Protokollet har fyra nivåer av information. Röd – informationen ges endast verbalt och till namngivna personer. Gul – begränsad distribution inom organisationerna. Grön – informationen kan

spridas inom organisationerna men inte publiceras exempelvis på Internet. Vit – kan distribueras utan restriktioner.

VMA – Viktigt meddelande till allmänheten.

WAN (Wide Area Network) – Ett nätverk av datorer som sträcker sig över ett stort område. Kan koppla ihop olika lokala nätverk (LAN).

WARP (Warning, Advice and Reporting Point) – En brittisk nätverks-modell med organisationer som delar råd och information om hot och sårbarheter relaterat till informationssäkerhet.

WIS (Webbaserat informationssystem) – Ett nationellt webbaserat informationssystem som används för informationsdelning mellan aktörerna i det svenska krishanteringssystemet före, under och efter en kris.

Bilaga D: Förteckning över stödjande rutiner

Samverkansprocesser och stödjande rutiner	Övergripande innehåll	Existerar (E) eller existerar ej (EE)
Hanterandeplanens ram		
Beslut om aktivering av den nationella hanterandeplanen för allvarliga IT-incidenter	Beskriver hur den nationella hanterandeplanen för allvarliga IT-incidenter aktiveras samt vilka som omedelbart informeras om detta. Såväl kriterier som beslutsprocess.	E/EE (beskrivs i stycke 4.2.1) Ägs och förvaltas av MSB
Informering om aktivering av plan till berörda aktörer (via TiB)	Format för informerande om planens aktivering, samt uppdaterade kontaktlistor	E/EE Ägs och förvaltas av MSB
Beslut om avaktivering av den nationella hanterandeplanen för allvarliga IT-incidenter	Beskriver hur den nationella hanterandeplanen för allvarliga IT-incidenter avaktiveras, såväl kriterier som besluts-process.	EE (beskrivs i stycke 4.2.2) Ägs och förvaltas av MSB
Beslut om utvärdering och erfarenhetsåterkoppling	Beskriver när beslut tas och av vem för att initiera en utvärdering av en samordningshändelse samt erfarenhetsåterkoppla resultaten till berörda aktörer	EE Tas fram, ägs och förvaltas av MSB
Utvärdering och erfarenhetsåterkoppling	Beskriver formatet för utvärderingsarbetet och erfarenhetsåterkopplingen	EE Tas fram, ägs och förvaltas av MSB
Nationell lägesbild		
MSB beslut om samordningshändelse	Beskriver hur beslut om att initiera en samordnings-händelse går till och vem som tar detta beslut	E Ägs och förvaltas av MSB
Avslut av samordningshändelse	Beskriver hur ett avslut av en samordningshändelse görs (på vilka kriterier) och av vem	E Ägs och förvaltas av MSB
Informerande om pågående händelse till existerande tekniska kompetensnätverk	Beskriver hur informations-delning om pågående händelse förmedlas, och av vem, till existerande tekniska kompetensnätverk	EE Tas fram, ägs och förvaltas av MSB
Samverkanskonferens	Beskriver hur en	E

	samverkanskonferens genomförs och hur beslutsprocessen ser ut	Ägs och förvaltas av MSB
Incidentrapportering	Beskriver hur en incidentrapportering går till (såväl format som inrapporteringsvägar)	EE Arbete pågår med att ge förslag till obligatorisk incident-rapportering
Rapportering till regeringen	Beskriver vad som ska rapporteras (frågor), hur (format), när och till vem	E Ägs och förvaltas av MSB
Rapportering till berörda aktörer (nationellt och internationellt)	Beskriver vad som ska rapporteras (frågor), hur (format), när och till vem	E/EE Finns i viss utsträckning. Bör kompletteras med det internationella perspektivet avseende IT-dimensionen (CERT)
Informationssamordning		
FAQ	Beskriver hur FAQ:s tas fram och av/med vem	E
Underlag nationell lägesbild	Beskriver såväl format som process för att säkerställa informationsdelning mellan arbetet med den nationella lägesbilden och informations-samordningen	E/EE Finns i viss utsträckning men behöver kompletteras. Ägs och förvaltas av MSB
Samlad konsekvens- och hanterandebedömning		
Underlag enskilda konsekvensbedömningar	Beskriver formatet på de enskilda konsekvensbedöm-ningarna som tas fram av aktörerna i systemet samt den process med vilken detta underlag förs in i arbetet med den samlade konsekvens- och hanterandebedömningen.	EE Tas fram och ägs och förvaltas sedan av MSB
Kontaktperson (liaison) med processen nationell lägesbild	Beskriver hur informations-delningen och överföringen av arbetet från den nationella lägesbilden till processen med den samlade konsekvens- och hanterandebedömningen ska gå till	EE Tas fram och ägs och förvaltas sedan av MSB

Teknisk operativ samverkan		
Informationsdelning (TLP – Traffic Light Protocol)	Beskriver en modell för informationsdelning mellan olika aktörer	E
Operativt stöd	Beskriver hur en förfrågan eller ett avrop av operativt stöd till myndigheter med särskilt ansvar för informationssäkerhet går till	EE Tas fram, ägs och förvaltas av respektive ansvarig aktör
Förmedling av kontakt med tekniska kompetensnätverk	Beskriver hur förmedling av kontakt med tekniska kompetensnätverk går till	EE Tas fram, ägs och förvaltas av MSB

Bilaga E: Tekniska kompetensnätverk

Åtgärdsförslag tekniska kompetensnätverk

I syfte att öka samhällets samlade förmåga att hantera allvarliga IT-incidenter avser MSB att göra följande:

- MSB ska i samråd med myndigheterna i SAMFI undersöka möjligheten att skapa ett mer formaliserat tekniskt kompetensnätverk bestående av tekniskt operativa SAMFI-experter. Detta i syfte att öka förutsättningarna för informationsdelning, kompetenshöjning och nätverkande på nationell nivå.
- MSB ska ta initiativ till att gemensamt med berörda aktörer genomföra en pilotstudie i syfte att utveckla metoder och verktyg till stöd för att skapa och underhålla tekniska kompetensnätverk på kommunal, regional och nationell nivå.
- MSB ska aktivt verka för att skapa förutsättningar för privat–offentlig samverkan mellan olika experter och mellan experter och mottagare i syfte att skapa och vidareutveckla relevanta kontaktytor. MSB ska arrangera seminarier, konferenser och övningar.

Bakgrund

Det finns ett underskott på teknisk kompetens inom olika samhällsviktiga verksamheter och infrastrukturer. Detta underskott kan medföra allvarliga svårigheter i samband med kriser i samhället. Det är till exempel relativt få personer i Sverige som har tillräcklig erfarenhet av att hantera trafikflöden på operatörsnivå eller olika typer av specialiserade industriella kontrollsystem (SCADA). Av dessa är det dessutom bara en liten grupp som har det omfattande kontaktnät som kan behövas för att praktiskt operativt hantera allvarliga IT-incidenter. En stor del av den tekniska kompetensen finns också inom den privata sektorn.

För att skapa en bild av hur behovet av kompetensnätverk ser ut är det viktigt att inventera dels de olika sektorernas förmågor och brister, dels de formella och informella nätverk som redan existerar. Därefter behöver det skapas förutsättningar för olika resurser som kan användas till stöd för den nationella hanteringen av allvarliga IT-incidenter. Dessa resurser kan förslagsvis organiseras som tekniska kompetensnätverk på alla samhällsnivåer (sektoriellt, lokalt, regionalt och nationellt) – och utifrån de behov och förutsättningar som finns.

Det övergripande målet med att bemöta underskottet på teknisk kompetens är att *öka samhällets samlade förmåga att hantera allvarliga IT-incidenter*.

