Myndigheten för samhällsskydd och beredskap

Uppdragsredovisning

Datum	Diarienr
2010-01-13	2009-14471

Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter

Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap

(Fö2009/2162/SSK, 2009-10-29)

Förord

Den 29 oktober 2009 fick Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag av regeringen att i januari 2010 lämna förslag angående samhällets samlade förmåga att förebygga och hantera IT-incidenter. MSB:s svar redovisas i denna rapport. Arbetet har skett under koncentrerade former och synpunkter har inhämtats från myndigheter och andra aktörer med särskilt viktiga uppgifter och ansvar inom informationssäkerhetsområdet.

Samhällsutvecklingen har på några decennier gjort IT-systemen till en naturlig del av vardagen. Men utvecklingen har även medfört nya hot och risker. Informationssäkerheten måste hålla jämna steg med IT-utvecklingen för att fördelarna med IT ska kunna utnyttjas till sin fulla potential.

Att förebygga och ha förmåga att hantera IT-incidenter är en väsentlig del av Sveriges samhällsskydd och beredskap. För att förebygga och hantera IT-incidenter krävs en samlad insats i samhället och ett brett samarbete mellan aktörer av olika slag, som alla tar sitt ansvar.

Stockholm i januari 2010

Helena Lindberg
Generaldirektör

Richard Oehme
Chef enheten för samhällets informationssäkerhet

Publikationsnummer MSB 0162-10

ISBN 978-91-7383-075-1

Sammanfattning

Utvecklingen inom informationssäkerhetsområdet

Den gränslösa digitala informations- och kommunikationsinfrastrukturen behövs inom alla områden i dagens samhälle. Den ger väsentligt stöd till samhällsviktiga verksamheter och kritisk infrastruktur. Informationstekniken har på ett avgörande sätt ändrat villkoren för vårt sätt att leva och kommunicera.

I dag har en växande krets av statliga och icke-statliga aktörer – till exempel främmande underrättelsetjänster, kriminella grupper och terroristgrupper – skaffat sig förmåga att komma över, stjäla, förändra och förstöra information. Aktörerna riktar sitt intresse mot hela skalan av tänkbara mål; från enskilda medborgare och affärsverksamheter till samhällsviktiga verksamheter och kritisk infrastruktur. Allvarliga IT-incidenter kan därför ytterst komma att hota Sveriges säkerhet och svenska intressen.

Under de senaste åren har allt fler länder ökat sina förebyggande aktiviteter inom informationssäkerhetsområdet. Fler och fler skapar nationella strukturer för koordinering och samverkan och bygger upp omfattande kompetenser och resurser. Flera länder har skapat, eller står i begrepp att skapa, nya nationella samverkansfunktioner för att koordinera hanteringen av IT-incidenter.

Sverige har goda förutsättningar för att skapa starka strukturer för att förebygga och hantera IT-incidenter. I det svenska samhället, både i den privata och den offentliga sektorn, finns redan många av de nödvändiga kompetenser och resurser som möjliggör ett över tiden hållbart system för att förebygga och hantera IT-incidenter. De samlade resurserna behöver dock kompletteras för att de ska bli mer ändamålsenliga, samordnade, tillgängliga och rätt dimensionerade.

Det huvudsakliga förslaget – en nationell struktur

För att förebygga och hantera IT-incidenter bör det förebyggande informationssäkerhetsarbetet i samhället stärkas och samordnas ytterligare. Genomförandet av den nationella handlingsplanen för samhällets informationssäkerhet och en uppdatering av den nationella strategin för informationssäkerhet är av stor betydelse för detta arbete.

Myndigheten för samhällsskydd och beredskaps (MSB) huvudsakliga förslag är att skapa en sammanhållen struktur för att stärka den nationella förmågan att förebygga och hantera allvarliga IT-incidenter. En viktig del i denna nationella struktur är en central operativ samordningsfunktion för informationssäkerhet, som tar tillvara på och förstärker samhällets samlade resurser. Dessutom bör ett antal åtgärder genomföras för att öka förmågan till ledning, samverkan och samordning, öka informationsdelningen, skapa en gemensam lägesbild samt skapa en ökad responsförmåga.

Ett nationellt operativt samverkanscenter

MSB avser att inrätta ett nationellt operativt samverkanscenter för informationssäkerhet vid myndigheten. Samverkanscentrets uppgift ska vara att stödja samhällets förebyggande informationssäkerhetsarbete och att samordna hanteringen av allvarliga IT-incidenter.

Grunden för samverkanscentrets arbete bör vara samarbetet mellan de myndigheter som har operativa uppgifter inom informationssäkerhetsområdet. Vid behov ska experter från såväl offentliga och privata organisationer kunna verka vid centret. Samverkanscentret ska ha tillgång till säkra och ändamålsenliga lokaler, adekvat IT-stöd samt säker och redundant kommunikation.

En bärande princip är att det nationella operativa samverkanscentret för informationssäkerhet bör vara en central del av krishanteringssystemet. Centret bör ligga nära både den lägesbildsfunktion som redan finns vid MSB och det förebyggande arbete som sker inom ramen för myndighetens uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. På så sätt blir centret en integrerad del av krishanteringssystemet och det förebyggande informationssäkerhetsarbetet. Detta ökar förutsättningarna för att regeringen och andra berörda aktörer ska kunna få samlad information om läget.

Den privata sektorn äger och driver huvuddelen av den digitala informations- och kommunikationsinfrastrukturen. Det är därför viktigt att utveckla samverkansformer mellan det offentliga och det privata som bygger på ömsesidigt förtroende och ömsesidig nytta. Av den anledningen bör operatörer av samhällsviktig verksamhet och kritisk infrastruktur tillfälligt kunna beredas plats vid centret, beroende på händelsens karaktär.

Åtgärder för att förstärka den nationella strukturen

Utöver inrättande av ett nationellt operativt samverkanscenter bör följande åtgärder genomföras för att skapa den struktur som syftar till att öka den nationella förmågan att förebygga och hantera allvarliga IT-incidenter.

Åtgärder för att öka förmågan till ledning, samverkan och samordning:

- Regeringen bör ge en myndighet i uppdrag att med andra berörda aktörer närmare utreda hur en säker digital informations- och kommunikationsinfrastruktur för offentlig sektor, ett så kallat GovNet, kan skapas.
- MSB avser att i samråd med Försvarsmakten och Försvarets Radioanstalt närmare analysera hur befintliga eller kommande kryptosystem kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.

Åtgärder för att öka informationsdelning:

- MSB avser att verka för att det skapas en tydlig nationell struktur för privat-offentlig samverkan inom informationssäkerhetsområdet.
- MSB avser att utreda hur ett system för obligatorisk IT-incident-rapportering skulle kunna införas för statliga myndigheter. Övriga aktörer i samhället bör erbjudas att på frivillig grund delta i ett sådant system.
- Formerna för delning av underrättelser och annan information bör närmare utredas inom ramen för Samverkansgruppen för informationssäkerhet (SAMFI). Information som genereras utifrån underrättelse- och säkerhetstjänsternas olika myndighetsuppdrag kan vara mycket värdefull både i det förebyggande informationssäkerhetsarbetet och i hanteringen av allvarliga IT-incidenter.

Åtgärder för att skapa en gemensam lägesbild:

- MSB har för avsikt att, utifrån sitt uppdrag att reglera myndigheternas arbete med risk- och sårbarhetsanalyser (RSA), se till att relevanta informationssäkerhetsparametrar redovisas i analyserna.
- MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, utreda om ett mer strukturerat tekniskt intrångsdetekterings- och varningssystem för kritisk infrastruktur och samhällsviktig verksamhet kan införas i Sverige.

Åtgärder för att skapa en ökad responsförmåga:

- MSB avser att, i samråd med de myndigheter som ingår i SAMFI, ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras.
- MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter.
- MSB avser att fortsätta arbetet med att skapa en förtroendefull samverkansstruktur med samhällets aktörer för att praktiskt hantera allvarliga IT-incidenter.
- MSB avser att fortsätta arbetet med att genomföra regelbundna informationssäkerhetsövningar för att utveckla och utvärdera strukturer för hantering av allvarliga IT-incidenter.

Innehållsförteckning

1. Uppdrag, läsanvisning och begrepp

1.1 Uppdrag

Den 29 oktober 2009 fick Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag av regeringen att till den 15 januari 2010 lämna förslag angående samhällets samlade förmåga att förebygga och hantera IT-incidenter.[1]

> *”Myndigheten för samhällsskydd och beredskap ska lämna förslag på åtgärder för att förebygga och hantera IT-incidenter mot exempelvis samhällsviktig verksamhet, kritisk infrastruktur samt övriga verksamheter och system inom ramen för det tvärsektoriella informationssäkerhetsarbetet från normaltillstånd till kris. Förslagen ska omfatta ledning och samordning, informationsdelning, gemensam lägesbild samt responsförmåga. I detta arbete ska befintliga resurser och funktioner beaktas.*
>
> *Myndigheten för samhällsskydd och beredskap ska i arbetet inhämta berörda aktörers synpunkter. Kostnader för eventuella förslag ska redovisas samt hur dessa förslag ska finansieras inom ramen för befintliga budgetramar. Myndigheten för samhällsskydd och beredskap ska vidare hålla Regeringskansliet (Försvarsdepartementet) fortlöpande informerat under arbetets genomförande.”*

Uppdraget har genomförts av en avdelningsövergripande arbetsgrupp inom MSB under ledning av chefen för enheten för samhällets informationssäkerhet vid avdelningen för risk- och sårbarhetsreducerande arbete. Försvarsdepartementet har fortlöpande informerats om arbetets framskridande. Under arbetet har ett representativt urval av berörda samhällsaktörer kontaktats och beretts tillfälle att lämna synpunkter. MSB har här lagt särskild vikt vid de myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI). Se vidare bilaga 2 för information om SAMFI.

Frågor om informationssäkerhet har varit föremål för utredning under många år. I januari 2007 fick Krisberedskapsmyndigheten (KBM) i uppdrag av regeringen att utarbeta ett förslag till en handlingsplan för samhällets informationssäkerhet. Vid utarbetandet av åtgärdsförslagen i handlingsplanen togs hänsyn till bland annat InfoSäkutredningens betänkande *Säker information – Förslag till informationssäkerhetspolitik* (SOU 2005:42), regeringens proposition *Stärkt krisberedskap – för säkerhets skull* (prop. 2007/08:92) samt kommittédirektivet *En ny myndighet med ansvar för frågor om samhällets krisberedskap och säkerhet* (Dir. 2008:27). Arbetet med handlingsplanen bedrevs i samverkan med myndigheter, kommuner, landsting samt med näringslivet. Myndigheterna inom SAMFI tecknade samråd på handlingsplanen.

[1] Fö 2009/2162/SSK, se även bilaga 1

MSB har i sina förslag i det nu aktuella arbetet beaktat handlingsplanen och i allt väsentligt lagt den till grund för sina ställningstaganden.

1.2 Läsanvisning

Rapporten beskriver inledningsvis övergripande varför IT-incidenter har vuxit till ett allvarligt problem som ytterst kan hota grundläggande värden och den nationella säkerheten.

Därefter görs en övergripande jämförelse av internationella trender, hur några andra länder organiserar sig för att möta denna typ av hot och hur de hanterar denna typ av frågor.

Sedan följer en redogörelse för några centrala utgångspunkter i form av tidigare ställningstaganden från regeringen (kapitel 3) samt nödvändigheten i att nyttja samhällets samlade förmåga för att förebygga och hantera allvarliga IT-incidenter (kapitel 4).

I kapitel 5 redogörs för de åtgärder som föreslås för att skapa en sammanhållen struktur för att stärka den nationella förmågan att förebygga och hantera allvarliga IT-incidenter. Först beskrivs åtgärder med syfte att öka förmågan till ledning, samverkan och samordning, öka informationsdelningen, skapa en gemensam lägesbild samt att skapa en ökad responsförmåga. Därefter följer en närmare beskrivning av åtgärdsförslaget att inrätta ett nationellt operativt samverkanscenter för informationssäkerhet.

För tydlighetens skull inleds varje avsnitt i kapitel 5 med för rapporten viktiga principer. Dessa presenteras i skuggad text och följs av MSB:s åtgärdsförslag i separata textrutor.

Avslutningsvis redogörs i kapitel 6 för den föreslagna finansieringen.

1.3 Begrepp

Många centrala begrepp som är relaterade till att förebygga och hantera IT-incidenter saknar entydiga definitioner. I detta avsnitt beskrivs därför kortfattat ett antal av de viktigaste begreppen och hur de används i rapporten.

Informationssäkerhet
Rapportens terminologi följer SIS handbok *Terminologi för informationssäkerhet*.[2] Begreppet *informationssäkerhet* omfattar både administrativa och tekniska aspekter med avseende på konfidentialitet, riktighet och tillgänglighet av informationstillgångar. Som komplement till dessa tre aspekter används bland andra även begreppet spårbarhet.

Med *informationstillgångar* menas både information och de resurser som används för att hantera informationen. Informationssäkerhet handlar därmed

[2] *SIS handbok,* SIS HB 550 utgåva 3

om mer än att säkra informationssystem. Även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhets-begreppet.[3]

Kritisk infrastruktur och samhällsviktig verksamhet
Med begreppet *kritisk infrastruktur* avser EU-kommissionen ”anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet och människors ekonomiska eller sociala välfärd och där driftsstörning eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner”. [4]

För att verksamhet ska betraktas som *samhällsviktig* ur ett svenskt krisberedskapsperspektiv, måste minst ett av följande villkor vara uppfyllda[5]:

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

Digital informations- och kommunikationsinfrastruktur
Med *digital informations- och kommunikationsinfrastruktur* avses de tvärsektoriella och ansvarsnivåöverskridande IT-system som är en förutsättning för funktionaliteten i kritisk infrastruktur och samhällsviktig verksamhet, nationellt och internationellt, samt för samhällets normala funktion. I denna rapport används begreppet synonymt med det som i omvärlden benämns som ”cyberspace”.[6]

IT-incident
En *IT-incident* är en ”oönskad och oplanerad störning och drabbar eller påverkar ett IT-system. En IT-incident kan resultera i allvarliga negativa konsekvenser för ägaren av systemet.”[7]

---

[3] *SIS handbok*, SIS HB 550 utgåva 3
[4] EPCIP Direktivet, Artikel 2a
[5] Samhällsviktig verksamhet (MSB:s definition)
[6] ”Cyberspace” definieras i de amerikanska dokumenten National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) som ”the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people”. Se även *Cyberspace Policy Review* (”The 60-Day Review”).
[7] *Hantering av IT-incidenter – Vem gör vad och hur?* IT-kommissionen, Statskontoret, 2001

En IT-incident behöver inte vara ett resultat av brottsligt uppsåt. Orsaken kan vara bristande kompetens, misstag, felaktig användardokumentation eller liknande. En IT-incident kan också orsakas av tekniska sammanbrott och naturhändelser.

Med en *allvarlig, eller storskalig, IT-incident* avses en IT-incident som kan få omfattande negativa konsekvenser för hela samhället. Konsekvenserna kan vara ekonomiska, men kan även involvera skador på miljön eller påverka människors liv och hälsa. Ofta handlar det om en händelse som drabbar flera samhällssektorer, men även händelser som kan få mycket omfattande konsekvenser i en enskild samhällssektor räknas hit.

Operativ verksamhet
Med *operativ verksamhet* avses i denna rapport verksamhet i samband med allvarliga IT-incidenter samt krisrelaterade händelser inom informations-säkerhetsområdet på nationell nivå, t.ex. mottagandet av incidentrapportering, externa larm och förfrågningar. I detta ingår att kunna sammanställa och analysera lägesinformation om tillstånd, förväntad utveckling, vidtagna åtgärder och tillgängliga resurser samt utifrån detta utföra åtgärder i form av varningar och lägesbildsrapportering till berörda aktörer.

CERT
En *CERT* (Computer Emergency Response Team) kan utformas på en mängd olika sätt. I sin enklaste form är det en grupp IT-säkerhetsexperter vars huvudsakliga uppgift är att bevaka och hantera IT-incidenter. En *nationell CERT* är inte en renodlad teknisk funktion, snarare är det en kontaktpunkt för informationsdelning och koordinering inom landet och i ett internationellt sammanhang.[8] På nivån under CERT, myndighetsnivå eller lokal nivå, kallas motsvarande funktioner ofta *CSIRT* (Computer Security Incident Response Team).

[8] Enligt rapporten *Baseline capabilities for national / governmental CERTs* utgiven av Enisa i December 2009 har ungefär hälften av EU:s medlemsländer etablerat nationella CERT-funktioner. Enligt samma rapport pågår arbete i övriga länder med inrättandet.