Uppdraget och viktiga utgångspunkter för arbetet

MSB fick i april 2010 i uppdrag av regeringen att i samband med framtagandet av den nationella planen för hantering av allvarliga IT-incidenter skapa tekniska kompetensnätverk som kan stödja samhället vid kriser. Uppdraget formulerades:

> *Myndigheten för samhällsskydd och beredskap ska ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras samt skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter för att skapa en ökad förmåga till respons. Myndigheten för samhällsskydd och beredskap skall genomföra uppdraget i samråd med de myndigheter som ingår i samverkansgruppen för informationssäkerhet.*

Arbetet har, med tanke på det begränsade tidsutrymmet, kommit att fokusera på att ta fram *förslag* till stöd för skapande och upprätthållande av tekniska kompetensnätverk snarare än att de facto skapa nätverken.

Viktiga utgångspunkter för arbetet:

- Fokus för kompetensnätverken såsom beskrivna i detta arbete är hantering av allvarliga IT-incidenter.
- Styrande principer för det svenska krishanteringssystemet gäller.
- Myndigheter med utpekat ansvar för informationssäkerhetsfrågor har en särskild roll att spela (de så kallade SAMFI-myndigheterna).
- Det är viktigt att verka för privat–offentlig samverkan inom ramen för befintliga och planerade initiativ och aktiviteter.

Det övergripande syftet att verka för att öka samhällets samlade förmåga att hantera allvarliga IT-incidenter innebär att fokus naturligen hamnar på *hanterandefrågor* av mer operativ karaktär snarare än på kompetensnätverk till stöd för det förebyggande arbetet.

I likhet med skrivningarna i huvudtexten för hanterandeplanen är det viktigt att även här betona betydelsen av de styrande principerna i krishanteringssystemet (som exempelvis ansvarsprincipen) och vilka konsekvenser det får för utformningen av förslagen. *Tonvikten vid utformningen av nedanstående förslag har i linje med dessa principer kommit att ligga på stöd till samverkan och nätverkande och framtagande av metodik och verktyg till det gemensamma*. Detta i vetskap om att aktörernas behov av teknisk kompetens varierar, och så även de förutsättningar som finns för att skapa och underhålla olika nätverk.

Myndigheterna i SAMFI, det vill säga Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen samt Rikskriminalpolisen/Säkerhetspolisen, har olika ansvar och mandat men har det gemensamt att de har ett utpekat ansvar för informationssäkerhetsfrågor. Vid samtliga dessa myndigheter finns det tekniska experter som i händelse av en allvarlig IT-incident, i varierande utsträckning, kommer att vara inblandade i hanteringen av incidenten. Det är rimligt, givet det särskilda ansvar dessa myndigheter har inom informationssäkerhetsområdet, att de även har en *särskild roll att spela betraktat ur ett kompetensnätverksperspektiv*. Exakt hur detta ansvar kan se ut är givetvis en fråga som ska utredas av de inblandade parterna gemensamt.

Vikten av att etablera fungerande samverkan mellan offentliga och privata aktörer till stöd för hanteringen av allvarliga IT-incidenter kan inte nog betonas. Det är i allra högsta grad en gemensam angelägenhet och en framgångsfaktor.

Förslagen i korthet

Förslag 1:

MSB avser att i samråd med myndigheterna i SAMFI undersöka möjligheten att skapa ett förtroendebaserat nätverk bestående av tekniskt operativa experter hos myndigheter med uttalad roll vid allvarliga IT-incidenter (SAMFI-myndigheterna).

Som tidigare nämnts utgörs samverkansgruppen för informationssäkerhet (SAMFI) av sex myndigheter som alla har ett utpekat ansvar inom informationssäkerhetsområdet. SAMFI-myndigheterna samverkar om frågor som rör informationssäkerhet under visionen att *verka för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet*. Samverkan mellan myndigheterna sker också i vardagen, utanför ramen för dessa mer formaliserade möten. *För att ytterligare stärka denna samverkan föreslås att möjligheten att skapa en mer formaliserad samverkan inkluderandes de tekniskt operativa experterna utreds närmare under ledning av MSB men i samverkan med berörda parter*.

Under 2011 kommer den nationella operativa samverkansfunktionen (NOS) att skapas inom MSB. Funktionen är tänkt att bestå dels av CERT-SE och personal vid MSB:s enhet för samhällets informationssäkerhet, dels av adjungerad personal från SAMFI-myndigheterna. Uppgiften för NOS är bland annat att skapa en förbättrad förmåga i samhället att hantera allvarliga IT-incidenter. Det är viktigt att frågan om ett eventuellt tekniskt operativt expertnätverk beaktas i ljuset av synergier med nämnda initiativ samt andra relevanta och befintliga nätverk.

Förslag 2:

MSB avser att i samverkan med berörda aktörer på kommunal, regional och nationell nivå ta fram en ”verktygslåda” bestående av processer och metoder till stöd för att skapa och underhålla tekniska kompetensnätverk.

Det finns i dag ett antal formella och informella nätverk inom informationssäkerhetsområdet. Det är viktigt att dessa nätverk även kompletteras med tekniska kompetensnätverk anpassade till de behov som finns hos de samhällsviktiga aktörerna på lokal, regional och nationell nivå – och då specifikt avseende den operativa hanteringen av allvarliga IT-incidenter. Sådana tekniska kompetensnätverk bidrar till att öka samhällets samlade förmåga att hantera allvarliga IT-incidenter genom att de bland annat skapar kontaktytor mellan relevanta aktörer och ökar den tekniska kompetensen avseende just hanterandefrågor.

För att nå framgång med att skapa tekniska kompetensnätverk föreslår MSB att myndigheten tillsammans med berörda aktörer på kommunal, regional och nationell nivå tar fram en ”verktygslåda” till stöd för att skapa och underhålla tekniska kompetensnätverk. Förslagsvis genomförs detta arbete inom ramen för ett pilotprojekt där relevanta representanter från olika nivåer i samhället deltar (inklusive såväl offentliga som privata aktörer). Syftet är att utveckla användbara verktyg som sedan kan delges andra intresserade parter via lämpliga kanaler. Stöd och inspiration för arbetet finns att få genom tidigare spridda koncept som exempelvis ”WARP” som använts med framgång i England.

I Storbritannien har NISCC (National Infrastructure Co-ordination Centre, numera en del av CPNI, Centre for the Protection of National Infrastructure) utvecklat en nätverksmodell för delning av information om IT-säkerhet, benämnd WARP – Warning, Advice and Reporting Point. Syftet med dessa nätverk är att höja informationssäkerheten i olika aktörers system, genom att medlemmarna i nätverken förser varandra med varningar om sårbarheter och hot, samt delar råd om hur risker kan minskas. Nätverken hålls förhållandevis små, med 20–100 medlemmar, för att skapa en grund för tillit mellan medlemmarna. Det koncept för WARP som används i Storbritannien fyller inte precis det syfte som finns uttalat för de svenska kompetensnätverken. Grundtanken skulle kunna återanvändas i detta sammanhang: att skapa ett förtroligt nätverk med samma intresseområden för att hålla kontaktvägar öppna och snabbt kunna nå rätt personer inom relevant kompetensområde.[5]

[5] http://www.warp.gov.uk/index.html (2010-12-03)

Förslag 3:

MSB ska ta initiativ till aktiviteter som främjar privat–offentligt nätverkande i syfte att öka förmågan att hantera allvarliga IT-incidenter.

Detta förslag syftar till att både ge stöd till befintliga nätverk med relevant verksamhet och att ta konkreta initiativ till aktiviteter som främjar kontakt mellan privata och offentliga aktörer på bredare front. Kontakter behövs både experter emellan och mellan aktörer som kan komma att behöva experthjälpen vid en allvarlig IT-incident. Exempel på möjliga aktiviteter kan vara att arrangera seminarier och konferenser men även att genomföra övningar med mera. Det är här även viktigt att beakta den internationella dimensionen och behov av tekniska kompetensnätverk som är gränsöverskridande till sin karaktär (som exempelvis CERT-nätverken).

Bilaga F: Internationell utblick

Nationella planer för att hantera IT-incidenter – Internationell utblick

Inom ramen för projektet har en studie av ett urval länders arbete med att ta fram handlingsplaner för att hantera IT-incidenter gjorts. Studien har genomförts av Fredrik Lindgren vid Totalförsvarets forskningsinstitut (FOI). De länder som valdes att studera närmare var USA, Storbritannien, Finland, Estland och Tyskland.

Underlaget bygger på offentligt tillgängligt material och dokument, som respektive land gjort tillgängligt via sina officiella webbplatser. Underlaget om Estland bygger också på intervjuer med personer inom den estniska statsförvaltningen.

I den avslutande jämförelsen mellan ländernas organisering och hantering av IT-incidenter har Lindgren identifierat ett antal element som återkommer hos de olika länderna, trots att deras val av organisation skiljer sig:

En sådan grupp av element handlar i stor grad om att prata samma språk i det utbyte som kan behövas i samband med hantering av en IT-incident:

- Definitioner av begrepp
- Skala över ”allvarlighetsgraden” av en händelse
- Indikatorer för klassificering av händelser enligt den angivna skalan

En annan grupp av element handlar i stor utsträckning om att förstå vilken roll respektive aktör som är inblandad i hanteringen av en incident har:

- Förtydligande av roller
- Förtydligande av ansvar hos respektive aktör
- Förtydligande av samspelet mellan berörda aktörer

En tredje grupp är snarast en fördjupning av punkten ”samspel” ovan, men ges så mycket utrymme i de dokument som studerats att den är värd en egen kommentar. Det handlar här om att i relativt konkreta termer beskriva hur själva interaktionen mellan olika aktörer bör gå till:

- Rapporteringsvägar
- Kommunikationsmedel

En fjärde och sista grupp av element som återkommer är olika typer av möjligheter till extraordinära befogenheter eller åtgärder vid hantering av särskilt allvarliga incidenter. Det kan antingen handla om direkta mekanismer, dvs. om en händelse klassas på ett visst sätt så medför det automatiskt utökade befogenheter för en viss aktör, exempelvis:

- Rätt att utnyttja andra aktörers resurser
- Undantag från regler om offentlig upphandling.

Det finns också exempel på indirekta mekanismer för utökade befogenheter, exempelvis genom att aktivera förberedda strukturer som snabbt kan sammankallas vid behov och har befogenheter att besluta om prioritering av knappa resurser, avsteg från ordinarie regelverk eller särskild finansiering.

Nationella planer för att hantera IT-incidenter – Internationell utblick

Sändlista/Distribution: Myndigheten för samhällsskydd och beredskap, att. Malin Fylkner, Enheten för samhällets informationssäkerhet

Detta underlag har tagits fram av FOI Försvarsanalys på uppdrag av MSB, Enheten för samhällets informationssäkerhet, inom ramen för uppdraget ”Nationell plan för hantering av allvarliga IT-incidenter” (MSB dnr 2010-4545, 2010-09-02 respektive FOI-2010-1286, 2010-08-30).

Förord

Detta underlag har tagits fram av FOI Försvarsanalys på uppdrag av MSB som en delstudie inom ramen för beställningen ”Nationell plan för hantering av allvarliga IT-incidenter”. Arbetet har genomförts av Fredrik Lindgren vid Enheten för samhällets säkerhet, FOI Försvarsanalys.

Studien syftar till att ge en överblick över innehållet i ett urval av andra länders nationella planer för att hantera IT-incidenter. MSB har svarat för urvalet av länder. Underlaget bygger i huvudsak på material och dokument som respektive land gjort tillgängligt via sina officiella webbplatser. Underlaget om Estland bygger även på intervjuer med personer inom den estniska statsförvaltningen.

1. Inledning

Strukturen för att hantera IT-incidenter skiljer sig mellan olika länder, men det finns också gemensamma drag. I det följande beskrivs arbete med informationssäkerhet, cybersäkerhet och därtill kopplad incidenthantering i USA, Storbritannien, Finland, Estland och Tyskland. I första hand är det innehållet i planer på nationell nivå för hantering av mer omfattande IT-incidenter som är av intresse.

Med begreppet *cybersäkerhet* avses i denna text frågor om säkerhet i den digitala informations- och kommunikationsinfrastrukturen i vid mening, det finns till exempel ingen avgränsning till det publika nätverket Internet i detta begrepp. För de länder som själva använder begreppet *cyber security* kommer begreppet cybersäkerhet att användas i redovisningen nedan. För de länder som använder det bredare begreppet *information security* för att beskriva sitt arbete så kommer på motsvarande sätt informationssäkerhet att användas. Generellt sett är de definitioner av cybersäkerhet som används i de studerade länderna väldigt breda och täcker in en stor del av det som vanligen räknas in under begreppet informationssäkerhet.

Redovisningen fokuserar på frågor om säkerhet och hantering av IT-relaterade incidenter i icke-militära offentliga system och nätverk samt sådana system och nätverk som utgör delar av landets kritiska infrastruktur. De senare ägs och drivs inte sällan av privata aktörer.[6]

För respektive land redovisas först något om den organisatoriska strukturen för frågor om informations-/cybersäkerhet, dels i fråga om inriktning och samordning på övergripande nivå, dels i fråga om hantering av IT-incidenter.

[6] För militära system och nätverk, som i sig oftast är uppbyggda separat från övriga offentliga system, finns det vanligen särskilda strukturer för hantering av IT-incidenter.

För de länder där det finns nationella strategier inom området följer sedan en beskrivning av innehållet i dessa. Slutligen redovisas innehållet i de planer som finns för hantering av mer omfattande incidenter. För flera av de studerade länderna har det dock inte gått att identifiera några specifika responsplaner i det underlag som funnits tillgängligt i arbetet. I dessa fall har mer fokus lagts på vad som redovisas om förmågan att hantera incidenter i andra dokument, exempelvis nationella strategier inom området.

2. USA

Organisation och aktörer

Ansvaret för inriktning och samordning av icke-militära cybersäkerhetsfrågor på övergripande nivå vilar på Department of Homeland Security (DHS). För detta ändamål finns en särskild enhet, Office of Cybersecurity and Communications (CS&C) som utgör en del i DHS National Protection and Programs Directorate (NPPD). Till ansvarsområdena för CS&C hör samordning och krishantering i samband med allvarliga IT-incidenter, vilket hanteras av underenheten National Cyber Security Division (NCSD). Strukturen för hantering av IT-incidenter har utvecklats relativt nyligen genom inrättandet av National Cybersecurity and Communications Integration Center (NCCIC) under hösten 2009. De mer konkreta delarna av ansvaret för hantering av IT-incidenter utövas numera genom NCCIC som samordnar ett antal aktörer och verksamheter inom cybersäkerhet på federal nivå.

NCCIC ska bl.a. skapa och upprätthålla en samlad lägesbild för informations- och kommunikationssystem på nationell nivå och samordna aktiviteter för hantering. NCCIC omfattar bl.a. US-CERT (en del av NCSD) som är den statliga CERT-funktionen för federala icke-militära system och nätverk, National Cyber Security Center (NSCS) som koordinerar utbytet mellan övriga statliga aktörer inom området (försvaret, underrättelsetjänsten och brottsbekämpande myndigheter) och National Coordination Center for Telecommunications (NCC).