2. Inledning

2.1 Hot mot den digitala informations- och kommunikationsinfrastrukturen

Utvecklingen under det senaste årtiondet har inneburit att IT-incidenter kan hota kritisk infrastruktur, samhällsviktiga verksamheter och Sveriges säkerhet. Det finns därför ett behov av att på ett helt annat sätt än vad som tidigare skett fokusera resurser på att förebygga och hantera IT-incidenter.

Den digitala informations- och kommunikationsinfrastrukturens föränderlighet när det gäller teknik, organisation, metoder och kompetens ställer särskilda krav på säkerhet och nationell IT-incidenthanteringsförmåga. Mängden hot, risker och sårbarheter fortsätter att öka medan förmågan att hantera dessa inte tillnärmelsevis ligger på samma nivå.

De flesta IT-incidenter är inte ett resultat av brottsligt uppsåt utan de uppstår på grund av bristande kompetens, misstag, felaktig användardokumentation eller liknande. Incidenter kan också orsakas av tekniska sammanbrott och naturhändelser. Men de antagonistiska hoten går inte att bortse ifrån, informationssystem utsätts regelbundet för angrepp. De flesta incidenter och angreppsförsök leder inte till allvarliga konsekvenser. Många av dem kan avvärjas snabbt genom de tekniska säkerhetsmekanismer som finns i bruk, genom egna åtgärder inom den drabbade organisationen eller genom kontakt med och hjälp från berörd nätoperatör eller motsvarande.

En växande krets av statliga och icke-statliga aktörer – till exempel främmande underrättelsetjänster, kriminella grupper och terroristgrupper – har dock skaffat sig förmåga att komma över, stjäla, förändra och förstöra information. Aktörerna riktar sitt intresse mot hela skalan av tänkbara mål; från enskilda medborgare och affärsverksamheter till kritisk infrastruktur och samhällsviktig verksamhet.

Hoten mot den globala, digitala informations- och kommunikationsinfrastrukturen är en av de allvarligaste ekonomiska och säkerhetsmässiga utmaningar som samhället idag står inför.

2.2 Förändrad gräns mellan det offentliga och det privata

Under de senaste årtiondena har gränserna mellan det offentliga och det privata förändrats alltmer. Privata aktörer äger och driver idag huvuddelen av den kritiska infrastrukturen. Det gäller även sådan verksamhet som traditionellt setts som statliga och offentliga kärnområden. Privata aktörers ansvar och verksamhet blir därmed allt viktigare i frågor som rör samhällsskydd och beredskap. Ansvarsfrågan blir särskilt viktig eftersom staten har det yttersta ansvaret gentemot medborgarna, samtidigt som krisens lösning ofta finns i näringslivet. Då en allt mindre del av den kritiska infrastrukturen och

samhällsviktiga verksamheten är statligt ägd innebär det i praktiken att staten har allt mindre direkt inflytande över hur denna infrastruktur hanteras, vilket i sin tur betyder att det blir allt viktigare att bygga en förtroendefull privat-offentlig samverkan.[9]

Behovet av en nära privat-offentlig samverkan är mycket tydligt när det gäller säkerhet i de IT-baserade system som används för att styra och kontrollera stora tekniska processer och system. (Dessa benämns även industriella kontrollsystem eller SCADA – Supervisory, Control, and Data Acquisition). Industriella kontrollsystem är avgörande för funktionen i kritisk infrastruktur och i samhällsviktiga verksamheter som vatten och avlopp, eldistribution, kärnkraft, olja och gas, transporter och tillverkningsindustri. Traditionellt har kontrollsystemen varit fysiskt isolerade och byggt på patentskyddad (privatägd) industriell teknik. Av kostnads- och effektivitetsskäl görs dock systemen nu i allt högre grad tillgängliga via publika nätverk som internet, och de bygger allt mer på samma öppna teknik, och standardprodukter, som vanliga IT-system. Resultatet är en radikalt förändrad riskbild under de senaste tio åren.[10]

Nätoperatörer och internetleverantörer är andra viktiga privata aktörer i detta sammanhang. De hanterar dagligen en stor mängd incidenter som för det mesta inte innebär något allvarligt hot. Samtidigt finns det ett antal incidenter, till exempel sofistikerade, riktade intrång, som kan få stora effekter i olika situationer. Sådana intrång är ofta mycket svåra att detektera. Det rör sig framförallt om kriminell verksamhet och främmande underrättelseverksamhet riktad mot olika mål i Sverige och mot svenska intressen. Kunskap om de tekniska detaljerna för sådana incidenter är värdefulla framförallt för nätägare och enskilda företag som behöver försvara sina egna nät mot liknande hot samt för det svenska polisväsendet och underrättelse- och säkerhetstjänsterna. Att finna sätt för att förmedla information om sådana mer kvalificerade hot till dem som behöver informationen är en utmaning för de flesta länder.

Det faktum att allt mer av den kritiska infrastrukturen och den samhällsviktiga verksamheten i huvudsak är privatägd påverkar i allra högsta grad möjligheter att i särskild ordning reglera vilken informationssäkerhetsnivå som bör finnas i olika verksamheter. Detta påverkar i sin tur hur IT-incidentförmågan ska byggas.

---

[9] *Mind the gap! Hur bygger vi broar mellan stat och näringsliv i arbetet med krisberedskap?* KBM:s temaserie 2005:8
Privat-offentlig samverkan – från idé till fungerande praktik. KBM:s temaserie 2006:2
Handbok i privat-offentlig samverkan inom området krisberedskap. KBM:s utbildningsserie 2008:5

[10] *Vägledning till ökad säkerhet i industriella kontrollsystem*. MSB, 2010
Strategy for Securing Control Systems. U.S. Department of Homeland Security (DHS), 2009

2.3 Att förebygga och hantera IT-incidenter

Utgångspunkten för en effektiv IT-incidenthantering är tillgång till kunskap om misstänkta angrepp och konstaterade incidenter. Detta gäller oavsett vilken ansvarsnivå som incidenten ska hanteras på eller inom vilken sektor.

De flesta vardagsincidenter hanteras idag nära användarna och enligt ansvarsprincipen. Det är ändamålsenligt, men hanteringen behöver bland annat kompletteras med en utvidgad rapportering för att kunna upprätthålla lokala, regionala, nationella och internationella lägesbilder.

Vid allvarliga incidenter, med nätangreppen mot Estland och Georgien som välkända exempel, krävs en samhällsövergripande lägesuppfattningsförmåga och samordning, samt en etablerad samverkan med experter för att hantera kritiska situationer.[11]

Storskaliga IT-incidenter blir snabbt till tvärsektoriella frågor som kräver ett samfällt agerande från många olika aktörer. Vid angrepp som drabbar kritisk infrastruktur och samhällsviktig verksamhet saknas det för närvarande möjlighet att skapa en samlad lägesbild. En sådan lägesbild handlar dels om att detektera verkliga och potentiella intrång, dels om att studera avvikelser från normalbilden. Idag förfogar nätoperatörerna och andra aktörer var och en över sin del av lägesbilden, men ingen av dem kan idag se helheten.

Några riktigt omfattande angrepp mot viktiga svenska samhällsfunktioner eller mot den svenska grenen av internet har hittills inte skett. Det är dock mycket troligt att ett sådant angrepp idag skulle hanteras som flera skilda incidenter, åtminstone under en inledande fas.

I dagsläget saknas en samlad bild av de incidenter som inträffar i samhällsviktiga och kritiska informationssystem. För att kunna skapa en sådan är det nödvändigt att kontinuerligt och systematiskt samla kunskap om både normalbild och avvikelser i systemen. Denna kunskap utgör en förutsättning för att i tid kunna upptäcka allvarliga IT-relaterade hot, varna och ha förmåga att hantera dessa.

2.4 En internationell utblick

2.4.1 Inledning

I det här avsnittet ges en övergripande internationell översikt av andra länders arbete med att förebygga och hantera IT-incidenter. InfoSäkutredningens andra delbetänkande[12] berörde ett flertal internationella aspekter som fortfarande äger giltighet; exempelvis nationella strategier, privat-offentlig samverkan, nationell och internationell lagstiftning, särskilda funktioner för

[11] *Sveriges beredskap mot nätangrepp*. KBM:s utbildningsserie 2008:1
[12] SOU 2004:32 *Informationssäkerhet i Sverige och internationellt – en översikt*

IT-incidenthantering, utbildning och medvetandehöjning. Under de senaste åren, efter utredningen, har olika nationers aktiviteter inom området ökat ytterligare och allt fler länder skapar övergripande strukturer för koordinering och samverkan samt bygger upp omfattande kompetenser och resurser. Ett antal länder har till exempel skapat, eller står i begrepp att skapa, nya centrala samhällsövergripande samverkansfunktioner för att koordinera den nationella hanteringen av IT-incidenter.[13]

2.4.2 Internationella aspekter på policy och strategi

Ett stort antal länder har numera en nationell strategi inom området. Exempelvis har Australien, Estland och Storbritannien lanserat nya strategier under det senaste året. Arbete i denna riktning pågår även i Frankrike, Japan, Kanada, Norge, Tyskland, USA, med flera länder. Idag betraktar de flesta länder säkerhet i den digitala informations- och kommunikationsinfrastrukturen (cybersecurity) som en av de stora nationella utmaningarna och den anses ha en hög nationell säkerhetspolitisk dignitet. Förklaringen till att den strategiska dimensionen betonas allt mer är att en storskalig IT-incident bedöms kunna få både omfattande ekonomiska konsekvenser och allvarligt störa funktionen hos kritisk infrastruktur i samhället. Exempelvis slår EU-kommissionen fast att den kritiska informationsinfrastrukturen är avgörande för ekonomin och samhällsutvecklingen inom EU, och att säkerheten och motståndskraften måste förbättras[14]. I sitt tal den 29 maj 2009 betecknade USA:s president den digitala infrastrukturen som en ”strategic national asset” och slog fast att skyddet av denna är en ”national security priority”.[15]

Många av de nationella strategierna liknar varandra genom att de betonar behovet av ökad privat-offentlig samverkan, nationella kampanjer för att öka medvetenheten på alla nivåer i samhället och skapandet av en säkerhetskultur. Andra teman som återkommer är behovet av mer internationell samverkan och informationsdelning, kompetenshöjning, samt ett tydligt nationellt ledarskap. De här områdena är hörnstenar i det förebyggande arbetet och när det gäller att hantera IT-incidenter.

Informationssäkerhetsfrågor i bred bemärkelse har även fått stor uppmärksamhet i många internationella fora de senaste åren. De 11 generella principer för Critical Information Infrastructure Protection (CIIP) som G8 godkände den 5 maj 2003[16], antogs i en något omarbetad form som en FN-resolution den 30 januari 2004. Sedan dess har ett antal resolutioner till-

[13] För information om internationella aspekter på skydd av kritisk informationsinfrastruktur, se även *International CIIP Handbook 2008/2009*. Center for Strategic Studies, ETH, Schweiz
[14] EU-kommissionens meddelande KOM(2009)149
[15] *Remarks by the President on Security Our Nation’s Cyber Infrastructure*. May 29, 2009, the White House, Office of the Press Secretary.
[16] *G8 Principles for Protecting Critical Information Infrastructures* (Adopted by the G8 Justice & Interior Ministers, May 2003)

kommit och 2008 gav OECD[17] ut en rekommendation för CIIP som bygger vidare på de tidigare resolutionerna. I det utkast till FN-resolution, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure*, daterat 20 november 2009 betonas återigen många av de principer som återfinns i de nationella strategierna ovan. Utkastet lyfter även fram behovet av att bekämpa IT-brottslighet och att uppdatera nationell lagstiftning, bland annat för att den ska harmonisera med internationella konventioner. Kopplingen till lagstiftning och IT-brottslighet är också mycket tydlig i FN-organet ITU:s arbete med informationssäkerhet (*Global Cybersecurity Agenda*)[18].

2.4.3 Internationella aspekter på IT-incidenthantering

Vikten av en kapacitet för IT-incidenthantering framhålls i ett flertal nationella strategier och i de rekommendationer från EU, FN, OECD och G8 som nämns ovan. Hantering av IT-incidenter kräver internationell samverkan. De strukturer som hittills byggts upp är främst förtroendebaserade nätverk för CERT-funktioner. Huvuddelen av samverkan är av teknisk art och två nätverk som är viktiga för Sveriges del är FIRST (Forum of Incident Response and Security Teams) och EGC (European Governmental CERTs). Det finns även en viss samverkan som omfattar både tekniska frågor och policyfrågor; exempelvis samarbetar Sverige, genom MSB och Post- och telestyrelsen (PTS), med ett antal nationer i gruppen IWWN (International Watch & Warning Network). Till detta kommer den samverkan som sker inom underrättelse- och säkerhetstjänsternas ordinarie utbyte med andra länder vilket också är betydelsefullt vid allvarliga IT-incidenter.

Behovet av ett tydligt nationellt ledarskap och en bättre koordinering på nationell nivå är något som återkommer i de flesta nationella strategier. Ett antal länder har skapat, eller kommer att skapa, nya centrala funktioner för att koordinera hanteringen av IT-incidenter och nationell samverkan. Några exempel på sådana länder är: Australien, Finland, Frankrike, Kanada, Norge, Storbritannien, Ungern och USA. De organisatoriska strukturerna skiljer sig visserligen något åt mellan länderna, men gemensamt är inrättandet av en central operativ funktion på nationell nivå som möjliggör användning av samhällets samlade resurser. De länder med strukturer som mest liknar det förslag som MSB föreslår i denna rapport är Kanada, där den centrala funktionen tillhör Public Safety Canada, och USA, där den centrala funktionen tillhör Department of Homeland Security (DHS)[19]. I båda dessa fall skapas en

[17] *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures (CIIP)*. OECD Ministerial Meeting on the Future of the Internet Economy. Seoul, Korea, 17-18 June, 2008
[18] *Global Cybersecurity Agenda*. International Telecommunication Union (ITU), 2008
[19] Se exempelvis http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm och http://www.publicsafety.gc.ca/prg/em/ccirc/abo-eng.aspx

närhet till det generella krishanteringssystemet och de funktioner som finns för att skapa en nationell lägesbild.

Två viktiga faktorer för att hantera IT-incidenter är beredskapsplaner och övningar. EU-kommissionen uppmanar därför EU:s medlemsstater att ta fram nationella beredskapsplaner och att ordna regelbundna övningar för insatser och återställning efter allvarliga IT-incidenter. Jämför även med den beredskapsplan (National Cyber Incident Respons Plan) som DHS för närvarande tar fram. Övningar är även ett bra sätt att stärka den internationella samverkan inom området. Tillsammans med länderna i det internationella nätverket IWWN kommer Sverige under hösten 2010 att delta i övningen Cyber Storm III, där MSB koordinerar det svenska deltagandet.

3. Tidigare ställningstaganden med relevans för denna rapport

I propositionen Stärkt krisberedskap – för säkerhets skull[20] konstateras att:

”En kris kännetecknas ofta av betydande komplexitet och stor osäkerhet. Vid kriser behöver samhällets resurser samordnas och samverka för att utnyttjas på ett effektivt sätt. Det räcker därför inte att inom det egna ansvarsområdet ha en uppfattning om vad som har hänt, vilka konsekvenserna blir och vad det ställer för krav på agerande. Det krävs dessutom en uppfattning om hur andra aktörer har uppfattat krisen och vilka åtgärder de vidtar. Det egna agerandet måste sättas in i ett bredare perspektiv. Därför finns det ett behov av samlade lägesbilder och samlad lägesuppfattning som sträcker sig över sektorsgränser och ansvarsnivåer, nationellt och i vissa fall även inom EU och internationellt.”

I proposition Ett användbart försvar[21] fastställs vidare att:

”Ett brett perspektiv på utmaningar och hot måste prägla den säkerhetspolitiska analysen. Utmaningar och hot mot vår säkerhet är föränderliga, gränslösa och komplexa.”

”Hot mot vårt allt mer IT-beroende informationssamhälle utgör också en del av den bredare hotbilden.”

Regeringen har slagit fast ett antal grundprinciper och mål för det nationella säkerhetsarbetet som ett arbete med uppbyggandet av en nationell IT-incidenthanteringsförmåga måste ta sin utgångspunkt i.

I propositionen Samverkan vid kris – för ett säkrare samhälle[22] uttalar regeringen följande:

”Nuvarande struktur för arbetet med Sveriges säkerhet är, trots de förändringar som genomförts under senare år, mycket komplex. Ansvaret för Sveriges säkerhet är fördelat på ett flertal departement, myndigheter och organisationer inom olika samhällssektorer. Sektorisering förstärks av det moderna samhällets allt högre krav på specialisering, kostnadseffektivitet, o.s.v. Emellertid kan en sektorisering försvåra möjligheterna att bedöma och begränsa konsekvenser av tvärsektoriell karaktär, liksom att göra avvägningar, prioriteringar och åtgärder utifrån den politiska ambitionen att stärka Sveriges säkerhet. För att möta de förändrade krav som ställs och ta tillvara de möjligheter som ges, föreslår regeringen ett förändrat sätt att fortlöpande arbeta med säkerhet”.