Utöver det ansvar som DHS har för att upprätthålla säkerheten och funktionaliteten nationellt på detta område har det amerikanska försvaret betydande resurser och en egen struktur för att upptäcka och hantera olika former av IT-relaterade hot. Sedan hösten 2010 finns en överenskommelse mellan DHS och Department of Defense om fördjupat samarbete inom cybersäkerhet som bl.a. reglerar hur det militära försvarets resurser kan utnyttjas i skyddet av kritisk informationsinfrastruktur.[7]

Nationell strategi

Den senast fastställda samlade nationella strategin inom cybersäkerhetsområdet är från 2003 och innehåller fem prioriterade områden:[8]

- Nationellt system för respons vid cyberattacker
- Reducering av cyberrelaterade hot och sårbarheter

[7] *Memorandum of agreement between the Department of Homeland Security and the Department of Defense regarding cybersecurity*, publicerat 2010-10-13

[8] *The National Strategy to Secure Cyberspace*, The White House, feb 2003

- Nationellt program för utbildning och ökat medvetande om cybersäkerhet
- Skydd av statliga system och nätverk
- Internationellt samarbete om cybersäkerhet

Därefter har såväl Bush- som Obamaadministrationen tagit initiativ på policynivå och gjort översyner inom området.[9] De ställningstaganden som gjorts i anslutning till dessa initiativ har inneburit en vidareutveckling av USA:s strategi, även om områdena som de senare initiativen omfattar är ungefär desamma som tidigare. I *The Comprehensive National Cybersecurity Initiative* (CNCI), som ursprungligen initierades under Bushadministrationens tid, redovisas ett åtgärdsprogram i tolv punkter. Dessa går bland annat ut på att kraftigt reducera antalet externa accesspunkter (inklusive kopplingar till Internet) från amerikanska myndigheters nätverk, att förstärka den tekniska övervakningen av federala system för att upptäcka intrång och att koppla ihop de federala organ som ansvarar för cybersäkerhet för att åstadkomma en gemensam lägesbild.[10] Inrättandet av NCCIC var en åtgärd för att realisera den sistnämnda punkten.
I den översyn som initierades av Obama lyftes behovet av en utvecklad responsplan för hantering av cyberincidenter fram.[11] Raden av initiativ visar att frågan om cybersäkerhet i hög grad är en levande fråga. Ytterligare ett exempel är att Obama har inrättat en ny funktion i Vita huset (Cybersecurity Coordinator) för att samordna strategi- och policyfrågor på nationell nivå.[12]

Nationell plan för hantering av IT-incidenter

Den senast fastställda nationella responsplanen, *Cyber Incident Annex*, är från 2004 och utgör en del av DHS samlade responsplan för händelser som hotar säkerheten på det egna territoriet.[13] En utvecklad responsplan, *National Cyber Incident Response Plan* (NCIRP), finns i utkast från september 2010.[14] Under övningen Cyberstorm III som genomfördes i slutet

[9] Bush: *Cyber Security and Monitoring*, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23), jan 2008. Detta dokument är inte öppet och har inte funnits tillgängligt under arbetet, men nämns eftersom övriga dokument om utvecklingen i USA från 2008 och framåt hänvisar till detta.
[10] *Comprehensive National Cybersecurity Initiative* (CNCI),The White House, mars 2010
[11] Obama: *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*. (“The 60-Day Review”). The White House, maj 2009
[12] Introducing the New Cybersecurity Coordinator, The White House Blog, 2009-12-22
[13] *Cyber Incident Annex*, DHS, dec 2004. Detta annex utgör en del av DHS National Response Plan. Sedan 2008 är denna samlade plan ersatt av *National Response Framework*.
[14] *National Cyber Incident Response Plan* (NCIRP), Interim Version, DHS, Sep 2010

av september 2010 prövades mekanismerna i NCIRP.[15] Utkastet ska därefter revideras baserat på erfarenheterna från övningen innan den fastställs. Som överordnat dokument för NCIRP finns *National Response Framework*, som anger generella principer för hur olika typer av påfrestningar på samhället ska hanteras.[16]

NCIRP utgör i första hand ett ramverk för samordning och omfattar såväl offentliga som privata aktörer. Tyngdpunkten ligger på hur samspelet mellan olika aktörer ska se ut snarare än vilka åtgärder som bör vidtas i olika situationer. Mycket av innehållet redovisar vilka de berörda aktörerna är samt vilka roller och vilka ansvar de har. Särskilt omfattande redovisas vilka roller och ansvar det relativt nyinrättade NCCIC har och hur samverkan mellan NCCIC och andra aktörer är tänkt att fungera. Generella krav och förväntningar på berörda aktörer redovisas också.

NCIRP täcker såväl förberedelser, respons som återuppbyggnad (åtminstone inledande åtgärder för återuppbyggnad) och beskriver arbetet i dessa olika faser i hanteringen av IT-incidenter. Fokus i planen ligger på det som kallas *Significant Cyber Incidents* och de mekanismer som då kan komma att behövas för att åstadkomma en ökad nationell samordning jämfört med normalläget vid hantering av mer vardagliga incidenter.

Det finns en skala för när dessa mekanismer utlöses, kallad National Cyber Risk Alert Level (NCRAL), se tabell nedan. I denna skala vägs hot, sårbarheter och potentiella konsekvenser in. Nivåerna bestäms i första hand av hur allvarliga konsekvenserna av en händelse bedöms bli. En händelse(-utveckling) anses vara ”Significant” när riskbedömningen placerar den på Level 2 ”Substantial”.

Level	Label	Description of Risk	Level of Response
1	**Severe**	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential.
2	**Substantial**	Observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with	Surged posture becomes indefinitely necessary, rather than only temporarily. The Department of Homeland Security (DHS) Secretary is engaged, and appropriate designation of authorities and

[15] *Preventing and Defending Against Cyber Attacks*, DHS, nov 2010

[16] *National Response Framework*, DHS/FEMA (Federal Emergency Management Agency), jan 2008

		indicators of higher levels of consequences impending	activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged.
3	**Elevated**	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slightly enhanced, operational posture.
4	**Guarded**	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation.

Tabell 1: National Cyber Risk Alert Levels (ur NCIRP)

Värt att notera är att det i USA på nationell nivå används olika skalor för gradering av hotnivån inom olika sektorer, exempelvis finns det skillnader mellan NCRAL och de skalor som används inom det militära försvaret. Arbete pågår dock för att jämka ihop de olika systemen.

3. Storbritannien

Organisation och aktörer

Inom Cabinet Office (”statsrådsberedningen”) finns Office of Cyber Security and Information Assurance (OCSIA). Denna funktion inrättade under 2009 som ett led i genomförandet av den cybersäkerhetsstrategi som beslutades samma år (se nedan) och benämndes ursprungligen Office of Cyber Security (OCS).[17] Förutom att samordna cybersäkerhetsfrågorna inom den brittiska regeringen ska OCSIA även bidra med strategisk inriktning för området, prioritera mellan olika åtgärder och leda genomförandet av den nationella cybersäkerhetsstrategin.

Inom Storbritanniens civila signalspaningsmyndighet, General Communications Headquarters (GCHQ)[18], har det relativt nyligen etablerats en särskild funktion för cybersäkerhetsfrågor, Cyber Security Operations Centre (CSOC). Enheten inrättades i september 2009 för att vara operativ under våren 2010. CSOC ska samordna skyddet av kritiska IT-system, följa utvecklingen inom området, upprätthålla en samlad lägesbild, analysera trender, sprida information samt förbättra samordningen av respons vid incidenter.

Ytterligare en aktör som arbetar med cybersäkerhet är Centre for the Protection of National Infrastructure (CPNI) som sorterar under Home Office (“inrikesdepartementet”). CPNI bistår bland annat med rådgivning till offentliga och privata aktörer om hur den kritiska infrastrukturen, varav informationsinfrastrukturen är en del, kan skyddas och säkras. Rådgivningen omfattar ett brett spektrum av säkerhetsfrågor, inklusive fysiskt skydd av system och anläggningar, personskydd och informationssäkerhet.

Inom CPNI finns också Combined Security Incident Response Team (CSIRTUK), en CERT-funktion som stöttar och ger råd till aktörer inom den privata sektorn som förvaltar och driver system som är en del av den kritiska infrastrukturen. Arbetet omfattar såväl förebyggande rådgivning som direkt stöd i samband med incidenter.

Inom GCHQ finns ytterligare en statlig CERT-funktion, GovCertUK som har till uppgift att stötta aktörer inom den offentliga sektorn i att hantera

---

[17] *Office of Cyber Security & Information Assurance*, information på Cabinet Office webbplats (http://www.cabinetoffice.gov.uk/intelligence-security-resilience/national-security/cyber-information-security.aspx)

[18] GCHQ sorterar under Cabinet Office

incidenter i sina informationssystem. GovCertUK bistår även med förebyggande rådgivning i syfte att minska sårbarheten i offentliga system och nätverk.