[20] Prop. 2007/08:92, sid. 19
[21] Prop. 2008/09:140, sid. 28
[22] Prop. 2005/06:133, sid. 48

Vidare konstateras att:

”Vi måste organisera vårt kontinuerliga arbete så att en helhetssyn på säkerhet främjas. Förutsättningarna för att ta tillvara synergier och undvika onödig dubblering av aktörer och verksamheter måste förbättras.”

I budgetpropositionen för 2009/10[23] uttrycker regeringen även följande:

”Regeringen anser att ett ändamålsenligt arbete med informationssäkerhet på nationell och internationell nivå är av central betydelse för samhällsutvecklingen. Det är också viktigt att arbeta förebyggande, ha en operativ förmåga samt att ha förmågan att snabbt kunna återgå till normalläget. Det är också viktigt att detta arbete bedrivs på EU-nivå och internationellt.

Inom ramen för regeringens översyn för en effektiv myndighetsförvaltning finns anledning att även se över informationssäkerhetsfrågorna.

Det finns ett behov av att samla resurserna för att skapa goda förutsättningar för att förebygga IT-incidenter liksom för att hantera dem när de inträffar. Rapporteringen av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behöver förbättras. Varje myndighet har enligt ansvarsprincipen att i första hand tillförsäkra den egna verksamheten en tillräcklig informationssäkerhet. Det överordnade ansvaret för informationssäkerhet på nationell nivå är idag uppdelat på ett flertal myndigheter vilket innebär att ansvaret är splittrat. Detta betyder att styrningen och samordningen av arbetet försvåras och att resurser riskerar att inte nyttjas på ett optimalt sätt. ”

Regeringen förtydligar sitt ovanstående ställningstagande ytterligare i det uppdrag[24] som den ställt till MSB och som MSB besvarar genom denna rapport.

[23] Budgetproposition 2009/10:1, Utgiftsområde 6
[24] Se vidare Bilaga 1

4. Utgångspunkt – nyttja samhällets samlade förmåga

4.1 Inledning

Sverige har goda förutsättningar för att skapa ett starkt nationellt system för IT-incidenthantering som omfattar såväl den privata som den offentliga sektorn. I det svenska samhället finns redan många av de nödvändiga kompetenser och resurser som möjliggör ett över tiden hållbart system för att möta IT-relaterade hot. De samlade resurserna behöver dock kompletteras för att de ska bli ändamålsenliga, samordnade, tillgängliga och rätt dimensionerade.

Grunden för allt informationssäkerhetsarbete är förebyggande åtgärder inom varje samhällssektor och på varje ansvarsnivå. För att förebygga och hantera allvarliga IT-händelser krävs både nationell mobilisering av samhällets samlade resurser och internationellt samarbete. För att ansvarsprincipen, kompletterad med skyldigheten att samverka, ska fungera behövs dessutom funktioner och mötesplatser för samverkan och samordning samt en överblick över vilka resurser som finns tillgängliga.

Faktiska förmågor är nödvändiga för att förebygga och hantera IT-incidenter. De resurser som finns bör kompletteras för att bättre kunna hantera extraordinära förhållanden orsakade av allvarliga IT-incidenter som hotar Sverige och svenska intressen.

Den större delen av den digitala informations- och kommunikationsinfrastrukturen ägs och drivs av den privata sektorn. Här finns också kompetens och erfarenhet. Därför är det viktigt att utveckla samverkansformer mellan det offentliga och det privata. Dessa måste bygga på ömsesidigt förtroende och ömsesidig nytta samt leda till att konkreta förmågor byggs upp. Föränderligheten och gränslösheten inom den digitala informations- och kommunikationsinfrastrukturen nödvändiggör även samarbete mellan nationella och internationella aktörer.

4.2 Nyttja samhällets samlade resurser och kompetenser

4.2.1 Samverkansstrukturer

Grunderna för användningen av samhällets samlade resurser är långsiktighet, ett gemensamt mervärde, ömsesidighet och en förtroendefull samverkan. Detta skapas i vardagligt samarbete, men också genom ändamålsenliga plattformar för samverkan. Dessa kan vara informella nätverk eller grupper av mer formell operativ samverkanskaraktär. I den nationella handlingsplanen för samhällets informationssäkerhet pekas på att staten bör utveckla samarbetet mellan

offentlig sektor och näringsliv ytterligare, framförallt i fråga om samhällsviktig verksamhet inom informationssäkerhetsområdet. [25]

Redan idag finns det inom vissa områden väl fungerande samarbeten kopplat till informationssäkerhet i vid bemärkelse. Kostnaderna för vardagliga IT-incidenter och det faktum att allvarligare IT-incidenter kan hota grundläggande värden, svenska intressen och Sveriges säkerhet gör dock att samarbetsstrukturerna måste kompletteras och utvecklas så att de kan utgöra grund för nödvändiga förmågor för att förebygga och hantera IT-incidenter. Kompletteringarna är såväl administrativa och organisatoriska som tekniska. De innefattar också information och åtgärder för att öka medvetandet om utmaningar inom informationssäkerhetsområdet och om vilka åtgärder som alla kan bidra med.

Inom den offentliga sfären spelar SAMFI en särskilt viktig roll. SAMFI har till syfte att skapa samverkan mellan de statliga myndigheter som har särskilda uppgifter inom sakområdet. De myndigheter som finns representerade är MSB, PTS, Rikskriminalpolisen (RKP) och Säkerhetspolisen (SÄPO), Försvarets radioanstalt (FRA), Försvarsmakten (FM) samt Försvarets materielverk (FMV). I olika arbetsgrupper kopplade till SAMFI deltar också andra offentliga aktörer såväl som näringsliv och ideella organisationer.

Det finns även ett antal grupper som arbetar med privat-offentlig samverkan. En strategisk grupp är *Informationssäkerhetsrådet* som ska bistå MSB med:

- Information om utvecklingstrender inom området informationssäkerhet, det vill säga skydd av information och säkring av informationssystem.
- Synpunkter på inriktning, prioritering och genomförande av MSB:s arbete inom området.
- Kvalitetssäkring av, och skapande av trovärdighet för, MSB:s arbete genom rätt sammansättning och koppling till vitala samhällsfunktioner.
- Spridning av information om MSB:s arbete med informationssäkerhet i omvärlden.

Ledamöterna i Informationssäkerhetsrådet ska med sin kompetens täcka vitala delar av de samhällsfunktioner som har betydelse för samhällets informationssäkerhetsarbete. Ett viktigt kriterium är att ledamöterna är etablerade som sakkunniga i omvärlden och har ett brett kontaktnät. De ska också ha förmåga att se frågorna både ett nationellt och internationellt perspektiv.

En annan beprövad samverkansform är konceptet FIDI (Forum för informationsdelning avseende informationssäkerhet). MSB har framgångsrikt använt

[25] *Samhällets informationssäkerhet – Handlingsplan 2008*. KBM. Handlingsplanen förvaltas nu av MSB.

FIDI inom SCADA-området, forumet *FIDI-SC*. FIDI-konceptet baseras på riktlinjer och erfarenheter från brittiska Centre for the Protection of National Infrastructure (CPNI) och innebär att myndigheter och industri delar information om risker och sårbarheter. Syftet med samverkan är bland annat att skapa en mekanism där en enskild organisation kan ta lärdom av andras erfarenheter, misstag och framgångar för att höja sin egen säkerhetsnivå (se vidare avsnitt 5.3.3). En annan framgångsrik privat-offentlig samverkansgrupp är Nationella telesamverkansgruppen (NTSG) som administreras av PTS. Gruppen är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Gruppen består av organisationer som har stor möjlighet att påverka den kritiska nationella infrastrukturen för elektronisk kommunikation.[26]

Huvuddelen av Sveriges kritiska informationsinfrastruktur ägs och drivs av privata aktörer. Där återfinns en betydande del av kompetensen och de internationella kontakterna. Nätoperatörerna har ett väl etablerat system för samverkan. De internetrelaterade incidenter som sker idag hanteras till största delen av nätoperatörerna, efter att ha kontaktats av drabbade nätägare. Bland dessa aktörer finns det sedan länge samverkansformer som bedöms fungera mycket väl. Nätoperatörerna undersöker dagligen en mängd kundklagomål och har för det ändamålet så kallade abusefunktioner. Mellan dessa finns det ett fungerande vardagssamarbete och etablerade kontaktvägar med bland annat polisen.

Hanteringen av kundklagomål, som spänner över hela registret från skräppostanmälningar till DDoS-attacker, är vanligen en prioriterad del av nätoperatörens arbete. Många incidenter stjäl dyrbar bandbredd, ställer till problem i operatörens egen e-posthantering eller utsätter operatörens nät för risken att bli blockerat hos andra operatörer om det visar sig att nätet inte är tillräckligt rensat från attackerande datorer eller skräppostavsändare.

Sammanslutningen Föreningen svenskt operatörsforum (SOF) skickar varje månad ut en lista (den så kallade abuselistan) med kontaktinformation till de olika operatörerna via knutpunktsbolaget Netnod. Att Netnod har tagit på sig denna uppgift hör ihop med den viktiga roll som företaget har för Internet i Sverige, både som centralpunkt för trafikutbyte mellan svenska nätoperatörer och som en aktör med internationellt erkänd expertis på området.

Bankernas Säkerhetskommitté (BSK) har det övergripande ansvaret för det bankgemensamma säkerhetsarbete som bedrivs inom Svenska Bankföreningen. Kommittén är ett beslutsorgan för säkerhetsrekommendationer och ansvarar även för att löpande analysera och bedöma den branschgemensamma hotbilden mot bankernas verksamhet. Detta arbete inkluderar även

[26] Se vidare http://www.pts.se/upload/Faktablad/SE/faktablad-ntsg-2008-09-19.pdf

informationssäkerhet vilket är en viktig del av BSK:s arbete. Det finns en särskild arbetsgrupp inom kommittén som arbetar med informationssäkerhetsfrågor.

Ytterligare ett viktigt samverkansforum är den DNS-referensgrupp som Stiftelsen för Internetinfrastruktur (.SE) håller i. Där deltar alla de stora nätoperatörer som driver särskilt betydelsefulla DNS-servrar i Sverige, i dagsläget runt 15 stycken.

Inom annan samhällsviktig verksamhet i den privata sfären finns det inte en lika omfattande aktiv samverkan som hos nätoperatörer och nätägare. Vad som däremot finns är mer allmänna forum som gör ett betydelsefullt arbete genom att erbjuda utbildningar och engagera sig i andra medvetandehöjande åtgärder. Ett sådant forum är Näringslivets säkerhetsdelegation (NSD) som samlar ett stort antal personer från olika delar av det svenska näringslivet. Ett annat exempel är föreningen SIG Security som organiserar personer som är verksamma inom informationssäkerhetsområdet samt Dataföreningen.

Sammantaget finns det ett väl utvecklat samarbete inom vissa sektorer. Inom det stora flertalet sektorer är samarbetet dock endast i sin linda. Vad som framförallt saknas är ett övergripande nationellt operativt samverkansforum samt regionala och sektorsvisa forum.

4.2.2 Ansvarsfördelning

Tydlighet vad gäller ansvar och roller är en förutsättning för ett effektivt förebyggande arbete. En annan förutsättning är en ändamålsenlig samverkan inom offentlig sektor och mellan offentlig och privat sektor.

Idag har en rad myndigheter ett reglerat ansvar för olika centrala frågor som är av betydelse för hanteringen av IT-incidenter. Det finns både ett övergripande ansvar och ett ansvar för olika mer konkreta och avgränsade sakfrågor. För att kunna nyttja samhällets kompetenser och resurser och göra dem ändamålsenliga, samordnade, tillgängliga, gripbara och rätt dimensionerade är det nödvändigt att identifiera, nyttja och samordna det handlingsutrymme den rättsliga regleringen inom informationssäkerhets- och krishanteringsområdet ger.

Statliga myndigheters skyldighet att vidta åtgärder inom informationssäkerhetsområdet och inom krisberedskapsområdet i övrigt framgår av förordningen (2006:942) om krisberedskap och höjd beredskap (nedan kallad krisberedskapsförordningen). Med stöd av bemyndigande i krisberedskapsförordningen har MSB utfärdat ytterligare föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10). Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) samt lagen (2003:389) om

elektronisk kommunikation bör också nämnas i detta sammanhang.[27] Särskilda uppgifter för enskilda myndigheter framgår av respektive myndighets instruktion.

Enligt Krisberedskapsförordningen har myndigheter en skyldighet att säkerställa att de egna informationshanteringssystemen uppfyller sådana säkerhetskrav att verksamheten kan genomföras på ett tillfredsställande sätt[28], att genomföra risk- och sårbarhetsanalyser i syfte att stärka sin egen och samhällets krisberedskap[29] samt att vidta skyddsåtgärder enligt säkerhetsskyddslagstiftningen.

Utöver dessa allmänna åligganden har, som nämnts ovan, vissa myndigheter särskilt utpekade uppgifter inom området för informationssäkerhet och krisberedskap. Hit hör Rikspolisstyrelsen (RPS), PTS, FRA, FM och MSB. I korthet kan konstateras att RPS har tillsynsansvar för frågor med anknytning till säkerhetsskyddet. Hithörande föreskriftsrätt delar RPS med FM. PTS har tillsynsansvar för elektronisk kommunikation och har i särskild uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer.

FRA har särskilt ansvar för att bedriva signalspaning och utföra matematiska bedömningar av kryptosystem. Vidare ska FRA ha hög teknisk kompetens inom informationssäkerhetsområdet för att särskilt kunna stödja vid nationella kriser med IT-inslag, samt ge annat tekniskt stöd. FRA får efter begäran också genomföra IT-säkerhetsanalyser åt vissa statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- och försvarspolitiskt avseende.

FM ansvarar för att vissa försvarsrelaterade myndigheter tilldelas säkra kryptografiska funktioner. Vidare ska FM särskilt leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information. Det här beskrivna formella ansvaret är i princip knutet till en viss miljö, elektronisk kommunikation, eller skydd av viss typ av information, säkerhetsskydd. Slutligen ska MSB säkerställa en helhetssyn. Myndigheten har därför till uppgift att stödja och samordna arbetet med informationssäkerheten i hela samhället samt att utfärda föreskrifter både vad gäller informationssäkerhet och risk- och sårbarhetsanalyser.

Kombinationen av en myndighet med ett utpekat ansvar att samordna och stödja och myndigheter med både formellt ansvar för, och spetskompetens inom, särskilt utpekade områden skapar goda möjligheter att på ett ändamålsenligt sätt kunna dra nytta av och vidareutveckla de resurser som samhället idag har. MSB:s bedömning är att det rättsliga regelverket ger handlingsutrymme för att förebygga och hantera IT-incidenter.

---

[27] Uppräkningen ger inte anspråk på fullständighet utan kan kompletteras ytterligare.
[28] 30a§ Förordning (2006:942) om krisberedskap och höjd beredskap
[29] 9§ Förordning (2006:942) om krisberedskap och höjd beredskap

4.3 Ett förebyggande informationssäkerhetsarbete

4.3.1 Strategi och handlingsplan för samhällets informationssäkerhet

En tydlig strategi med bred förankring är en viktig förutsättning för ett nationellt förebyggande informationssäkerhetsarbete. Den strategi för samhällets informationssäkerhet som MSB för närvarande förbereder på uppdrag av regeringen omfattar nationella mål med informationssäkerhet utifrån ett brett perspektiv.

Handlingsplanen för samhällets informationssäkerhet, som togs fram i samråd med SAMFI våren 2008 och förvaltas av MSB, är en viktig grund för inriktningen av det förebyggande informationssäkerhetsarbetet. Handlingsplanen består av ett 50-tal åtgärdsförslag. Den pekar på behov av sektorsövergripande och tvärsektoriellt arbete samt heltäckande föreskrifter på informationssäkerhetsområdet. I planen framhålls att det grundläggande säkerhetsarbetet bör ges prioritet. Vidare lyfter handlingsplanen också fram behovet av en nationell samordning för att kunna hantera omfattande IT-incidenter. Också behovet av kompetens- och medvetandehöjning framhålls mycket tydligt.[30]

4.3.2 Medvetandehöjning

En god förmåga att hantera IT-incidenter börjar hos den enskilda användaren. Därför bygger användningen av samhällets samlade resurser på informerade och kompetenta användare. Informations- och utbildningsinsatser för att höja människors säkerhetsmedvetande är därför viktiga framgångsfaktorer.

Arbete med medvetandehöjning handlar om att identifiera och stötta olika verksamheter där det finns behov. Som exempel kan kampanjen ”Surfa lugnt”[31] nämnas. Kampanjen riktar sig främst till ungdomar och deras föräldrar och spelar därför en viktig roll i strävan mot ett ökat informationssäkerhetsmedvetande i det svenska samhället. Kampanjen arbetar också med folkbildningen i Sverige som har en viktig roll för medvetandehöjning.

4.3.3 Rekommendationer för förebyggande informationssäkerhetsarbete

Det krävs tydlig styrning för av att förebygga kriser och allvarliga incidenter. Rekommendationer i form av föreskrifter och råd spelar en mycket viktig roll som stöd till hela samhället.

Flera aktörer har till uppgift att utfärda föreskrifter och rekommendationer för förebyggande informationssäkerhet. Exempelvis utfärdar Säkerhetspolisen

---

[30] *Samhällets informationssäkerhet – Handlingsplan 2008*. KBM. Handlingsplanen förvaltas nu av MSB.
[31] Se vidare http://surfalugnt.se/

föreskrifter och rekommendationer utifrån sin roll kopplat till säkerhetsskyddslagen. PTS gör motsvarande inom sitt ansvarsområde elektronisk kommunikation och kopplat till internetanvändning (se vidare avsnitt 4.2.2).

MSB utgår i sina rekommendationer och föreskrifter för statliga myndigheter om informationssäkerhet från vedertagna standarder och väl prövade synsätt. De standarder som föreskrivs eller rekommenderas har ett processorienterat synsätt, täcker hela informationssäkerhetsområdet och utgör ett kvalitetssystem för ständig förbättring och kontinuerlig anpassning till respektive organisations behov. Det är väsentligt att ett sådant synsätt främjas inom alla delar av samhället. Inte minst av det skälet att IT-användningen inte är en isolerad företeelse för varje enskild organisation. Sambanden mellan organisationer och det nationella och internationella perspektivet är påtagliga och ställer därför krav på gemensamma synsätt och normer.

MSB avser vidare att, bland annat inom ramen för projektet SVISA (Stöd för verksamheters informationssäkerhetsarbete) utveckla rekommendationer och stöd för förebyggande arbete i sin helhet, men naturligtvis även med särskild inriktning på hantering av IT-incidenter. Rekommendationerna omfattar också stöd för användning av verifierat säkra IT-produkter, genom modeller för kravställning vid upphandling, stöd för certifiering av säkerhet i IT-produkter med mera.

5. Förslaget

5.1 Sammanfattande förslag

För att förebygga och hantera IT-incidenter bör det förebyggande informationssäkerhetsarbetet i samhället stärkas och samordnas ytterligare. Genomförandet av den nationella handlingsplanen för informationssäkerhet och en uppdatering av den nationella strategin är av stor betydelse för detta arbete. Vidare bör det skapas en sammanhållen struktur för att stärka den nationella förmågan att förebygga och hantera allvarliga IT-incidenter riktade mot samhällsviktig verksamhet och kritisk infrastruktur.

En väsentlig del i den nationella strukturen utgörs av en central operativ funktion som tar tillvara på och förstärker samhällets samlade resurser. Utöver inrättandet av den centrala operativa funktionen bör ett antal åtgärder genomföras för att stärka strukturen och därigenom öka förmågan till ledning, samverkan och samordning, informationsdelning, gemensam lägesbild och respons.

MSB avser att inrätta ett nationellt operativt samverkanscenter för informationssäkerhet vid myndigheten. Samverkanscentrets uppgift ska vara att stödja samhällets förebyggande informationssäkerhetsarbete och att samordna hanteringen av allvarliga IT-incidenter. Grunden för samverkanscentrets arbete bör vara samarbetet mellan de myndigheter som har operativa uppgifter inom informationssäkerhetsområdet. Vid behov ska experter både från offentliga och privata organisationer kunna verka vid centret. Samverkanscentret ska ha tillgång till säkra och ändamålsenliga lokaler, adekvat IT-stöd samt säker och redundant kommunikation.

MSB anser att nedanstående ytterligare åtgärder bör genomföras för att skapa den struktur som syftar till att öka den nationella förmågan att förebygga och hantera allvarliga IT-incidenter.

Åtgärder för att öka förmågan till ledning, samverkan och samordning:

- Regeringen bör ge en myndighet i uppdrag att med andra berörda aktörer närmare utreda hur en säker digital informations- och kommunikationsinfrastruktur för offentlig sektor, ett så kallat GovNet, kan skapas.
- MSB avser att i samråd med FM och FRA närmare analysera hur befintliga eller kommande kryptosystem kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.

Åtgärder för att öka informationsdelning:

- MSB avser att verka för att det skapas en tydlig nationell struktur för privat-offentlig samverkan inom informationssäkerhetsområdet.

- MSB avser att utreda hur ett system för obligatorisk IT-incident-rapportering skulle kunna införas för statliga myndigheter. Övriga aktörer i samhället bör erbjudas att på frivillig grund delta i ett sådant system.
- Formerna för delning av underrättelser och annan information bör närmare utredas inom ramen för SAMFI. Information som genereras utifrån underrättelse- och säkerhetstjänsternas olika myndighets-uppdrag kan vara mycket värdefull både i det förebyggande informationssäkerhetsarbetet och i hanteringen av allvarliga IT-incidenter.

Åtgärder för att skapa en gemensam lägesbild:

- MSB har för avsikt att, utifrån sitt uppdrag att reglera myndigheternas arbete med risk- och sårbarhetsanalyser (RSA), se till att relevanta informationssäkerhetsparametrar redovisas i analyserna.
- MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, utreda om ett mer strukturerat tekniskt intrångsdetekterings- och varningssystem för kritisk infrastruktur och samhällsviktig verksamhet kan införas i Sverige.

Åtgärder för att skapa en ökad responsförmåga:

- MSB avser att, i samråd med de myndigheter som ingår i SAMFI, ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras.
- MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter.
- MSB avser att fortsätta arbetet med att skapa en förtroendefull samverkansstruktur med samhällets aktörer för att praktiskt hantera allvarliga IT-incidenter.
- MSB avser att fortsätta arbetet med att genomföra regelbundna informationssäkerhetsövningar för att utveckla och utvärdera strukturer för hantering av allvarliga IT-incidenter.

5.2 Ledning, samverkan och samordning

Principer: Ansvarsprincipen är grunden för att förebygga och hantera IT-incidenter i samhället.

Alla aktörer i samhället bör ha en förmåga att snabbt kunna agera och informera vid allvarliga IT-incidenter. Detta bör bygga på ett förberett och övat nyttjande av relevanta resurser i samhället.

All samverkan och samordning vid en allvarlig IT-incident bör bygga på redan befintliga samverkansstrukturer. Det är oftast inte möjligt att skapa nya strukturer vid en kris.

Åtgärder: För att garantera en grundnivå av säker kommunikation mellan myndigheter från normaltillstånd till kris, även under omfattande IT-störningar, bör en säker digital informations- och kommunikationsinfrastruktur för offentlig sektor skapas, ett så kallat *GovNet*. Regeringen bör ge en myndighet i uppdrag att närmare utreda frågan med andra berörda aktörer.

Ledning, samverkan och samordning förutsätter att den information som aktörer hanterar och förmedlar kan ges ett skydd mot obehörig insyn och påverkan. Det bör för detta informationsutbyte finnas *kryptosystem* som är nationellt godkända för skydd av skyddsvärd eller sekretessbelagd information. I syfte att kunna stödja de aktörer som har behov av skyddad informationsöverföring för IT-incidenthantering har MSB för avsikt att i samråd med FM och FRA närmare analysera hur befintliga eller kommande kryptosystem kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.

5.2.1 Ansvarsprincipen

Informationssäkerhetsarbetet i Sverige bedrivs tvärsektoriellt och styrs av ansvarsprincipen. I propositionen Stärkt krisberedskap – för säkerhets skull tydliggör regeringen ansvarsprincipen och behovet av sektorsövergripande samverkan[32]:

> *”I ansvarsprincipen, som innebär att den som bedriver verksamhet under normala förhållanden har motsvarande ansvar även under krissituationer, ingår även att initiera och bedriva sektorsövergripande samverkan. Förmågan att samverka över sektorsgränserna bör förbättras.”*

I samma proposition uttrycker regeringen följande:

> *”Krisberedskapsarbetet bygger bl.a. på den s.k. ansvarsprincipen som innebär att den som har ett ansvar för en verksamhet under normala förhållanden har motsvarande ansvar även under krissituationer. Ansvaret inkluderar därmed att i förebyggande syfte*

[32] 2007/08:92, sid. 37 och 38

vidta de åtgärder som krävs för att både skapa robusthet och krishanteringsförmåga. Ansvaret innebär också att under en kris kunna bedriva verksamhet och hantera situationer så långt det är möjligt. Det finns ofta ett behov av att den som är ansvarig för en verksamhet samverkar, såväl inom sin sektor som utanför för att kunna lösa uppgiften. Därför innebär ansvarsprincipen också ett ansvar för varje aktör att samverka med andra."

I Förordning (2006:942) om krisberedskap och höjd beredskap, 30a §, förtydligas informationssäkerhetsansvaret för myndigheter ytterligare:

"Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt."

Fokus behöver framöver ligga på att förstärka förmågan att nyttja samhället samlade resurser inom ramen för ansvarsprincipen. På så sätt ökar förmågan att förebygga och hantera IT-incidenter under alltifrån normaltillstånd till kris. För att detta ska bli framgångsrikt fordras att gemensamma förutsättningar, ledning, samordning och ansvar vid en allvarlig IT-incident tydliggörs. De erfarenheter som görs bör fortlöpande sammanställas och användas för att stärka den samlade förmågan inför kommande incidenter.

Idag finns det djup sektorsvis kompetens både på teknisk nivå och verksamhetsnivå inom olika samhällsviktiga sektorsområden, till exempel inom hälso- och sjukvård-, energi-, transport- och finanssektorn. Förståelse för hur olika styrsystem påverkas av störningar och incidenter inom sektorerna, och vilka följder det får för verksamheterna och i förlängningen för samhället, är oumbärlig och värdefull information som måste samlas och tas tillvara på ett ansvarsfullt sätt.

Många av de erfarenheter som över tid samlas i samhällets olika delar kan vara av betydelse vid analys och tolkning av IT-incidenter. Därför bör särskild vikt läggas vid att samla information som kan ha strategisk betydelse för framtida incidenthantering och som därmed stärker samhällets förebyggande informationssäkerhetsarbete.

5.2.2 Ett förberett nyttjande av relevanta resurser

På alla nivåer i samhället bör det finnas en förberedd möjlighet att utbyta relevant information vid allvarliga IT-incidenter. Det räcker inte att en central brandkårsstyrka av experter finns till förfogande och hålls informerad. Det behövs också en struktur som förfogar över eller känner till samverkansresurser, nätverk av informatörer, larmkanaler och kontakter med regionala eller sektoriella grupper, som har självständig förmåga att interagera och agera på de situationer som kan uppstå. Det handlar om att skapa en utbredd handlingsförmåga, och det behöver därför redan i normaltillståndet etableras kontaktvägar och rutiner som är välkända, övade och enkla att hantera för alla parter.

I andra länder, till exempel i Storbritannien, har det visat sig att en motsvarande organisationsmodell för informationsdelning – med centrala resurser i kombination med stark regional och sektoriell aktivitet – har stora förutsättningar att lyckas. En sådan struktur kan nyttjas även vid akutsituationer.

I detta förmågeskapande arbete över tiden är det väsentligt att ta vara på alla de resurser som redan finns i samhället. Länsstyrelserna, med det geografiska sektorsansvaret, har en nyckelroll i kontakten med framför allt Sveriges kommuner. Sektorsansvariga myndigheter har motsvarande nyckelroll i kontakten med aktörer inom respektive område. En samhällsgemensam struktur för IT-incidenthantering bör ha ett nära samarbete med dessa aktörer.

Även privata aktörer har en central roll i arbetet med att förebygga och hantera IT-incidenter. Det är därför väsentligt att de ansvariga för IT-incidenthantering på nationell nivå tar initiativ till en utvecklad privat-offentlig samverkan. Denna verksamhet bör samordnas med redan existerande privat-offentliga samverkansformer.

Arbetet med att larma vid och hantera IT-incidenter är ofta tidskritiskt. Därför måste konkret incidentsamverkan mellan berörda aktörer ha en mer operativ karaktär än den samverkan som normalt sker i det förebyggande informationssäkerhetsarbetet. Detta kan till viss del lösas genom att information kanaliseras via det system med Tjänsteman i beredskap (TiB) som idag finns vid ett flertal myndigheter. Det är dock tveksamt om detta i sig är tillräckligt. Vid större incidenter kan denna samverkanskanal visserligen få stor betydelse, men en incidentsamverkan innebär även ett mer vardagsbetonat informationsutbyte av teknisk karaktär, kontakt med en bredare krets aktörer än enbart statliga myndigheter och samverkan hamnar inte sällan i gränslandet mellan incidenthantering och löpande förebyggande informationssäkerhetsarbete. Det behövs därför en kombination av dels snabba larmkanaler och utbyggda kontaktnät som i ett akutläge når ett stort antal aktörer, dels mer specifika kontaktvägar till personal hos respektive aktör som snabbt kan agera konkret på information; till exempel vidta åtgärder av teknisk natur eller snabbt sprida information internt inom sin organisation. Den riktigt stora utmaningen är sannolikt att skapa och upprätthålla sådana kontaktnät som sträcker sig till samhällets alla delar.

För att etablera det förtroende som krävs för samverkan vid oväntade händelser krävs en nära samverkan även i vardagen. Vardaglig samverkan kan ske genom ett systematiskt, förebyggande arbete som bygger på redan existerande samarbetsformer för informationsdelning, myndighetssamverkan samt regional och lokal samverkan. Detta arbete tjänar därmed ett dubbelt syfte. Dels stärker det samhällets alla delar, dels lägger det grunden till en snabb och samordnad respons i kristider.

5.2.3 Behov av säker och redundant kommunikation

I det svenska samhället behövs det en administrativ och teknisk infrastruktur 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 som kan fungera som stöd under allvarliga störningar och kriser. En sådan stödorganisation och infrastruktur måste självfallet ha en hög informationssäkerhet, så att den inte slås ut vid allvarliga störningar. För att bli kostnadseffektiv och för att på bästa sätt ta vara på befintlig kompetens och organisation bör infrastrukturen bygga på nuvarande teknisk struktur. En övergång från normalläge till krisläge ska inte innebära stora förändringar vad gäller aktörer och arbetssätt, eftersom det försvårar och fördröjer arbetet i en redan pressad situation.

En säker digital informations- och kommunikationsinfrastruktur för offentlig sektor (GovNet)

Att myndigheterna och andra offentliga aktörer alltid kan kommunicera på ett säkert sätt är en viktig förutsättning för god nationell informationssäkerhet och möjligheten att hantera allvarliga IT-incidenter eller andra allvarliga störningar. Ett sätt att åstadkomma detta är att bygga en gemensam nätstruktur för myndigheter och andra offentliga aktörer, ett GovNet, som säkerställer att det allmänna har en fungerande grundnivå även vid svåra IT-störningar. En sådan nätstruktur säkerställer också det offentliga samhällets incidenthanteringsarbete i och med att den fungerar som en säker kanal för larm, varningar och annan samverkan.

För att etablera ett GovNet bör nuvarande tekniska strukturer användas för att skapa så hög tillgänglighet och säkerhet som möjligt i informationsutbytet. Ett nationellt GovNet 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.

Det finns idag ingen klar och ensad bild av hur den tekniska plattformen, det administrativa regelverket, rutinerna och avtalen för ett GovNet ska vara formulerade. MSB anser att regeringen bör ge en myndighet i uppdrag att, tillsammans med andra berörda aktörer, närmare utreda hur ett nationellt GovNet ska utformas för att säkerställa förmågan till säkert informationsutbyte mellan myndigheter med höga krav på tillgänglighet. Uppdraget bör genomföras under 2010. Ett GovNet bör sedan skapas och etableras under 2011–2012.

Säker kommunikation med samhällets övriga aktörer (kryptografiska funktioner)

För att skapa förtroende för en nationell funktion som ska förebygga och hantera IT-incidenter krävs att den information som hanteras av och förmedlas mellan aktörer kan ges ett skydd mot obehörig insyn och påverkan. Detta gäller dels för de offentliga aktörer som är anslutna till GovNet, dels för samhällets

övriga aktörer som har behov av att utbyta information. Den information som ska utbytas och förmedlas är sannolikt känslig och skyddsvärd med höga krav på riktighet. Den omfattas i många fall av sekretess. Informationen kan behöva förmedlas som samtal över publika fasta och mobila telekommunikationsnät, och elektroniskt över datakommunikationsnät. För detta informationsutbyte bör det finnas kryptosystem som är nationellt godkända för skydd av information som klassats som skyddsvärd, KSU (Krypto för skyddsvärda uppgifter).