Nationell strategi

I juni 2009 presenterade den brittiska regeringen, för första gången, en nationell strategi för cybersäkerhet.[19] Syftet med strategin är att landet fullt ut ska kunna dra nytta av den digitala informations- och kommunikationstekniken. För att hantera de olika utmaningar som rör säkerheten i dessa system och nätverk lyfter strategin fram behoven av att engagera såväl offentliga som privata aktörer i arbetet, ökad medvetenhet om riskerna, satsningar på utbildning, anpassad lagstiftning och ett utvecklat internationellt samarbete.

Strategin går inte närmare in på hur förmågan att hantera de incidenter som ändå uppstår bör utvecklas. Däremot inrättas som en del i strategin två nya organ i den samlade nationella strukturen för cybersäkerhet. Det första, Cyber Security Operations Centre (CSOC, se även avsnittet ovan) har som ett av sina uttalade syften att förbättra incidenthanteringen. Det andra organet, OCSIA, syftar framförallt till att stärka den övergripande samordningen av cybersäkerhetsfrågor.

I den nationella säkerhetsstrategi som den brittiska regeringen presenterade under hösten 2010 pekas cyberattacker ut som en av de fyra högst prioriterade riskerna för Storbritannien de kommande åren, vid sidan av internationell terrorism, militära kriser i omvärlden samt stora olyckor och naturkatastrofer.[20] För att möta detta hot, vare sig det riktas mot staten, näringslivet eller befolkningen, föreslås i strategin ett särskilt utvecklingsprogram för cybersäkerhet (National Cyber Security Programme).

Det närmare innehållet i programmet redovisas i den försvars- och säkerhetsöversyn som presenterades kort efter den nationella säkerhetsstrategin.[21] Programmet innehåller bland annat åtgärder för att stävja cyberkriminalitet, satsningar för att täppa till brister i förmågan att

---

[19] *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*. Cabinet Office, June 2009. Sedan tidigare fanns det dock en nationell strategi för att säkerställa integritet, tillgänglighet och konfidentialitet i samhällets informationshantering (*National Information Assurance Strategy*. Cabinet Office, 2003 och 2007)

[20] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cabinet Office, okt 2010

[21] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, Cabinet Office, okt 2010

upptäcka och avvärja cyberattacker från andra stater, kriminella och terrorister, investeringar i ökad underrättelsekapacitet (i första hand vid CSOC inom GCHQ), forskningssatsningar samt förstärkning av landets kritiska informationsinfrastruktur.[22] Inom ramen för den sistnämnda åtgärden inrättas ett Cyber Infrastructure Team inom Department for Business, Innovation and Skills (”näringsdepartementet”). Detta för att förstärka statens samarbete med de privata aktörer som äger och driver delar av landets kritiska informationsinfrastruktur.

I programmet ingår också åtgärder för att stärka den militära förmågan att hantera cyberhot. Bland annat inrättas en expertgrupp inom försvarsministeriet, UK Defence Cyber Operations Group, som dels ska förbättra skyddet av militära informations- och kommunikationsnätverk, dels inrikta utvecklingen av militära offensiva förmågor inom området.

För att samordna och följa upp implementeringen av utvecklingsprogrammet i sin helhet inrättas en särskild sådan funktion inom OCSIA. I försvars- och säkerhetsöversyn framgår det att OCSIA ska förstärkas, men utan några närmare preciseringar. Med anledning av de åtgärder som följer av inriktningen i den nationella säkerhetsstrategin kommer en reviderad strategi för cybersäkerhet att presenteras under våren 2011.

Nationell plan för hantering av IT-incidenter

I det underlag som funnits tillgängligt om Storbritannien har det inte gått att identifiera någon nationell responsplan. Det som sägs om förmågan att hantera IT-incidenter i strategin från år 2009 utmynnar i förslaget om att inrätta två nya organisationer (CSOC och OCSIA).

GovCertUK har tagit fram ett dokument med riktlinjer för hantering av incidenter riktat till den offentliga sektorn.[23] Det handlar dock inte om någon plan för agerande utan är en vägledning för att klassificera en händelse enligt en skala över hur allvarlig den bedöms vara (Critical, Significant, Minor, Negligible Impact). I dokumentet beskrivs också olika typer av möjliga incidenter och ett antal begrepp definieras.

[22] Programmet ska löpa över fyra år och finansieras med totalt 650 miljoner pund.

[23] *Incident Response Guidelines*, GovCertUK, aug 2008

4. Finland

Organisation och aktörer

På regeringsnivå hanteras frågor om informationssäkerheten i samhället av Kommunikationsministeriet. Inom ministeriet finns bl.a. en särskild arbetsgrupp, med såväl offentliga som privata aktörer, vilka följer upp genomförandet av den nationella strategin inom området.

Under Kommunikationsministeriet sorterar Kommunikationsverket (Finnish Communiations Regulatory Authority, FICORA[24]**)** med uppgift att bl.a skapa ett informationssäkert samhälle och störningsfria kommunikationsnät. Kommunikationsverket är sedan november 2010 formellt utsedd till nationell myndighet för informationssäkerhet (i den betydelse detta begrepp används i internationella avtal och överenskommelser), med ansvar bl.a. för att bedöma säkerhet i fråga om informationssystem och telekommunikation och ge utlåtanden om säkerheten i system som finska företag tillhandahåller.[25] Detta är en av de åtgärder som föreslogs i den nationella informationssäkerhetsstrategin från 2008.

Inom FICORA är också den statliga CERT-funktionen, CERT-FI, organiserad. CERT-FI ska bl.a. ta emot rapportering om incidenter i kommunikationssystem och -nätverk, utarbeta och upprätthålla en lägesbild av hoten mot informationssäkerheten, informera om eventella hot och hjälpa till att lösa informationssäkerhetsproblem. CERT-FI har också en samordnande roll i förhållande till polis och övriga myndigheter samt arbetar förebyggande genom rekommendationer, råd och anvisningar om hur informationssäkerheten kan utvecklas.[26]

På myndighetssidan finns även Försörjningsberedskapscentralen (National Emergency Supply Agency, NESA) som sorterar under Handels- och industriministeriet. Målet för NESA är att minimera konsekvenserna av olika typer av kriser och allvarliga störningar i samhällets vitala funktioner. NESA planerar och genomför den operativa verksamhet som behövs för att upprätthålla och utveckla landets försörjningsberedskap (exempelvis beredskapslagring av energitillgångar och livsmedel).[27] Fokus för NESA

[24] Ungefär motsvarande svenska PTS och Radiotjänst i en och samma organisation.

[25] Justitieministeriet, pressmeddelande 2010-10-21 *Myndighetsuppgifter i anslutning till internationella förpliktelser som gäller informationssäkerhet ska preciseras.*

[26] CERT-FI svenskspråkiga webbplats

[27] För en närmare genomgång av Finlands samlade arbete med kris- och försörjningsberedskap, se *Strategi för tryggande av samhällets vitala funktioner,* Säkerhets- och försvarskommittén, Försvarsministeriet, nov 2006.

idag är att säkerställa nödvändig funktionalitet i samhällets tekniska system, särskilt i fråga om samhällets kritiska informationssystem. I detta syfte driver NESA bl.a. två reservdatacentraler.[28]

Inom den statliga sektorn finns också ett samordningsorgan för styrning och utveckling av informationssäkerhet inom statsförvaltningen. Detta organ, Ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) är organiserat inom Finansministeriet. Till uppgifterna hör bl.a. att samordna och prioritera statsförvaltningens interna arbete med informationssäkerhet, men även ta fram normer, anvisningar och rekommendationer inom området.