Mellan vissa organisationer kan sannolikt informationen som omfattas av sekretess enligt Offentlighets- och sekretesslag (2009:400) och röra rikets säkerhet behöva förmedlas.

I syfte att kunna stödja de aktörer som har behov av skyddad informations-överföring för IT-incidenthantering har MSB för avsikt att i samråd med FM och FRA närmare analysera hur befintliga eller kommande kryptosystem kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.

5.3 Informationsdelning

Principer: Inhämtning och delgivning av information är en central förutsättning för att förebygga och hantera IT-incidenter. Det ställer stora krav på att tillgänglig information inhämtas och delges i rätt tid, till rätt aktörer och på ett säkert sätt. Informationen finns hos både privata och offentliga aktörer, nationella och internationella.

Utgångspunkten för en ändamålsenlig informationsdelning är att det finns ett ömsesidigt förtroende mellan de berörda aktörerna. Det måste också finnas en gemensam nytta och incitamentsstruktur, som uppmuntrar och skapar förutsättningar för samverkan. Detta kräver ett långsiktigt och målmedvetet arbete.

Åtgärder: För att informationsdelning ska ske på ett ändamålsenligt sätt krävs att alla sektorer och nivåer i samhället, utifrån sin verksamhet och sitt ansvar, skapar strukturer för informationsdelning. Arbetet börjar i vardagen men måste också ta höjd för allvarliga händelser. För att underlätta informationsdelning avser MSB att verka för att det skapas en tydlig nationell struktur för privat-offentlig samverkan inom informationssäkerhetsområdet.

MSB avser att utreda hur ett system för obligatorisk IT-incidentrapportering skulle kunna införas för statliga myndigheter. Övriga aktörer i samhället bör erbjudas att på frivillig grund delta i ett sådant system.

Information som genereras utifrån underrättelse- och säkerhetstjänsternas olika myndighetsuppdrag kan vara mycket värdefull både i det förebyggande informationssäkerhetsarbetet och i hanteringen av allvarliga IT-incidenter. Formerna för delning av underrättelser och annan information bör närmare utredas inom ramen för SAMFI.

5.3.1 Behov av informationsdelning

Att förebygga och hantera IT-incidenter förutsätter ett väl etablerat samarbete mellan berörda organisationer och funktioner. Att parter kan dela information med förtroende är nödvändigt för att kunna skapa och förmedla en aktuell och relevant lägesbild.

Det finns redan idag en rad forum för samverkan inom informationssäkerhetsområdet (se vidare avsnitt 5.5.3). Ett problem är dock att dessa forum inte i når ut och får ta del av relevant information från hela samhället i tillräcklig omfattning. Kommuner, länsstyrelser, landsting och näringsliv behöver därför representeras i högre grad i dessa sammanhang. För att skapa en kontinuitet i samverkan är det dock viktigt att ta hänsyn till existerande

samverkansgruppers verksamhet. En viktig framgångsfaktor är att det inte förekommer parallella, eller överlappande, informationsdelningsgrupper.[33]

5.3.2 Strukturer för informationsdelning

För att öka säkerheten och krishanteringsförmågan i samhället krävs det etablerade rutiner och samarbeten för att dela information, också sekretessbelagd sådan. Erfarenheter från den privat-offentliga samverkan som genomförs av MSB (tidigare KBM) inom informationssäkerhetsområdet visar att det behövs en mer formaliserad nationell struktur för samverkan; dels mellan aktörerna i den offentliga sfären, dels mellan det privata och det offentliga.

MSB avser verka för att det etableras en tydlig nationell struktur för privat-offentlig samverkan inom informationssäkerhetsområdet, där att alla deltagande grupper använder ett strukturerat arbetssätt. I första hand avser dock MSB verka för att det byggs upp en nationell struktur för samverkan mellan större samhällsviktiga aktörer inom privat sektor och berörda myndigheter. Här föreslås att SAMFI ska utgöra den kärna som den nationella informationsdelningen inom informationssäkerhetsområdet byggs upp runt. SAMFI är ett naturligt val. Alla myndigheter med ett nationellt informationssäkerhetsansvar är representerade i gruppen och det finns redan idag ett väl upparbetat samarbete mellan dessa myndigheter. Till detta kommer de redan befintliga privat-offentliga arbetsgrupperna som redan finns vid myndigheter som ingår i SAMFI.

Den nationella struktur som MSB föreslår ovan bör kompletteras med strukturer för samverkan på regional och lokal nivå, som får vara något friare och växa efter behov. Det är viktigt att tillåta både områdesspecifika och tvärsektoriella samverkansgrupper. Det är också viktigt att de centrala myndigheterna, och då kanske framförallt MSB med sitt tvärsektoriella ansvar, stöttar dessa grupper när de ska bygga upp strukturen.

5.3.3 Modell för informationsdelning

Informationsdelningen inom informationssäkerhetsområdet bör bygga på den brittiska informationsdelningsmodellen, *Information Exchange (IE)*. Modellen är baserad på riktlinjer som National Infrastructure Security Co-ordination Centre (NISCC), nuvarande Centre for Protection of National Infrastructure (CPNI), har tagit fram. I dag är CPNI navet i det brittiska informationsdelningssystemet, och ett flertal länder tillämpar framgångsrikt IE-modellen i någon form, exempelvis Nederländerna, Schweiz och till viss del även Sverige (se nedan). Genom att välja en etablerad nationell samverkansmodell, som

[33] En nationell privat-offentlig samverkansstruktur diskuteras i rapporten *Ökad samverkan inom informationssäkerhetsområdet – Förslag till ett nationellt privat-offentligt samverkanssystem* (Arbetsmaterial MSB). (En preliminär version gavs ut av KBM i slutet av 2008: ”Ökad samverkan inom informationssäkerhetsområdet – Utveckling av FIDI-konceptet för informationsdelning”, dnr. 1394/2008).

denna, skapas också förutsättningar för ett fruktbart internationellt samarbete. KBM anpassade modellen till svenska förhållanden och MSB tillämpar idag modellen under namnet *FIDI*. PTS samverkansgrupp NTSG, fungerar också ungefär enligt de principer som ligger till grund för IE-modellen. Även Säpo har ett antal värdefulla samverkansgrupper som använder sig av IE-modellen.

IE-modellen syftar till att skapa en mekanism som gör att en enskild organisation kan dra lärdom av andras erfarenheter, misstag och framgångar. Därmed ska varje deltagare kunna förbättra sin säkerhetsnivå. Detta ska ske utan rädsla för att behöva exponera den egna organisationens svagheter för exempelvis konkurrenter eller andra aktörer. Erfarenheter från Sverige och andra länder visar att samverkansgrupperna måste ha ett konkret praktiskt innehåll och en tydlig verksamhetsidé. För att skapa ett riktigt partnerskap måste grupperna få gemensamma projekt till stånd, exempelvis kring övnings- och utbildningsverksamhet.

Att kunna erbjuda verktyg för informationsdelning är en grundläggande förutsättning för att kunna skapa en effektiv samverkansgrupp. Detta är speciellt viktigt om en struktur för informationsdelning på regional och lokal nivå ska kunna växa fram.

Framöver planerar MSB att tillhandahålla metodstöd och tekniska lösningar som underlättar samverkan och informationsdelning. MSB kommer att utreda vilka metoder och system som kan användas inom ramen för SAMFI.

5.3.4 Delning av information från underrättelse- och säkerhetstjänsterna

Information som genereras utifrån underrättelse- och säkerhetstjänsternas olika myndighetsuppdrag kan vara mycket värdefull både i det förebyggande informationssäkerhetsarbetet och i hanteringen av allvarliga IT-incidenter.

Inom ramen för de enskilda underrättelse- och säkerhetstjänstmyndigheternas mandat finns redan i lag olika reglerade möjligheter att dela underrättelse-information och annan information till specificerade aktörer.

Regeringen anger följande i sitt uppdrag (detta uppdrag) till MSB:

> *”Det behöver formaliseras hur information om hot, sårbarheter och incidenter rapporteras, hanteras, förs vidare och hur information kan leda till förbättringsåtgärder. Den nuvarande underrättelse- och säkerhetstjänsterna bör därför kompletteras med en utökad informationsdelning samt en bättre förmåga att genom bl.a. samverkan agera mot hot och inträffade incidenter på nationell nivå. Detta innebär att arbetet inte kan avgränsas till staten utan även måste inbegripa näringsliv och andra organisationer.”*

Ett led i etablerandet av en mer formell struktur för samverkan inom informationssäkerhetsområdet bör därför vara att skapa processer och rutiner för hur underrättelseinformation, eller annan information från underrättelse- och säkerhetstjänsterna, på ett säkert sätt kan komma berörda aktörer vid en IT-

incident till nytta. Detta dock utan att vare sig kränka den personliga integriteten eller kompromettera underrättelse- och säkerhetstjänsternas metoder.

Underrättelse- och säkerhetstjänsterna bör ges bättre förutsättningar för en utökad informationsdelning. I detta inbegrips förbättrade möjligheter att genom framförallt samverkan bistå i det förebyggande arbetet och vid inträffade allvarliga IT-incidenter aktivt kunna bistå framförallt samhällsviktig verksamhet och kritisk infrastruktur med teknisk kompetens och information. Detta måste dock ske på ett sådant sätt att den personliga integriteten inte kränks och att tjänsternas metoder inte röjs.

Formerna för delning av underrättelser och annan information bör närmare utredas inom ramen för SAMFI.

5.3.5 Ett system för IT-incidentrapportering

Den rapportering av IT-incidenter som idag sker på frivillig basis är otillräcklig för att kunna bidra till en löpande aktuell lägesbild av tillståndet vid kritisk infrastruktur och vid samhällsviktig verksamhet.

MSB avser att utreda hur ett system för obligatorisk IT-incidentrapportering skulle kunna införas för statliga myndigheter. Övriga aktörer i samhället bör erbjudas att på frivillig grund delta i ett sådant system. Utgångspunkten är att deltagande ska kunna ske på ett sådant sätt att alla aktörer känner sig trygga i att den information som delges inte kommer att röjas.

MSB:s utredning ska behandla vilka former av IT-incidenter som ska rapporteras samt andra väsentliga ingångsvärden. Under utredningsarbetet kommer samverkan att ske med berörda aktörer.

En central utgångspunkt är att 18 kap 8 §, Offentlighets- och sekretesslag (2009:400), ger utrymme att sekretessbelägga incidentrapporter.

5.4 Gemensam lägesbild

Principer: Information om det aktuella läget är en nödvändig förutsättning för att de inblandade aktörerna ska få en ömsesidig förståelse för situationen och kunna bedriva samordnade åtgärder.

Det finns stark koppling mellan en gemensam informationssäkerhets-relaterad lägesbild och den övergripande nationella lägesbild som MSB upprätthåller och rapporterar till regeringen.

Utgångspunkten för en gemensam informationssäkerhetsrelaterad lägesbild är att det finns en normalbild. Normalbilden bygger på en systematiskt strukturerad identifiering av tillståndet inom olika sektorer över tid och i varje givet läge.

En avgörande faktor i skapandet av en gemensam lägesbild är kontakter med nyckelaktörer inom såväl som utanför landet.

En central förutsättning för lägesbilden är en substantiell rapportering av IT-incidenter, vilket bör ske enligt fastställda kriterier och rutiner, så att en helhetsbild kan upprätthållas.

Åtgärder: I syfte att på ett systematiskt sätt identifiera tillståndet inom offentlig sektor har MSB för avsikt att, inom ramen för sitt uppdrag att reglera myndigheternas arbete med risk- och sårbarhetsanalyser (RSA), se till att relevanta informationssäkerhetsparametrar redovisas i analyserna.

Utöver detta behövs ett antal metoder och instrument för att löpande identifiera allmäntillståndet i den digitala informations- och kommunikations-infrastrukturen. MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, utreda om ett mer strukturerat tekniskt intrångsdetekterings- och varningssystem för kritisk infrastruktur och samhällsviktig verksamhet kan införas i Sverige.

5.4.1 Behov av en gemensam lägesbild

En krissituation kännetecknas av såväl många informationskällor som många informationsmottagare. Lägesinformation utgör en nödvändig förutsättning för att alla inblandade aktörer ska förstå situationen och kunna hantera den. Ska aktörerna samordnat kunna planera åtgärder och fördela resurser måste lägesinformationen dessutom sammanfattas till en gemensam lägesbild. Samordnat handlande kräver alltså en gemensam uppfattning om det aktuella läget, det vill säga en lägesbild, som gör att aktörerna tillsammans kan gå vidare mot ett koordinerat beslutsfattande. Beslutsfattandet kan till exempel gälla hur aktörerna ska lämna samlad information till allmänheten eller vilken handlingslinje de ska välja.

En gemensam lägesbild är således en övergripande bild av situationen. För att kunna upprätthålla en sådan kontinuerligt uppdaterad lägesbild av god

kvalitet, och att vid behov kunna erbjuda en fördjupad analys, krävs en aktiv, behovsanpassad och systematisk omvärldsbevakning. Det ställer också krav på metoder och strukturer för informationshantering och informationsdelning.[34]

5.4.2 Normalbild

För en lägesbild är inflödet av information avgörande. Utan ett kontinuerligt inflöde är det svårt att få ett normalläge att utgå ifrån.

För att få en gemensam lägesbild, och därigenom kunna agera vid allvarliga IT-incidenter, krävs mycket god kunskap över tid om hur normalbilden för varje sektor ser ut. En normalbild kan skapas genom att man bygger upp kompetens om de olika verksamheterna. Det är nödvändigt att veta vilken verksamhet som bedrivs inom olika samhällssektorer, vilka krav som finns vid olika tidpunkter, vad som är på gång inom olika verksamheter etc. Utifrån normalbilden sker sedan en rapportering enligt principen om avvikelserapportering (incident-rapportering). Rapporterna vilar med andra ord på avvikelser från det normala. Det är därför av avgörande betydelse att det finns möjligheter till samverkan med samtliga inblandade aktörer, så att rätt information och kunskap från alla berörda kan förmedlas. Ett nyckelord för att skapa och upprätthålla normal-bilden är alltså samverkan i alla nödvändiga former. En annan förutsättning är att information kan delges på ett säkert sätt, som tidigare nämnts (se avsnitt 5.2.3).

För den statliga sektorn kan normalbilden kompletteras i och med incident-rapportering (se avsnitt 5.3.5).

MSB har för avsikt att, inom ramen för sitt arbete med att reglera myndig-heternas arbete med risk- och sårbarhetsanalyser (RSA), se till att relevanta informationssäkerhetsparametrar redovisas i analyserna. Denna åter-rapportering blir central i byggandet av normalbild inom den offentliga sektorn.

Det är viktigt att processerna för rapportering inom den offentliga sektorn byggs upp så att de även medger frivilligt deltagande för andra relevanta aktörer i samhället. Det är naturligt att en frivillig rapportering av incidenter ökar i takt med att allt fler aktörer inser nyttan av att delta i systemet.

Information om normalbilden kan också skapas genom olika former av tekniska stödsystem. Ett sätt är till exempel att regelbundet kontrollera myndigheters och kommuners öppna tjänster på internet och mäta tillgänglighet och svarstid. Upptäcks någon avvikelse kan den fångas upp genom ett larm eller läggas in i standardiserade rapporter.

[34] En gemensam lägesbild diskuteras vidare i *Studie av gemensam lägesinformation* (daterad 2009-01-31). Kommande rapport, MSB

Det bör också utredas om ett mer strukturerat tekniskt intrångsdetekterings- och varningssystem för kritisk infrastruktur och samhällsviktig verksamhet kan införas i Sverige. I Norge finns sedan ett antal år ett system som heter *Varslingssystem for Digital Infrastruktur* (VDI)[35]. Det består av ett antal sensorer för intrångsdetektering på internet som detekterar om kritisk infrastruktur i Norge utsätts för oönskade aktiviteter. Informationen rapporteras till NorCERT, den norska nationella CERT-funktionen.

MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, utreda om ett liknande system kan införas i Sverige.

5.4.3 Gemensam lägesbild och lägesrapportering av IT-incidenter

En gemensam informationssäkerhetsrelaterad lägesbild är avgörande för att det nationella arbetet med att hantera allvarliga IT-incidenter ska kunna samordnas. Lägesbilden är därmed en viktig komponent i krishanteringssystemet.

Det finns en stark koppling mellan en gemensam informationssäkerhetsrelaterad lägesbild och den övergripande nationella lägesbild som MSB upprätthåller och rapporterar till regeringen. En gemensam informationssäkerhetsrelaterad lägesbild bygger på ett kontinuerligt informationsflöde från olika samhällsviktiga verksamheter. Det kan handla om verksamheter som är direkt involverade, exempelvis nätoperatörer, tjänsteleverantörer eller kontroll- och samordnande funktioner. Det kan också handla om verksamheter som står i beroendeförhållande till de direkt involverade, exempelvis operatörer av annan kritisk infrastruktur, som elkraft.

Inom IT-incidentområdet råder speciella förhållanden. Dels är tidsförloppen mycket snabba, dels berör incidenter alla viktiga sektorer och samhällsviktiga system eftersom IT-beroendet växer sig allt starkare.

De olika aktörerna har olika behov av information för att, utifrån roll och ansvar, kunna förebygga och hantera IT-incidenter. Varje aktör bibehåller sitt verksamhetsansvar, och därigenom även ansvaret för informationsinnehållet. Detta får emellertid inte leda till att åtgärder för att hindra, eller mildra, konsekvenserna av en IT-incident fördröjs. För att skapa en gemensam lägesbild behövs en särskild funktion som fogar samman informationen från de olika system och mekanismer som behövs för att upptäcka och identifiera hot och risker.

En gemensam lägesbildsfunktion ska kunna ge aktörer på nationell, regional och lokal nivå en samlad nationell lägesbild och en tvärsektoriell analys. En tvärsektoriell analys innefattar en slutsats av en sammanställning av hur ett

[35] Se vidare https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/

krisförlopp sträcker sig över flera sektorer i samhället. På så sätt identifieras ömsesidiga eller kritiska beroenden, orsakskedjor eller sekundära effekter av kriser som får omfattande konsekvenser i samhället.

5.5 Responsförmåga

Principer: En central utgångspunkt är att IT-incidenter bör hanteras så nära den drabbade verksamheten som möjligt. På grund av samhällets ökade IT-beroende och det faktum att IT-incidenter mycket snabbt kan eskalera från lokal till internationell nivå, krävs dock förmåga att skapa en gemensam lägesbild. Detta möjliggör ett samfällt nationellt agerande.

Åtgärder: Det behövs en förbättrad nationell responsförmåga. Åtgärder bör därför genomföras för att förtydliga och förstärka den samhälleliga förmågan att hantera allvarliga IT-incidenter som kan hota Sverige och svenska intressen.

Sverige behöver ett ramverk som tillförsäkrar en koordinerad nationell hantering av IT-incidenter. MSB avser därför att, i samråd med de myndigheter som ingår i SAMFI, ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras.

Det finns ett underskott i samhället på teknisk kompetens inom olika samhällsviktiga och kritiska infrastrukturer. Detta underskott kan medföra allvarliga svårigheter i samband med kriser i samhället. MSB avser att, i samverkan med de myndigheter som ingår i SAMFI, skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter.

MSB avser vidare att fortsätta arbetet med att:
- Skapa en förtroendefull samverkansstruktur med samhällets aktörer för att praktiskt hantera allvarliga IT-incidenter.
- Genomföra regelbundna övningar med olika aktörer för att utveckla och utvärdera strukturer för hantering av allvarliga IT-incidenter.

5.5.1 Behov av en förbättrad nationell förmåga att hantera IT-incidenter

Den första försvarslinjen mot IT-incidenter börjar hos varje användare. Det följer av ansvarsprincipen, men också av hur den digitala informations- och kommunikationsinfrastrukturen är uppbyggd och används.

Allvarliga IT-incidenter har i regel ett mycket snabbt händelseförlopp. Därför är det viktigt att snabbt kunna detektera och presentera ett sådant händelseförlopp. Åtgärder för att hantera IT-incidenter kan komma att sättas in mycket snabbt. Åtgärder startar på många olika ställen i samhället, hos vissa aktörer omedelbart, hos andra aktörer med stor fördröjning eller i värsta fall inte alls.

Det är viktigt att snabbt kunna klarlägga läget och att samordna de åtgärder som behöver vidtas för att akut hantera incidenten och sedan för att återställa drabbade verksamheter.

Beroende på incidentens karaktär blir många olika aktörer i många olika samhällssektorer inblandade. Både privata och offentliga aktörer involveras, dels som verksamhetsansvariga, dels för att hantera den aktuella incidenten. För att hantera en storskalig allvarlig IT-incident behöver berörda aktörers handlande koordineras. Det är angeläget att undvika onödig duplicering och att istället skapa synergier mellan myndigheters och andra aktörers åtgärder och insatser. Det behövs också samordnad information till allmänheten.

Allvarliga IT-incidenter har oftast en internationell dimension på grund av områdets gränslösa karaktär. I dag finns en mycket välutvecklad, och värdefull, praktisk samverkan inom de internationella CERT-nätverken. Ett problem är dock att de nationella policyfrågorna och samordningen med andra kris-hanteringsåtgärder inte hanteras inom dessa strukturer. Konsekvenserna för tredje part kan därför bli godtyckliga. Tekniska åtgärder måste sättas in i sitt juridiska och organisatoriska sammanhang. Vid en incident måste relevanta tekniska åtgärder vägas mot den verksamhet som drabbas.

Sammanfattningsvis behövs en förstärkt och förtydligad nationell förmåga att hantera nationella IT-incidenter.

5.5.2 Tekniska kompetensnätverk

Det finns ett underskott på teknisk kompetens inom olika samhällsviktiga och kritiska 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 hantera allvarliga IT-incidenter. Huvuddelen av den tekniska kompetensen finns också inom den privata sektorn.

Det behövs därför en koordinerad nationell inventering inom olika sektorer avseende vilka förmågor och brister som finns. Därefter behöver det skapas olika anpassade nationella resurser som kan stödja hanteringen vid större allvarligare IT-incidenter. Dessa resurser bör organiseras som tekniska kompetensnätverk på alla samhällsnivåer (sektoriellt, lokalt, regionalt och nationellt), utifrån de förutsättningar och behov som finns. Dessa nätverk kan omfatta personer både från det privata och det offentliga.

Praktiskt sett handlar det om personer som har kvalificerat IT-säkerhetsarbete som ordinarie uppgift eller nyckelpersoner med speciell kunskap om samhällsviktiga verksamheter och kritisk infrastruktur. Det kan exempelvis handla om:

- Tekniska experter vid myndigheterna med informationssäkerhets-uppgifter.[36]
- Personal hos operatörer som driver infrastruktur och samhällsviktig verksamhet.
- Konsulter och specialister hos de IT-leverantörer som på daglig basis hjälper företag och myndigheter med hantering av incidenter, säkerhetsgranskningar, utformning av säkerhetslösningar etc.

Utgångspunkten är att dessa tekniska kompetensnätverk ska finansieras av deltagarna själva. I huvudsak handlar det om egen arbetstid. MSB avser att ta fram modeller i form av allmänna råd för hur arbetet ska bedrivas. I vissa fall kan viss central finansiering komma att krävas. Det rör sig då om punktinsatser för att stödja eftersatta sektorer.

5.5.3 En samverkansstruktur för att praktiskt hantera nationella IT-incidenter

De olika samhällsverksamheternas ordinarie personal utgör basresursen för att praktiskt hantera allvarliga IT-incidenter i samhället under fredstid. Det rör sig här om exempelvis tekniker, driftpersonal, systemutvecklare och IT-säkerhetsexperter. Till detta kommer konsulter och leverantörer som medverkar i den dagliga verksamheten i olika omfattning. Denna basresurs riskerar att bli hårt belastad vid en allvarlig IT-incident.

Vidare kan IT-incidenter som drabbar ett flertal sektorer innebära att vissa samhällsviktiga verksamheter eller kritiska infrastrukturer i samhället får brist på kvalificerad kompetens.

Utöver den kompetensuppbyggnad som föreslagits ovan behövs det en bättre praktisk samverkan och samordning för att förstärka den nationella förmågan. Det behövs en nationell samverkansstruktur för att stödja hanteringen av storskaliga IT-incidenter.

En nationell samverkansstruktur för IT-incidenthantering bör bestå dels av de kompetensnätverk som föreslagits ovan, dels av ett operativt nationellt samverkanscenter. MSB:s förslag för ett nationellt operativt samverkanscenter för informationssäkerhet beskrivs närmare i avsnitt 5.6. En central uppgift för centret bör dock vara att stödja samordnandet och utvecklandet av de tekniska kompetensnätverken (se avsnitt 5.5.2). Detta arbete innefattar bland annat att:

- Identifiera vilken kompetens som är relevant för att i olika sammanhang hantera storskaliga IT-incidenter i samhället.
- Inventera befintlig kompetens för att hantera storskaliga IT-incidenter i samhället.

[36] Här kan särskilt nämnas SÄPO som har ett särskilt ansvar inom säkerhetsskyddsområdet. FRA har enligt Förordning (2007:937) med instruktion för Försvarets Radioanstalt uppgiften att ha en hög teknisk kompetens inom informationssäkerhetsområdet.

- Stödja utvecklandet och bevarandet av relevanta kompetensnätverk för att hantera storskaliga IT-incidenter i samhället.

Det är viktigt att betona att en nationell funktion inte tar över någon aktörs ansvar. Den praktiska hanteringen av IT-incidenter är främst kopplad till att en organisation driver en egen verksamhet (egna IT-system). Därför kommer de drabbade verksamheterna att hantera huvuddelen av IT-incidenterna själva.

De centrala myndigheterna med informationssäkerhetsuppgifter (SAMFI) har dock operativa uppgifter och stödjer därigenom myndigheter och verksamheter i olika omfattning. Arbetsuppgifterna kan exempelvis bestå i metodstöd i incidenthantering, felsökning, logganalys, analyser av skadlig kod, spårning, återställande av skadade system och säkerhetsåtgärder för att skydda mot upprepade attacker. Stöd till andra samhällsaktörer sker utifrån de centrala myndigheternas tillgängliga resurser och legala förutsättningar. Myndigheterna i SAMFI spelar en central roll vid allvarliga IT-incidenter och är en kvalificerad nationell resurs.

Kompetensnätverken som föreslagits ovan kan vara av olika typer. Den nationella samverkansstrukturen bör främst baseras på frivillig samverkan, men det kan också behövas mer formella avtalslösningar, särskilt när resurser från den privata sektorn ska länkas in i systemet.[37]

Samverkansstrukturen kan byggas av olika lager, och olika kompetensnätverk kan samverka kring frågor av olika känslighetsgrad. Kompetensnätverk kan i detta avseende ses som resurspooler. Den här typen av samverkan är betydelsefull om flera olika ansvarsnivåer eller samhällssektorer drabbas av liknande problem. Den ökar förutsättningarna för att experter kan användas där de bäst behövs vid en kris, och ger möjlighet att koordinera användningen av den nationella förmågan.

En viktig förutsättning för att en nationell samverkansstruktur ska fungera är aktörer som ansvarar för att kritisk infrastruktur och samhällsviktiga verksamheter analyserar sin beredskap mot allvarliga IT-incidenter. Dessa måste också analysera sitt behov av stöd från externa resurser och förbereda sig för att kunna ta emot hjälp i ett akut skede. Hjälpen kan bestå av stöd från både från privata och offentliga aktörer. Den kan omfatta såväl tekniska förberedelser för att ta emot praktisk hjälp som administrativa förberedelser i form av processer och rutiner.

5.5.4 Nationell plan för IT-incidenthantering

Erfarenheter av IT-incidenter visar att det är viktigt att ha en organisation som är förberedd, inte minst vad gäller ansvarsfördelning.

[37] KBM har tidigare låtit utreda frågan om beredskapsstrukturer. Resultatet redovisades i rapporten *Beredskap mot IT-relaterade nationella kriser* (KBM dnr. 1207-2005).

EU-kommissionen uppmanar därför EU:s medlemsstater att ta fram nationella beredskapsplaner och att anordna regelbundna övningar för insatser och återställning efter storskaliga IT-incidenter.[38]

Sverige behöver ett ramverk som garanterar en koordinerad nationell hantering av IT-incidenter. MSB avser därför att, i samråd med SAMFI, och i samverkan med sektorsansvariga myndigheter, ta fram en nationell plan som klargör hur allvarligare IT-incidenter ska hanteras. En sådan plan bör vara anpassad till olika typer av allvarliga IT-incidenter och sektorers olika förutsättningar. Den måste också ta hänsyn till myndigheternas ansvarsområden. Planen bör vidare klargöra ansvar och roller på nationell nivå samt ange processer och rutiner för den nationella hanteringen av IT-incidenter. Planen ska utgå från ansvarsprincipen och ta hänsyn till den viktiga roll som näringsliv och andra organisationer spelar.

5.5.5 Informationssäkerhetsövningar

För att hantera nationella IT-incidenter krävs flexibla och adaptiva förfaranden. Förfaranden bygger visserligen på ändamålsenliga och uppdaterade planer och metoder, men det måste fortfarande finnas utrymme för ett situationsanpassat agerande.

Regelbundna informationssäkerhetsövningar, inom och mellan olika sektorer och på olika ansvarsnivåer, är en förutsättning för att utveckla och utvärdera de strukturer som föreslagits för att hantera IT-incidenter.

Övningarna kan syfta till att utveckla privat-offentlig samverkan inom offentlig sektor, undersöka hur gemensamma nationella lägesbilder skapas och upprätthålls etcetera.

Övningarna kan också inriktas på processer, rutiner och relationer. Det kan till exempel gälla att undersöka rollfördelningen mellan expert- och samordningsmyndigheter och privata aktörer. Då ingår det att öva koordination, beslutsprocesser och policysamverkan mellan de berörda aktörerna. Övningarna kan slutligen vara inriktade på att identifiera sårbarheter i den digitala informations- och kommunikationsinfrastrukturen eller i användarnas system.

Framöver kommer MSB att regelbundet genomföra olika typer av IT-relaterade övningar med olika aktörer. Det kan då röra sig om alltifrån enklare skrivbordsövningar till nationella samverkansövningar.

[38] EU-kommissionens meddelande KOM(2009)149

5.6 Nationellt operativt samverkanscenter för informationssäkerhet

Principer: Ett väl fungerande nationellt operativt samverkanscenter bygger på den struktur som tidigare redovisats. Ju mer utvecklad denna struktur blir med tiden, desto bättre blir förutsättningarna för centret.

Åtgärder: MSB avser att inrätta ett nationellt operativt samverkanscenter för informationssäkerhet vid myndigheten. Samverkanscentrets uppgift ska vara att stödja samhällets förebyggande informationssäkerhetsarbete och att samordna hanteringen av allvarliga IT-incidenter. Centret ska ha tillgång till säkra och ändamålsenliga lokaler, adekvat IT-stöd samt säker och redundant kommunikation.

Mer detaljerade åtgärder och ingångsvärden:
- Samverkanscentret bör ligga nära både den lägesbildsfunktion som redan finns vid MSB och det förebyggande arbete som sker inom ramen för myndighetens uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. På så sätt blir centret *en integrerad del av kris-hanteringssystemet och det förebyggande informationssäkerhetsarbetet*. Detta ökar förutsättningarna för att regeringen och andra berörda aktörer ska kunna få samlad information.
- Samarbetet mellan de myndigheter som har operativa uppgifter inom informationssäkerhetsområdet utgör en grund för samverkanscentrets arbete. En särskild grupp för samordning av arbetet vid centret bör etableras. Denna grupp bör bestå av informationssäkerhetsansvariga chefer vid MSB, PTS, RKP/SÄPO, FM/MUST och FRA. Exakta formerna för hur detta ska ske bör närmare utredas.
- Huvuddelen av SAMFI-myndigheterna bör adjungera personal till centret efter samma principer som till Nationellt centrum för terrorhotbedömning (NCT).
- En liknande verksamhet som Sveriges IT-incidentcentrum (Sitic), och med liknande uppgifter, bör integreras i samverkanscentret.
- Operatörer av samhällsviktig verksamhet och kritisk infrastruktur bör tillfälligt kunna få plats vid centret, beroende på händelsens karaktär. En förtroendefull privat-offentlig samverkan med nytta för alla berörda aktörer är av avgörande betydelse för att hantera allvarliga IT-incidenter.
- Samverkanscentret bör ha tillgång till relevant information från den offentliga sfären. Härvidlag är framförallt den information som finns och som kan genereras utifrån MSB:s och PTS uppdrag, samt information från under-rättelse-och säkerhetstjänsterna väsentlig att integrera.
- Informationsdelning från centret bör ske till regeringen och alla berörda parter utifrån vad som är lämpligt och möjligt med hänsyn till olika författningar och överenskommelser.

5.6.1 Uppgift och hemvist för nationellt operativt samverkanscenter

Ett nationellt operativt samverkanscenter för informationssäkerhet bör inrättas vid MSB med uppgift att stödja samhällets ordinarie förebyggande informationssäkerhetsarbete och att bistå vid samordning och hanteringen av allvarliga IT-incidenter. En liknande verksamhet som Sitic, och med liknande uppgifter, bör integreras i samverkanscentret. Till centret bör även personal från de myndigheter som har operativa informationssäkerhetsuppgifter (SAMFI) adjungeras motsvarande en heltidstjänst från varje myndighet. Även olika former av expert- och samordningspersonal, både från det privata och från det offentliga, bör tillfällig kunna beredas plats vid centret.