Nationell strategi

Finland var tidigt ute med en nationell strategi för informationssäkerhet, den första beslutades år 2003 och täckte perioden fram till och med 2007.[29] Under 2008 beslutades en ny nationell strategi för informationssäkerhet, denna gång för perioden 2009-2015.[30] I fokus för strategin står ökade kunskaper för informationssamhället i vardagen, utvecklad riskhantering för att trygga samhällets vitala funktioner samt ökad konkurrenskraft och internationellt samarbete.

Utifrån strategin togs även ett handlingsprogram fram med förslag på tio så kallade nyckelprojekt som praktiska verktyg för att implementera strategins inriktning.[31] I november 2009 fattade regeringen beslut om att genomföra handlingsprogrammet.[32] Bland nyckelprojekten handlar ett om att förtydliga hur ansvaret för informationssäkerhet hos leverantörer av tjänster som är vitala för samhället ser ut. Ett annat handlar om att förbättra riskhanteringen hos alla berörda aktörer genom utvecklade metoder för att identifiera risker och krav. Ett tredje projekt syftar till att öka förmågan att hantera störningar i samhällets informations- och kommunikationssystem och att säkra funktionalitet och kontinuitet inom dessa system. Kartläggning av trender inom området och en bedömning av hot mot informationssäkerheten ur ett finskt perspektiv är ytterligare ett exempel. Gemensamt för de olika

---

[28] Försörjningsberedskapscentralens svenskspråkiga webbplats

[29] *Nationell datasäkerhetsstrategi*, sep 2003

[30] *Statsrådets principbeslut om en nationell informationssäkerhetsstrategi "Trygg vardag i informationssamhället – Inte med tur utan med kunskap"*, Kommunikationsministeriet, 62/2008, 2008-12-04

[31] *Handlingsprogram – Statsrådets principbeslut om en nationell informationssäkerhetsstrategi. Utkast.* Kommunikationsministeriet, 2008-12-04

[32] *Strategin för informationssäkerhet ska börja verkställas*, Kommunikationsministeriet, pressmeddelande, 2009-11-19

projekten är att såväl offentliga som privata aktörer är engagerade. Projekten för att realisera strategin ska vara genomförda senast i februari 2011.

Vid sidan av strategin, som omfattar aktörer i olika delar av samhället, har den finska regeringen också fattat ett separat beslut om hur informationssäkerheten ska utvecklas inom statsförvaltningen. Underlaget för detta beslut togs fram av det ovan nämna samordningsorganet VAHTI.[33]

Nationell plan för hantering av IT-incidenter

I det underlag som funnits tillgängligt om Finland har det inte gått att identifiera någon nationell responsplan.

[33] *Statsrådets principbeslut om utvecklandet av informationssäkerheten inom statsförvaltningen – VAHTI 7/2009*, Pressmeddelande, Finansministeriet, 26-11-2009

5. Estland

Organisation och aktörer

Inom närings- och kommunikationsministeriet finns RISO (Department of State Information System) som samordnar estniska statens policyåtgärder inom IT-området och hanterar utvecklingen av de statliga informationssystemen, vilket inkluderar ett samlat myndighetsnät. RISO tar också fram underlag för lagstiftning inom området.

Det finns också en underavdelning till Närings- och kommunikationsministeriet, RIA[34], (Estonian Informatics Centre) vars primära uppgift är att samordna utveckling, upphandling och förvaltning av den statliga IT-infrastrukturen.

Inom RIA är även den statliga CERT-funktionen, CERT Estonia, organiserad, med ansvar för hantering av säkerhetsincidenter i datanätverk inom .ee-domänen. CERT Estonia sprider information och varningar, arbetar med förebyggande åtgärder, tar emot incidentrapportering, analyserar incidenter, hanterar själva eller ger stöd för hantering av incidenter och står vid behov för samordning av hantering av IT-incidenter.

Department for Critical Information Infrastructure Protection (CIIP) är en avdelning inom RIA som inrättades i oktober 2009. Uppgiften för CIIP är att bygga upp och förvalta ett system för att skydda Estlands kritiska infrastruktur inom informationsområdet. Avdelningen hanterar skydd av viktiga IT-system oavsett om de är offentliga eller privata. Uppgiften för CIIP är att samordna övergripande skyddsåtgärder inom den kritiska informationsinfrastrukturen. Det dagliga skyddet av systemen hanteras fortsatt av respektive systemägare.

Även Försvarsministeriet har en aktiv roll inom området. Exempelvis var det Försvarsministeriet som ledde den interdepartementala arbetsgrupp som tog fram strategin för cybersäkerhet. Inom Försvarsministeriet har också Cyber Security Council varit inordnat fram till årsskiftet 2010/11 (då ledningen av detta råd flyttades över till Närings- och kommunikationsministeriet). Rådet utgör en del av den estniska regeringens säkerhetskommitté (Security Committee) och inrättades som ett led i strategin för cybersäkerhet med huvudsyftet att förstärka samordningen mellan olika aktörer. Rådet har också ansvar för att utvärdera implementeringen och effekterna av denna strategi. Det finns en arbetsgrupp

[34] Riigi Infosüsteemide Arenduskeskus

med experter knuten till rådet som ska bistå med råd om informationssäkerhet.

Från Försvarsministeriet leds också arbetet med att bygga upp det så kallade cyberhemvärnet (Küberkaitseliit) som en del av det estniska hemvärnet (National Defence League, Kaitseliit). För försvaret är syftet att på ett organiserat sätt knyta till sig kompetens inom informationssäkerhetsområdet och inte minst att motivera unga att satsa på utbildning och yrkesverksamhet inom detta område. I förlängningen innebär detta en förbättrad bas för rekrytering. Verksamheten är i huvudsak inriktad på utbildning och övningar och för det senare ändamålet har specifika övningsmiljöer byggts upp och utrustats. Ambitionen är att bredda cyberhemvärnets möjligheter till att bistå inte bara vid IT-relaterade militära insatser utan även vid incidenter som riktar sig mot samhällets kritiska informationsinfrastruktur i stort.[35]

Nationell strategi

Estland har sedan länge haft en hög ambition att ta tillvara informationsteknologins möjligheter i utvecklingen av samhällets olika funktioner och var t.ex. ett av de första länderna att möjliggöra röstning till politiska församlingar via Internet. Frågan om informationssäkerhet har därför hög prioritet, något som ytterligare förstärkts efter de omfattande nätangreppen under våren 2007. Under 2008 antog den estniska regeringen en nationell strategi för cybersäkerhet.[36] På regeringsnivå hanteras frågan om informationssäkerhet av flera ministerier, men framförallt av Närings- och kommunikationsministeriet.

Det finns en rad policy- och inriktningsdokument som berör frågan om informationssäkerhet, bl.a. *Estonian IT Policy* (2003), *National Security Concept* (2004), *Estonian Information Society Strategy 2013* (2007) och *Information Security Interoperability Framework* (2007). Som nämnts ovan antogs år 2008 en strategi specifikt inriktad på cybersäkerhet, *Cyber Security Strategy*. Begreppet cybersäkerhet ges en bred tolkning i dokumentet och omfattar säkerhet kopplad till alla informations-, data- och mediatjänster som påverkar landets intressen och välstånd, dvs. den täcker ett bredare område än de delar som definieras som kritisk informationsinfrastruktur.

Strategin tar upp grundläggande principer för att säkerställa cybersäkerhet, hotbilden inom området, en nulägesbeskrivning av arbetet med cybersäkerhet samt målsättningar för en förstärkt cybersäkerhet och åtgärder kopplade till respektive mål. Strategin betonar fem strategiska mål:

[35] Intervju med Johannes Kert, Estonian Ministry of Defence, nov 2010

[36] Cyber Security Strategy, Estonian Ministry of Defence, 2008

- Utveckling och införande av ett system av åtgärder för förstärkt cybersäkerhet
- Ökad kunskapsnivå inom området cybersäkerhet
- Utvecklat legalt ramverk för att stödja cybersäkerhet
- Utvidgat internationellt samarbete
- Ökat medvetande om cybersäkerhet

Frågor om hantering av IT-incidenter tas i huvudsak upp i det första av dessa fem mål. Åtgärderna inom detta mål handlar om att öka skyddsnivån för den kritiska informationsinfrastrukturen, utveckla säkerhetsstärkande åtgärder och förstärka samverkan. Analyser av sårbarheter i den kritiska informationsinfrastrukturen i kombination med återkommande riskvärderingar ska användas i arbetet med att identifiera, utforma och förbereda adekvata motåtgärder i samband med IT-attacker och andra störningar. Handlingsplaner för de motåtgärder som kan krävas i händelse av en omfattande IT-incident ska förberedas. Ansvaret för de olika aktörerna att vidta preventiva åtgärder kommer att förtydligas och följas upp av berörda ministerier.

Sedan cybersäkerhetsstrategin beslutades har arbetet med att implementera den bland annat resulterat i att offentliga aktörer är skyldiga att tillse att deras IT-system uppfyller vissa säkerhetsnivåer. Systemet med säkerhetsnivåer (ISKE) innebär att alla system klassificeras utifrån hur känslig information de hanterar och därmed vilken skyddsnivå som krävs.[37]

Nationell plan för hantering av IT-incidenter

RIA har arbetat med att ta fram en plan för respons vid storskaliga IT-attacker. Målsättningen är att regeringen fastställer denna plan i slutet av 2010 eller tidigt under 2011. Dokumentet riktar sig till de offentliga och privata aktörer som tillhandahåller samhällsviktiga tjänster och kommer inte att publiceras öppet.[38]

Planen innehåller en definition av begreppet storskalig IT-attack, fastställda rutiner för agerande vid en storskalig IT-attack och ett förtydligande av hur ansvaret för att koordinera en storskalig IT-attack ser ut. Vad gäller rutiner för agerande är det framförallt formerna för rapportering som förtydligas i planen.

Tillämpningen av planen bestäms av hur allvarlig IT-attacken bedöms vara. Det är chefen för RIA, som utifrån förslag från chefen för den nationella

[37] Intervju med Toomas Viira, RIA/CIIP, nov 2010. ISKE är utvecklat baserat på den tyska motsvarigheten till säkerhetsstandard för IT-system (IT Grundschutz).
[38] Intervju med Toomas Viira, nov 2010

CERT-funktionen, avgör om en incident är att betrakta som en storskalig IT-attack. Ett sådant beslut innebär även att planen aktiveras. I samband med att planen tillämpas utökas RIA:s ordinarie möjligheter att agera, dels genom att medge undantag från de normala reglerna för offentlig upphandling, dels genom att RIA i samband med en storskalig IT-attack kan begära stöd och resurser från andra offentliga aktörer.

6. Tyskland

Organisation och aktörer

I Tyskland ansvarar inrikesministeriet (Bundesministerium des Innern, BMI) för övergripande frågor om informationssamhället, inklusive den offentliga informationsinfrastrukturen och IT-säkerheten i samhället.

Under inrikesministeriet finns en myndighet, Das Bundesamt für Sicherheit in der Informationstechnik (BSI), som arbetar med konkreta frågor inom IT-säkerhet på nationell nivå. Med syfte att öka IT-säkerheten generellt i Tyskland arbetar BSI bland annat med att analysera säkerhetsrisker, utveckla skyddsåtgärder samt informera om risker med användning av informationsteknik.

Inom BSI är även den statliga CERT-funktionen, CERT-Bund, organiserad. CERT-Bund har bland annat till uppgift att varna för IT-relaterade hot, informera om incidenter och att stödja övriga statliga aktörer vid incidenthantering. CERT-Bund utgör också kontaktpunkt för samverkan mellan den offentliga och privata sektorn, vilket är en bärande del av den tyska policyn för skyddet av kritisk infrastruktur.

Nationell strategi

Tyskland har sedan 2005 en plan för skydd av informationsinfrastrukturen.[39] Trots namnet utgör dokumentet i hög grad en strategi för området. Planen tar upp hot och risker mot den nationella informationsinfrastrukturen, strategiska mål och principiell ansvarsfördelning, med betoning av behovet av samverkan mellan aktörer från olika samhällssektorer, offentliga och privata (framförallt de som äger och förvaltar kritisk infrastruktur). För de tre uttalade strategiska målen: adekvat skydd av informationsinfrastrukturen (förebyggande), effektiv hantering av IT-incidenter (beredskap) och utvecklad nationell kompetens inom IT-säkerhet/utveckling av internationella standarder (långsiktig förmåga) uttalas ett antal delmål.

Vad gäller hantering av IT-incidenter beskrivs i planen även upprättandet av BSI och dess uppgifter inför, under och efter IT-händelser. BSI ska löpande kunna följa och värdera läget avseende IT-säkerhetssituationen på nationell nivå och i detta arbete kunna samverka med motsvarande organ såväl inom som utom landet. Vid behov ska BSI sprida information till berörda aktörer om aktuella hot och risker. Ett varningssystem ska säkerställa att information om nära förestående eller identifierade IT-incidenter når ut till berörda för att minska de skadliga effekterna. Vid hantering av IT-incidenter

[39] *National Plan for Information Infrastructure Protection (NPSI),* Federal Ministry of the Interior, okt 2005

har BSI en samordnande roll mellan såväl olika nivåer som sektorer i samhället. I de fall en stor del av den statliga sektorn påverkas och ordinarie mandat inom respektive sektor inte bedöms vara tillräckliga finns ett nationellt samordningsorgan (National Crisis Management Organization) under ledning av BMI, med flera ministerier representerade, som kan fatta beslut om utvidgade mandat till BSI. Planen betonar även vikten av väl förberedda lokala planer för krishantering och tydliga procedurer.

Nationell plan för hantering av IT-incidenter

Baserat på den nationella planen har det också tagits fram en plan för implementering som framförallt riktar sig till privata aktörer som äger och förvaltar delar av den samlade informationsinfrastrukturen.[40] Planen för implementering diskuterar förebyggande åtgärder, beredskap (inklusive respons) och långsiktig förmåga att hantera IT-incidenter på tre olika nivåer: inom enskilda företag/organisationer, inom en viss sektor eller för flera sektorer gemensamt. I fråga om beredskap tar planen upp behoven av att:

- kunna följa säkerhetsläget (lägesbild med identifiering av nivå/status),
- kunna varna och larma såväl internt som till andra berörda,
- upprätta tydliga rutiner för hantering av incidenter i fråga om ansvar, samverkan, kontaktpunkter och kanaler för kommunikation, samt
- kunna logga och lagra ”händelsebaserad” information för att i efterhand kunna rekonstruera och analysera händelserförlopp.

I denna plan läggs stor vikt vid behoven av kommunikation inom och mellan olika aktörer både vid ett normalläge och vid olika typer av incidenter. Bland annat beskrivs ett system med utpekade Single Points of Contacts (SPOCs) för olika sektorer som kanaliserar kontakterna ”uppåt” med BSI och ”nedåt” med respektive företag i en viss sektor.

I ett nästa steg av arbetet i Tyskland, vilket också aviserades i den ovan nämnda implementeringsplanen, upprättades ett antal arbetsgrupper med offentliga och privata aktörer för att fördjupa olika områden. Ett av dessa var hantering och skademinimering vid IT-incidenter. Arbetsgruppen för detta område har utarbetat och redovisat en tämligen detaljerad struktur för hur kommunikationen mellan företagen, respektive SPOC och BSI bör ske utifrån deras respektive roller. Anvisningarna är också uppdelade efter vilken situation som råder (normalläge eller olika faser av en incident). De tar också upp lämpliga sambandsmedel för kommunikation med hänsyn till i

[40] *CIP Implementation Plan of the National Plan for Information Infrastructure Protection*, Federal Ministry of the Interior, 2007

vilken situation kontakterna tas.[41] För en översikt över den struktur som redovisas, se tabellen nedan.