En av samverkanscentrets centrala uppgifter bör vara att förmedla en gemensam lägesbild till regeringen och berörda vid allvarliga IT-incidenter. En viktig förutsättning för detta är att samverkanscentret är den utpekade aktör som tar emot och analyserar incidentrapporter från de statliga myndigheterna. Även andra aktörer bör uppmanas att rapportera incidenter till centret.

I syfte att kunna förebygga och hantera IT-incidenter som kan drabba Sverige och svenska intressen bör samverkanscentret även kunna stödja de aktörer som har till uppgift att göra strategiska bedömningar kring hot och risker inom informationssäkerhetsområdet. Samverkanscentret ska kunna producera analyser av händelser, trender och omvärldsutveckling med koppling till allvarliga IT-incidenter som berör eller kan komma att beröra Sverige och svenska intressen. Centret bör också fortlöpande kunna lämna råd och stöd i linje med de uppgifter som Sitic nu lämnar.

Samverkanscentret kommer starkt att öka förutsättningarna för en samlad nationell hantering av IT-incidenter som hotar Sverige och svenska intressen. Genom centret säkerställs att samhällets samlade resurser på bästa möjliga sätt nyttjas för hanteringen av allvarliga IT-incidenter samt att internationell hjälp vid behov kan tas emot säkert och effektivt.

5.6.2 Övergripande förutsättningar för nationellt operativt samverkanscenter

En nödvändig förutsättning för ett operativt nationellt samverkanscenter är att skapa och upprätthålla ett *förtroende* hos privata och offentliga aktörer i samhället för centret. Verksamheten vid centret måste bygga på kompetens, delaktighet och professionell integritet. För att kunna få tillgång till relevant information från alla samhällsaktörer måste centret vara en respekterad och efterfrågad aktör. Tillgång till kompetent personal och samhällets samlade resurser skapar förutsättningar för centret att vara den aktör som på ett balanserat och kvalificerat sätt informerar om IT-relaterade incidenter i samhället. En viktig fråga är därför att skapa en balans mellan sekretess och transparens så att värdefulla erfarenheter kan förmedlas utan att vare sig sekretess eller personlig integritet äventyras.

Det är viktigt att betona att *ansvarsprincipen* gäller och att det nationella samverkanscenter som här föreslås inte tar över någon aktörs eget ansvar. Den praktiska hanteringen av IT-incidenter kommer alltid att i mycket stor omfattning genomföras av de drabbade verksamheterna.

En bärande princip är att det nationella operativa samverkanscentret för informationssäkerhet bör vara *en naturlig del av krishanteringssystemet*. Samverkanscentret bör därför ligga nära den funktion för gemensam lägesbild som redan finns vid MSB. En sådan lösning kopplar tydligt samman ansvaret för krishanteringssystemet med samordningen av hantering av allvarliga IT-incidenter på nationell nivå, och möjliggör en samlad information och rapportering till regeringen och berörda aktörer. På så sätt förs förmågan att skydda kritisk infrastruktur och samhällsviktig verksamheten tydligare samman med skyddet av den digitala informations- och kommunikations-infrastrukturen. Det skapar en gemensam förmåga där hanteringen av IT-incidenter är en tydlig del av samhällets hantering av allvarliga olyckor och kriser (en ”all-hazards approach”).

Samverkanscentret bör ha en självklar och nära *koppling till det ordinarie förebyggande och inriktande informationssäkerhetsarbetet i samhället*. Avgörande framgångsfaktorer är en nära privat-offentlig samverkan och ett tvärsektoriellt arbete. En förmåga att skapa god samverkan mellan aktörer från vitt skilda verksamheter, är en förutsättning för att kunna hantera allvarliga IT-incidenter såväl lokalt, regionalt som nationellt. Det är också viktigt med ett nära samarbete i vardagen. Arbetet med att förebygga hot, risker och sårbarheter i samhället måste bygga på en helhetssyn, ett klargörande av ansvar, rutiner och tydliga prioriteringar. Det förebyggande och inriktande arbete som MSB utför i samverkan med olika sektorer vad avser samhällets säkerhet i allmänhet, och informationssäkerhet i synnerhet, bygger över tiden en förmåga att motstå hot, risker och sårbarheter. Det finns en växelverkan mellan att förebygga och hantera IT-incidenter, och det förebyggande arbetet är en förutsättning för att möjliggöra en proaktiv hantering av IT-incidenter. Vidare skapar MSB:s breda samverkans- och samordningsverksamhet goda villkor för samverkan även vid kriser. Kopplingen till policyutveckling, förmågeuppbyggnad och generell kunskap inom informationssäkerhetsområdet är också en förutsättning för att skapa den normalbild som är en viktig komponent i att upprätthålla en aktuell lägesbild.

Ett *nära samarbete med underrättelse- och säkerhetstjänsterna* är ytterligare en viktig förutsättning för en nationell operativ samverkansfunktion.

5.6.3 Ledning och samordning av verksamheten vid nationellt operativt samverkanscenter

Samarbetet mellan de myndigheter som har operativa uppgifter inom informationssäkerhetsområdet utgör en grund för samverkanscentrets arbete.

Som tidigare har redovisats har flera olika myndigheter ansvar för olika frågor inom informationssäkerhetsområdet. Arbetet inom centret syftar till att skapa

en gemensam nationell samverkansplattform för dessa myndigheter och andra aktörer vid allvarliga IT-incidenter.

En särskild grupp för samordning av arbetet vid centret bör etableras. Denna grupp bör bestå av informationssäkerhetsansvariga chefer vid MSB, PTS, RKP/SÄPO, FM/MUST och FRA. Arbetsformerna för samverkanscentret bör utredas närmare. Arbetet inom SAMFI och vid NCT bör dock kunna ge viktiga ingångsvärden.

Genom att säkerställa att huvuddelen av SAMFI-myndigheterna spelar en aktiv roll i det nationella operativa samverkanscentret skapas förutsättningar att få tillgång till kvalificerade tekniska och analytiska resurser, samt att relevant information finns tillgänglig vid en allvarlig IT-incident.

Centret ska vara lokaliserat i säkra och ändamålsenliga lokaler och ha ett adekvat IT-stöd med säkra och redundanta kommunikationer till berörda aktörer. Lokaler och teknik bör utformas i samverkan med myndigheterna i SAMFI. De myndigheter som ingår i SAMFI och som ingår i samverkanscentret ska ha tillgång till egna arbetsrum, teknisk utrustning och relevanta verksamhetssystem.

Vidare är det viktigt att tydliggöra den roll som experter kan ha i samordningsverksamheten. Detta gäller inte bara experter inom berörda myndigheter och organisationer, utan också experter och personal utanför myndighetssfären. Det måste också skapas rutiner och arrangemang som möjliggör resursförstärkning.

5.6.4 Verksamhet vid nationellt operativt samverkanscenter

Verksamheten vid samverkanscentret bör omfatta både arbete för att förebygga och hantera IT-incidenter.

Huvuddelen av det förebyggande arbetet som centret genomför bör vara att upprätthålla en liknande verksamhet som Sitic redan idag tillhandahåller[39]. Samverkanscentret bör kunna stödja det ordinarie arbetet i samhället för att förebygga IT-incidenter, exempelvis genom att:

- Löpande lämna råd och stöd i linje med de uppgifter som Sitic har i dag. En viktig del är att skapa olika former av samverkan med olika operativa funktioner i landet.
- Stödja olika kompetensnätverk genom exempelvis utbildning och övning.
- Vara Sveriges kontaktpunkt för liknande internationellt organisationer.

När det gäller arbetsuppgifter som är mer direkt kopplade till att hantera IT-incidenter bör centret exempelvis:

[39] Jämför även med Förordning (2007:951) med instruktion för Post- och telestyrelsen, 6 §.

- Uppdatera och analysera den nationella informationssäkerhetsrelaterade lägesbilden. Lägesbilden och en tvärsektoriell analys utgör basen för väl underbyggda beslut om nationell hantering av IT-incidenter.
- Varna och informera samhällsviktiga verksamheter, kritisk infrastruktur i samhället samt andra relevanta aktörer. Centret ska snabbt kunna upptäcka och verifiera allvarliga händelser. Vid behov ska det kunna larma aktörer på internationell, nationell, regional och lokal nivå.
- Samverka med berörda aktörer, inklusive andra nationella och internationella funktioner som hanterar IT-incidenter, för att förmedla kunskap och kontakter, samt för att skapa en god bild av vidtagna åtgärder och tillgängliga resurser som är av särskild betydelse för krishanterings-systemet.
- Rekommendera vissa typer av insatser och resurser, exempelvis nationella resurser som kan användas för att stödja centrala myndigheter eller andra aktörer.
- Beroende på en IT-incidents omfattning och karaktär kan centret komma att få en betydelsefull roll i samordningen av vissa mer operativa aktiviteter, exempelvis genom att stödja praktiska insatser inom olika sektorer, regioner eller på den nationella nivån.
- Rapportera till regeringen och till Kansliet för krishantering vid Statsrådsberedningen samt berörda aktörer.
- Informera media och allmänhet och därigenom möjliggöra ett samlat budskap från berörda myndighetsaktörer.

6. Finansiering

6.1 Inledning

I rapportens tidigare delar redogörs för förutsättningar och grunder för nationell operativ samverkan. Förslaget tydliggör behovet av ett stärkt förebyggande arbete inom informationssäkerhetsområdet och behovet av att etablera en sammanhållen struktur för att förebygga och hantera allvarliga IT-incidenter.

Rapportens förslag syftar till att på bästa möjliga sätt tillvarata de resurser som redan finns hos myndigheter och andra aktörer.

MSB föreslår i denna rapport att ett nationellt operativt samverkanscenter för informationssäkerhet etableras vid MSB. En bärande princip är att det nationella operativa samverkanscentret för informationssäkerhet bör vara en central del av krishanteringssystemet. Centret bör verka i nära anslutning till både den lägesbildsfunktion som redan finns vid MSB och det förebyggande arbete som sker inom ramen för myndighetens uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. På så sätt blir centret en integrerad del av krishanteringssystemet och det förebyggande informationssäkerhetsarbetet. Detta ökar förutsättningarna för att regeringen och berörda aktörer ska kunna få samlad information.

Med hänsyn till den pågående utredningen om placering av Sitic (Dir. 2009:110)[40], gör MSB bedömningen att det, utifrån det uppdrag som här återrapporteras, är mest effektivt såväl ur ett ekonomiskt som ett krishanteringsperspektiv att placera Sitic vid MSB. Detta för att med effektivitet och kvalitet i fokus snabbt kunna åstadkomma den i budgetpropositionen för 2010 efterfrågade utveckling av det nationella informationssäkerhetsarbetet, som är nödvändig för att stärka samhällets samlade förmåga att förebygga och hantera IT-incidenter. Att placera verksamheten i MSB ligger i linje med det uppdrag som myndigheten har i sin instruktion, i synnerhet vad avser informationssäkerhet.

En placering av den funktion som Sitic representerar på MSB medger också i framtiden stora möjligheter till ökad effektivitet bland annat eftersom MSB och Sitic redan idag, såväl nationellt som internationellt, agerar samtidigt i många sammanhang.

Det finns ett stort värde i den etablerade struktur som Sitic representerar. Organisationen besitter en omfattande erfarenhet, har etablerade kontakter med internationella motparter och har omvärldens förtroende. Den kompetens

[40] Dir. 2009:110. *Viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet*

och kunskap som finns hos personalen om ett brett förebyggande arbete inom informationssäkerhetsområdet är en värdefull tillgång som skulle ge ytterligare bidrag till MSB:s förmåga att genomföra sitt uppdrag.

6.2 Föreslagen finansiering

Förslaget innebär inte att ny omfattande verksamhet etableras utan innebär att redan befintlig verksamhet effektiviseras genom att ett nationellt operativt samverkanscenter för informationssäkerhet etableras vid MSB och att Sitic införlivas i detta center.

Sitics verksamhet, i den omfattning som den beskrivs i denna rapport, beräknas kosta cirka 20 miljoner kronor per år.[41] Under förutsättning att en överföring av Sitics verksamhet till MSB åtföljs av en överföring av cirka 20 miljoner kronor innebär förslaget om inrättande av ett nationellt operativt samverkanscenter vid MSB inget behov att ytterligare verksamhetsfinansiering.

De engångskostnader som blir aktuella vid en etablering av det nationella operativa centret utgörs bland annat av omdisponering och komplettering av MSB:s lokaler i Stockholm samt vissa säkerhetshöjande åtgärder. MSB bedömer att dessa kostnader kan finansieras inom myndighetens ram. Eventuella framtida utvecklingsbehov kan givetvis uppstå. MSB återkommer i sådana fall i den ordinarie budgetprocessen.

Det förebyggande arbetet som beskrivs i rapporten ingår redan idag till övervägande del i befintliga uppgifter hos berörda aktörer. De flesta aktiviteter framgår av den nationella handlingsplanen för informationssäkerhet som tagits fram i samråd med SAMFI och som förvaltas av MSB.

Övriga verksamhetskostnader för IT-incidenthantering inom ramen för detta förslag, exempelvis kostnader för personal som adjungeras till centret, tillkommer. MSB bedömer emellertid att kostnader för berörda samverkansmyndigheter, som kan härröras till deras ansvar och uppgifter, även fortsättningsvis bör täckas av respektive myndighets budget. MSB vill dock betona SAMFI:s viktiga roll och det tydliga behovet av att personal från myndigheter med operativa uppgifter adjungeras till det föreslagna samverkanscentret.

Kostnader och förutsättningar för en säker digitalt nätverks- och kommunikationsinfrastruktur (GovNet) för offentlig sektor och ett detekterings- och varningssystem måste utredas vidare.

Sammantaget innebär förslaget om placering av Sitic hos MSB möjligheter till effektivitetsvinster som möjliggör finansiering av de i rapporten redogjorda

[41] I PTS årsredovisning för 2008 framgår att verksamhet avseende Sitic uppgick till 18,5 miljoner kronor.

behov av ambitions- och förmågehöjningar inom informationssäkerhets-området.

Konsekvensen av att Sitic inte placeras på MSB är ett behov av att utöka MSB:s ram med motsvarande den ram som gäller för Sitic idag. Denna ökade kostnad beror på att det operativa samordningscentret med stor sannolikhet måste ha CERT-liknande resurser för att kunna leverera en lägesbild till regeringen och andra aktörer samt bedriva effektiv samverkan i övrigt. Enligt MSB:s bedömning blir resultatet dessutom en dubblering av verksamhet, lång-sammare uppbyggnad av funktionalitet hos MSB samt reducerad förmåga inom området på grund av splittrade resurser och ansvarsförhållanden.

Bilaga 1: Uppdraget

REGERINGEN

Regeringsbeslut **9**

2009-10-29 Fö2009/2162/SSK

Försvarsdepartementet

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad

Uppdrag till Myndigheten för samhällsskydd och beredskap angående samhällets samlade förmåga att förebygga och hantera IT-incidenter

Regeringens beslut

Myndigheten för samhällsskydd och beredskap ska lämna förslag på åtgärder för att förebygga och hantera IT-incidenter mot exempelvis samhällsviktig verksamhet, kritisk infrastruktur samt övriga verksamheter och system inom ramen för det tvärsektoriella informationssäkerhetsarbetet från normaltillstånd till kris. Förslaget ska omfatta ledning och samordning, informationsdelning, gemensam lägesbild samt responsförmåga. I detta arbete ska befintliga resurser och funktioner beaktas.

Myndigheten för samhällsskydd och beredskap ska i arbetet inhämta berörda aktörers synpunkter. Kostnader för eventuella förslag ska redovisas samt hur dessa förslag ska finansieras inom befintliga budgetramar. Myndigheten för samhällskydd och beredskap ska vidare hålla Regeringskansliet (Försvarsdepartementet) fortlöpande informerat under uppdragets genomförande.

Uppdraget ska redovisas senast den 15 januari 2010 till Regeringskansliet (Försvarsdepartementet).

Ärendet

I budgetpropositionen för 2010 (prop 2009/10:1) har regeringen angivit att det finns anledning att se över informationssäkerhetsfrågorna. Det finns behov av att samla resurserna för att skapa goda förutsättningar för att förebygga IT-incidenter liksom för att hantera dem när de inträffar. Rapporteringen av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behöver förbättras och anpassas efter de behov som finns bland relevanta aktörer i samhället.

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

Erfarenheter från bl.a. attackerna mot Estland under våren 2007 visar att IT-baserade störningar och angrepp inte sällan sprider sig över organisationsgränser med hög hastighet. Att ha en förberedd organisation för detta, inte minst vad gäller ansvarsfördelning, är därför av största vikt. Det behöver formaliseras hur information om hot, sårbarheter och incidenter rapporteras, hanteras, förs vidare och hur informationen kan leda till förbättringsåtgärder. Den nuvarande underrättelse- och säkerhetstjänsten bör därför kompletteras med en utökad informationsdelning samt en bättre förmåga att genom bl. a samverkan agera mot hot och inträffade incidenter på nationell nivå. Detta innebär att arbetet inte kan avgränsas till staten utan även måste inbegripa näringsliv och andra organisationer.