	Structures and parties involved	**Tasks/ operations**	**Means of communication**
Regular exchange of information	• BSI IT Situation Centre • Companies • SPOCs	• Compare notes • Crisis follow-up ("lessons learned")	• Meeting • Telephone • Conference call • Fax • E-mail • Communication platform • Video conference
IT security situation assessment	• BSI IT Situation Centre • Companies	• Assess situation • Prepare and circulate IT security situational picture	• Telephone • Conference call • Fax • E-mail • Video conference
Early crisis detection	• BSI IT Situation Centre • Companies • SPOCs	• Share information about IT security situation • Conduct analysis • Evaluate situation • Summarise information • Make decision • Alert • Sound the all-clear	• SMS • Telephone • Conference call • Fax • E-mail • Video conference *High availability:* • Mobile communications • Satellite telephone
Alerts and crisis mitigation	• Contact person in company or SPOC (depending on crisis situation) • BSI IT Situation Centre and other crisis situation centres • Relevant disaster control squads where necessary (state level)	• Provide recommendations • Execute crisis management • Coordinate countermeasures • Exchange information and recommendations • Coordination with other situation centres	• SMS • Telephone • Conference call • Fax • E-mail • Pager • Video conference *High availability:* • Mobile communications • Satellite telephone

Tabell 2: Aktörer, uppgifter och sambandsmedel för olika situationer (ur rapporten *Early Detection and Mitigation of IT Crises*, UP KRITIS Working Group 2, 2008)

[41] *Early Detection and Mitigation of IT Crises*, UP KRITIS Working Group 2 "Crisis Response and Mitigation", Federal Ministry of the Interior, dec 2008

7. Avslutning

Även om de studerade länderna skiljer sig åt i fråga om hur de väljer att organisera hanteringen av IT-incidenter finns det ett antal element som återkommer i de planer och andra dokument som tar upp hantering av IT-incidenter.

En sådan grupp av element handlar i stor grad om att prata samma språk i det utbyte som kan behövas i samband med hantering av en IT-incident:

- Definitioner av begrepp
- Skala över ”allvarlighetsgraden” av en händelse
- Indikatorer för klassificering av händelser enligt den angivna skalan

En annan grupp av element handlar i stor utsträckning om att förstå vilken roll respektive aktör som är inblandad i hanteringen av en incident har:

- Förtydligande av roller
- Förtydligande av ansvar hos respektive aktör
- Förtydligande av samspelet mellan berörda aktörer

En tredje grupp är snarast en fördjupning av punkten ”samspel” ovan, men ges så mycket utrymme i de dokument som studerats att den är värd en egen kommentar. Det handlar här om att i relativt konkreta termer beskriva hur själva interaktionen mellan olika aktörer bör gå till:

- Rapporteringsvägar
- Kommunikationsmedel

En fjärde och sista grupp av element som återkommer är olika typer av möjligheter till extraordinära befogenheter eller åtgärder vid hantering av särskilt allvarliga incidenter. Det kan antingen handla om direkta mekanismer, dvs. om en händelse klassas på ett visst sätt så medför det automatiskt utökade befogenheter för en viss aktör, exempelvis:

- Rätt att utnyttja andra aktörers resurser
- Undantag från regler om offentlig upphandling.

Det finns också exempel på indirekta mekanismer för utökade befogenheter, exempelvis genom att aktivera förberedda strukturer som snabbt kan sammankallas vid behov och har befogenheter att besluta om prioritering av knappa resurser, avsteg från ordinarie regelverk eller särskild finansiering.

8. Referenser

USA

Memorandum of agreement between the Department of Homeland Security and the Department of Defense regarding cybersecurity, publicerat 2010-10-13 (http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf).

The National Strategy to Secure Cyberspace, The White House, feb 2003

Cyber Security and Monitoring, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23), jan 2008. (Detta dokument är inte öppet och har inte funnits tillgängligt under arbetet, men nämns eftersom övriga dokument om utvecklingen i USA från 2008 och framåt hänvisar till detta.)

*Comprehensive National Cybersecurity Initiative (CNCI),*The White House, mars 2010

Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure ("The 60-Day Review"), The White House, maj 2009

Introducing the New Cybersecurity Coordinator, The White House Blog, 2009-12-22 (http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator)

Cyber Incident Annex, DHS, dec 2004 (http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf) Detta annex utgör en del av DHS National Response Plan. Sedan 2008 är denna samlade plan ersatt av National Response Framework, (http://www.fema.gov/emergency/nrf/)

National Cyber Incident Response Plan (NCIRP), Interim Version, DHS, Sep 2010 (http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf)

Preventing and Defending Against Cyber Attacks, DHS, nov 2010 (http://www.dhs.gov/xlibrary/assets/defending-against-cyber-attacks-november-2010.pdf)

National Response Framework, DHS/FEMA (Federal Emergency Management Agency), jan 2008 (http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf)

Storbritannien

Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, Cabinet Office, June 2009 (http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf).

National Information Assurance Strategy, Cabinet Office, 2007, (http://www.cabinetoffice.gov.uk/intelligence-security-resilience/national-security/cyber-information-security.aspx)

A Strong Britain in an Age of Uncertainty: The National Security Strategy, Cabinet Office, okt 2010 (http://www.official-documents.gov.uk/document/cm79/7953/7953.pdf)

Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, Cabinet Office, okt 2010 (http://www.official-documents.gov.uk/document/cm79/7948/7948.pdf)

Incident Response Guidelines, GovCertUK, aug 2008 (http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf)

Finland

Myndighetsuppgifter i anslutning till internationella förpliktelser som gäller informationssäkerhet ska preciseras, pressmeddelande från Justitieministeriet, 2010-10-21 (http://www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/sv.jsp?oid=309642)

CERT-FI svenskspråkiga webbplats (http://www.cert.fi/sv/index.html)

Strategi för tryggande av samhällets vitala funktioner, Säkerhets- och försvarskommittén, Försvarsministeriet, nov 2006, (http://www.defmin.fi/files/872/Strategi_for_tryggande_av_samhallets_vitala_funktioner_2006.pdf)

Försörjningsberedskapscentralens svenskspråkiga webbplats (http://www.se.nesa.fi/organisation/forsorjningsberedskapscentralen/)

Nationell datasäkerhetsstrategi, Förslag från delegationen för datasäkerhetsärenden2002-11-25, senare beslutad av regeringen 2003-09-04 (http://80.248.162.134/oliver/upl334-National_Datasakerhetsstrategi.pdf)

Statsrådets principbeslut om en nationell informationssäkerhetsstrategi ”Trygg vardag i informationssamhället – Inte med tur utan med kunskap”, Kommunikationsministeriet, 62/2008, 2008-12-04

Handlingsprogram – Statsrådets principbeslut om en nationell informationssäkerhetsstrategi, Utkast, Kommunikationsministeriet, 2008-12-04, (via www.lvm.fi)

Strategin för informationssäkerhet ska börja verkställas, Kommunikationsministeriet, pressmeddelande, 2009-11-19 (http://www.lvm.fi/web/sv/nyhet/view/986040)

Statsrådets principbeslut om utvecklandet av informationssäkerheten inom statsförvaltningen – VAHTI 7/2009, Pressmeddelande, Finansministeriet, 26-11-2009

Estland

Cyber Security Strategy, Estonian Ministry of Defence, 2008 (http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf)

Intervju med general Johannes Kert, Ministry Adviser, Estonian Ministry of Defence, 16 nov 2010.

Intervju med Toomas Viira, chef för avdelningen för Critical Information Infrastructure Protection inom RIA, 16 nov 2010.

Tyskland

National Plan for Information Infrastructure Protection (NPSI), Federal Ministry of the Interior, oktober 2005, (via www.bmi.bund.de)

CIP Implementation Plan of the National Plan for Information Infrastructure Protection, Federal Ministry of the Interior, 2007 (via www.bmi.bund.de)

Early Detection and Mitigation of IT Crises, UP KRITIS Working Group 2 “Crisis Response and Mitigation”, Federal Ministry of the Interior, dec 2008 (via www.bmi.bund.de)