Staten är beroende av en adekvat och aktuell lägesbild för att kunna hantera och förebygga kriser. Inom IT-incidentområdet är det speciella förhållanden som råder. Dels är tidsförloppen mycket snabba och dels är sannolikheten stor att samhällsviktig verksamhet inklusive samhällsviktiga system såsom finansiella system, ledningscentraler för trafiksystem, distributionsnät för el och vatten samt elektroniska kommunikationer m.m. berörs vid en IT-incident på grund av det ökande IT-beroendet.

Sverige behöver förbättra förmågan att hantera omfattande nätattacker där även attacker som genereras via öppna nät för elektroniska kommunikationer omfattas. Det behövs en övergripande lägesbild som baseras på incidentrapportering, trafikdata, underrättelser och information från krishanteringssystemets aktörer samt internationell samverkan. Det behövs också en förbättrad nationell förmåga till respons.

På regeringens vägnar

Sten Tolgfors

Linda Ericson

Bilaga 2: Samverkansgruppen för informationssäkerhet (SAMFI)

Samverkansgruppen för informationssäkerhet (SAMFI) består av sex myndigheter med särskilda uppgifter inom informationssäkerhetsområdet. SAMFI ska genom informationsutbyte och samverkan stödja de aktuella myndigheternas uppdrag inom området. Nedanstående myndigheter är medlemmar i SAMFI:

Försvarets materielverk (FMV) anskaffar, vidmakthåller och avvecklar materiel och förnödenheter på uppdrag av Försvarsmakten och andra myndigheter. FMV har genom CSEC uppgiften att utforma ett system för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med standarden ISO/IEC 15408, Common Criteria (CC).

Försvarets Radioanstalt (FRA) tillhandahåller tekniskt stöd med inriktning på informationssäkerhet till organisationer som hanterar information som bedöms känslig ur sårbarhetssynpunkt eller ur ett säkerhets- eller försvarspolitiskt avseende.

Försvarsmakten (FM) har föreskrifts- och tillsynsansvar för aktörer inom sitt ansvarsområde. Vidare ska Försvarsmakten särskilt leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information.

Myndigheten för samhällsskydd och beredskap (MSB) har i uppgift att stödja och samordna samhällets informationssäkerhet. Myndigheten har föreskriftsrätt när det gäller informationssäkerhetsarbetet hos statliga myndigheter.

Post- och telestyrelsen (PTS) med ansvar för infrastruktur inom telekommunikationsområdet inrymmer också **Sitic** som är Sveriges IT-incidentcentrum. Sitic är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder med uppgift att utveckla samarbetet och informationsutbytet med dessa.

Rikspolisstyrelsen (RPS) representeras genom **Rikskriminalpolisen (RKP)** och **Säkerhetspolisen (SÄPO)**. RKP bekämpar grov organiserad brottslighet, på nationell och internationell nivå. Målet är att motverka de kriminella organisationernas möjligheter att verka i Sverige. RKP utgör även svensk kontaktpunkt inom ramen för G8 24/7-arrangemang, Interpol och Europol när det gäller IT-relaterad brottslighet. SÄPO ansvarar för tillsyn och rådgivning inom informationssäkerhetsområdet för samhällsviktiga civila verksamheter. Tillsynen och rådgivningen avser skydd av rikets säkerhet och skydd mot terrorism. Rådgivningen ska också ges till myndigheter och företag som – utan att en fråga direkt avser rikets säkerhet – har ett ansvar för att minska samhällets sårbarhet i krissituationer.

Myndigheten för samhällsskydd och beredskap

Uppdragsredovisning

Datum	Diarienr
2010-01-13	2009-14471

Bilaga 3:
Förkortningar och vissa begrepp

Abusefunktion – funktioner hos operatörer som stöd till Internetanvändare dit dessa kan använda sig för rådgivning och stöd.

BITS – Basnivå för informationssäkerhet, utgiven av KBM.

CERT – Computer Emergency Response Team. Funktion för incident-hantering.

CIP – Critical Infrastructure Protection (skydd av kritisk infrastruktur).

CIIP – Critical Information Infrastructure Protection (skydd av kritisk informationsinfrastruktur).

CPNI – Centre for the Protection of National Infrastructure. Brittisk myndighet för säkerhet, inklusive informationssäkerhet.

CSEC – Sveriges Certifieringsorgan för IT-säkerhet. Är placerat 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 (CC).

Common Criteria (CC) – Standarden ISO/IEC 15408:2005 Evaluation criteria for IT security. Common Criteria är en standard för kravställning, deklaration och evaluering av säkerhet i IT-produkter och IT-system samt i deras användningsmiljöer.

DDoS – Distributed Denial of Service är en teknik som används för att attackera ett datorsystem eller nätverk, ofta genom att konsumera all tillgänglig bandbredd.

DNS – Domain Name Service. Funktion som översätter datorns namn till IP-adress (Internet Protocol).

EPCIP – European Programme for Critical Infrastructure Protection.

EU – Europeiska unionen.

EGC –European Governmental CERTs.

FIDI – Forum för informationsdelning avseende informationssäkerhet. En modell för samverkan inom informationssäkerhet mellan privata och offentliga aktörer.

FIDI-SC – Samverkansforum för aktörer beroende av industriella kontrollsystem (SCADA). Se även FIDI och SCADA.

FIRST – Forum of Incident Reports and Security Teams. Internationellt samverkansforum för CERT:s.

FOI – Totalförsvarets forskningsinstitut.

FM – Försvarsmakten.

FMV – Försvarets materielverk.

FRA – Försvarets radioanstalt.

GovNet – Governmental Network. En gemensam, skyddad informations- och kommunikationsinfrastruktur för myndighet eller för offentlig sektor.

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

ITU – International Telecommunication Union. ITU är FN:s ledande organ för informations- och kommunikationsteknologiska frågor.

IWWN – International Watch & Warning Network.

LIS – Ledningssystem för informationssäkerhet (se ISO/IEC 27001 och 27002).

KSU – Krypto för Skyddsvärda Uppgifter.

MSB – Myndigheten för samhällsskydd och beredskap.

MUST – Militära underrättelse- och säkerhetstjänsten.

NCT – Nationellt centrum för terrorhotbedömning.

NTSG – Nationella telesamverkansgruppen

PTS – Post- och telestyrelsen.

RKP – Rikskriminalpolisen.

RPS – Rikspolisstyrelsen.

RSA – Risk- och sårbarhetsanalys

SAMFI – Samverkansrådet för informationssäkerhet. SAMFI utgörs av representanter från FM, FMV, FRA, PTS, RPS och leds av MSB.

SCADA – Se industriella kontrollsystem.

SGSI – Swedish Government Security Intranet. Svenskt nationellt nät som används för kommunikation mellan svenska myndigheter och med EU-kommissionens nät TESTA.

Sitic – Sveriges incidentcentrum. Drivs av PTS.

SOF – Svensk Internet Operatörs Forum. SOF är ett samarbetsorgan för de svenska huvudoperatörerna på Internet i Sverige.

SVISA – Stöd för verksamheters informationssäkerhetsarbete, ett samverkansprojekt med syfte att ta fram stöd för förebyggande informationssäkerhetsarbete, initierat av MSB.

SÄPO – Säkerhetspolisen.

TESTA – Trans-European Service for Telematics between Administrations. EU-kommissionens nät för kommunikation med EU:s medlemsstater. Se även SGSI.

TiB – Tjänsteman i beredskap.

Myndigheten för samhällsskydd och beredskap

Uppdragsredovisning

Datum	Diarienr
2010-01-13	2009-14471

Bilaga 4:
Referenser och underlagsmaterial

Följande underlag utgör direkt eller indirekt viktiga utgångspunkter för denna rapport.

Lagar

Offentlighets- och sekretesslag (2009:400)

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

Lagen (2003:389) om elektronisk kommunikation (LEK)

Personuppgiftslagen (1998:204)

Säkerhetsskyddslagen (1996:627)

Förordningar

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

Förordning (2007:603) om intern styrning och kontroll (FISK)

Myndighetsförordningen (2007:515)

Förordningen (2006:942) om krisberedskap och höjd beredskap

Förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte

Förordningen (2000:555) med instruktion för Försvarsmakten

Förordningen (2002:1050) med instruktion för Säkerhetspolisen

Förordningen (1998:1192) med instruktion för Datainspektionen

Förordningen (1997:401) med instruktion för Post- och telestyrelsen

Säkerhetsskyddsförordningen (1996:633)

Förordningen (1996:103) med instruktion för Försvarets materielverk

Förordningen (1994:714) med instruktion för Försvarets radioanstalt

Föreskrifter och allmänna råd

DI: Allmänna råd – Säkerhet för personuppgifter, 1999.

FM: Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

MSB: Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, MSBFS2009:10 med tillhörande allmänna råd,

PTS: PTS allmänna råd om god funktion och teknisk säkerhet (PTSFS 2007:2).

RPS: Rikspolisstyrelsens föreskrifter (RPSFS 2004:11 FAP 244-1).

Propositioner, kommittédirektiv och SOU

Proposition 2009/10:1 *Budgetpropositionen för 2010*

Proposition 2008/09:140 *Ett användbart försvar*

Proposition 2007/08:92 *Stärkt beredskap – för säkerhets skull*

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

Proposition 2001/02:158 *Samhällets säkerhet och beredskap*

Kommittédirektiv Dir. 2009:110. *Viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet*

Kommittédirektiv Dir. 2008:27 *En ny myndighet med ansvar för frågor om samhällets krisberedskap och säkerhet*

Handlingsplan för eFörvaltning – Nya grunder för IT-baserad verksamhetsutveckling i offentlig förvaltning, Regeringskansliet, Fi2007/1981/SF

SOU 2007:31 *Alltid redo! En ny myndighet mot olyckor och kriser*

SOU 2005:71 *Informationssäkerhetspolitik – Organisatoriska konsekvenser* (Slutbetänkande från Infosäkutredningen)

SOU 2005:42 *Säker information – Förslag till informationssäkerhetspolitik* (Delrapport 3 från Infosäkutredningen)

SOU 2004:23 *Från verksförordning till myndighetsförordning*

SOU 2004:32 *Informationssäkerhet i Sverige och internationellt - en översikt* (Delrapport 2 från Infosäkutredningen)

SOU 2003:27 *Signalskydd* (Delrapport 1 från Infosäkutredningen)

SOU 2001:41 *Säkerhet i en ny tid* (Sårbarhets- och säkerhetsutredningen)

Dokument från myndigheter

KBM: *Samhällets informationssäkerhet - Handlingsplan 2008*

KBM: *Lägesbedömning av samhällets informationssäkerhet 2008*

KBM: Sveriges beredskap mot nätangrepp. KBM:s utbildningsserie 2008:1

KBM: *Handbok i privat-offentlig samverkan inom området krisberedskap*. KBM:s utbildningsserie 2008:5

KBM/.SE: *Nåbarhet på nätet – Hälsoläget i .SE 2007*

KBM: *Common Criteria (CC) – en introduktion*. KBM rekommenderar 2007:2

KBM: *Risk- och sårbarhetsanalyser – Vägledning för statliga myndigheter*. KBM rekommenderar 2006:4

KBM: *Vem gör vad inom EU? Informationssäkerhetsfrågorna i fokus*. KBM:s temaserie 2006:5

KBM: *Basnivå för informationssäkerhet (BITS)*. KBM rekommenderar 2006:1

KBM: Privat-offentlig samverkan – från idé till fungerande praktik. KBM:s temaserie 2006:2

KBM: *Mind the gap! Hur bygger vi broar mellan stat och näringsliv i arbetet med krisberedskap?* KBM:s temaserie 2005:8

KBM: *Beredskap mot IT-relaterade nationella kriser*. (Förstudie utförd av Ekelöw InfoSecurity AB), KBM dnr. 1207-2005, 2005

MSB: *Vägledning till ökad säkerhet i industriella kontrollsystem*. Myndigheten för samhällsskydd och beredskap (MSB), Stockholm, 2010

MSB: *Samhällets informationssäkerhet - Lägesbedömning 2009*

MSB: *Ökad samverkan inom informationssäkerhetsområdet – Förslag till ett nationellt privat-offentligt samverkanssystem*. Arbetsmaterial MSB, 2009

PTS: *Strategi för ett säkrare Internet i Sverige*. PTS-ER-2006:12

PTS: *Robusta elektroniska kommunikationer - Strategi för åren 2006-2008*. PTS-ER-2006:19 - 24 april 2006

Riksrevisionen: *Krisberedskap i betalningssystemet*. RiR 2007:28

Riksrevisionen: *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*. Riksrevisionen RiR 2007:10

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

Internationella dokument

Australien: *Cyber Security Strategy*. Australian Government, 2009

Estland: *Cyber Security Strategy*. Cyber Security Strategy Committee, Ministry of Defence, 2008

ENISA: *Baseline capabilities for national / governmental CERTs*. Version 1.0 (initial draft). European Network and information Security Agency (ENISA), 2009

ENISA: *A step-by-step approach on how to set up a CSIRT*. European Network and information Security Agency (ENISA), 2006

EU: *Skydd mot storskaliga it-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa*. Meddelande från kommissionen om skydd av kritisk informationsinfrastruktur (KOM/2009/149 slutlig), 2009

EU: *Meddelande från kommissionen om ett europeiskt program för skydd av kritisk infrastruktur* (KOM/2006/0786 slutlig), 2006

Finland: *Statsrådets principbeslut om en nationell informationssäkerhets-strategi "Trygg vardag i informationssamhället – Inte med tur utan med kunskap*". Kommunikationsministeriets publikationer 62/2008

Finland: *Valtionhallinnon 24/7-tietoturvavalvonnan hankeehdotus – VAHTI 5/2008* ("Förslag till planering och verkställandet av 24/7-funktion för övervakning av den statliga förvaltningens informationssäkerhet"). Finansministeriet.

FN: *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure*. Utkast till FN-resolution daterad 20 november 2009

Frankrike: *The French White Paper on defence and national security*. Présidence de la République, June 17th, 2008

G8: *G8 Principles for Protecting Critical Information Infrastructures*. Adopted by the G8 Justice & Interior Ministers, May 2003

ITU/FN: *Global Cybersecurity Agenda*. International Telecommunication Union (ITU), 2008

Japan: *The First National Strategy on Information Security – "Toward the realization of a trustworthy society"*. Information Security Council, 2 February 2006

Norge: *Nasjonal strategi for informasjonssikkerhet – Utfordringer, prioriteringer og tiltak*. Forsvarsdepartementet, Narings- og handelsdepartementet, Justis- og politidepartementet, 2003

OECD: *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures (CIIP)*. OECD Ministerial Meeting on the Future of the Internet Economy. Seoul, Korea, 17-18 June, 2008

OECD: *OECD:s riktlinjer för säkerheten i informationssystem och nät – På väg mot en säkerhetskultur*. 2004 (Utgiven på originalspråk 2002)

Storbritannien: *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*. Cabinet Office, June 2009

Storbritannien: *A National Information Assurance Strategy*. Cabinet Office, 2007

Tjeckien: *CR National Strategy for Information Security (CR NSIS)*. 2006

Tyskland: *IT Emergency and Crisis Exercises in Critical Infrastructures* (UP KRITIS, Working Group 1: "Emergency and Crisis Exercises"). Federal Ministry of the Interior (BMI), 2009

Tyskland: *Early detection and Mitigation of IT Crises* (UP KRITIS, Working Group 2: "Crisis Response and Mitigation"). Federal Ministry of the Interior (BMI), 2009

Tyskland: *CIP Implementation Plan of the National Plan for Information Infrastructure Protection (KRITIS)*. Federal Ministry of the Interior (BMI), 2007

Tyskland: *National Plan for Information Infrastructure Protection*. Federal Ministry of the Interior (BMI), 2005 .

USA: *Cyberspace Policy Review -Assuring a Trusted and Resilient Information and Communications Infrastructure*. ("The 60-Day Review"). The White House, 2009

USA: *CRS Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*. Congressional Research Service (CRS), 2009

USA: *Strategy for Securing Control Systems*. U.S. Department of Homeland Security (DHS), 2009

USA: *Securing Cyberspace for the 44th Presidency*. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Center for Strategic and International Studies (CSIS), 2008

USA: *National Infrastructure Protection Plan (NIPP)*.U.S. Department of Homeland Security (DHS), 2006

USA: *Computer Security Incident Handling Guide*. Recommendations of the National Institute of Standards and Technology (NIST), SP 800-61, 2004

USA: *The National Strategy to Secure Cyberspace*. The White House, 2003