Myndigheten för
samhällsskydd
och beredskap

Samhällets informationssäkerhet

Nationell handlingsplan 2012

Samhällets informationssäkerhet

Nationell handlingsplan 2012

Samhällets informationssäkerhet
Nationell handlingsplan 2012

Myndigheten för samhällsskydd och beredskap (MSB)

Layout: Advant Produktionsbyrå AB
Tryckeri: DanagårdLiTHO

Publ.nr: MSB423 - augusti 2012
ISBN: 978-91-7383-254-0

Förord

I dagens informationssamhälle bearbetar, lagrar, kommunicerar och mångfaldigar vi information i större mängder än någonsin tidigare. Informationshantering utförs manuellt och i allt högre grad med stöd av it – som till exempel det publika nätverket internet.

Informationssäkerhet handlar om att information ska skyddas utifrån krav på dess konfidentialitet, riktighet och tillgänglighet. Det gäller både hos enskilda personer och hos organisationer.

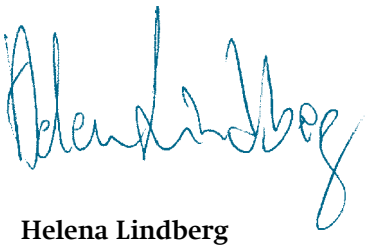
Informationssäkerhet är med andra ord en angelägenhet för alla.

Information och dess hantering ska hålla en hög kvalitet i Sverige. Samtliga aktörer i samhället ska ha relevanta kunskaper om informationssäkerhet och kunna känna tillit till information och dess hantering på alla nivåer i samhället.

Brister i informationshantering kan leda till att tilliten till aktuella tjänster och bakomliggande aktörer sjunker. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till flera aktörer och tjänster och även till andra sektorer i samhället.

För att lyckas med utmaningarna inom informationssäkerhet är det viktigt att det i samhället finns en gemensam uppfattning om informationssäkerhetsarbetet: en strategi.

Mot denna bakgrund har MSB, i samråd med Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen och Rikskriminalpolisen/Säkerhetspolisen tagit fram denna handlingsplan för samhällets informationssäkerhet.



Helena Lindberg
Generaldirektör

Innehåll

Inledning

Inledning

Myndigheten för samhällsskydd och beredskap (MSB) har tillsammans med övriga myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI)[1] tagit fram en strategi för samhällets informationssäkerhet 2010-2015.[2] För att förverkliga strategins intentioner behöver målen brytas ned till konkreta åtgärder. Den här handlingsplanen är ett verktyg för myndigheterna i SAMFI att ta fram prioriterade åtgärder, och ska också ses som en efterföljare till den handlingsplan som publicerades 2008 av Krisberedskapsmyndigheten (KBM) på uppdrag av regeringen.

Åtgärdsförslagen i handlingsplanen ligger inom ramen för de uppdrag som myndigheterna i SAMFI har, och de kan genomföras av en myndighet enskilt eller i gemensamma projekt. Planen ska dock inte ses som en komplett redovisning av alla de åtgärder som de olika myndigheterna kommer att genomföra inom sina respektive verksamheter.

Myndigheterna i SAMFI har särskilt angivna uppgifter avseende informationssäkerhet (bilaga 1). För att höja samhällets informationssäkerhet krävs dock engagemang och aktiviteter på alla nivåer i samhället. En grund för handlingsplanen är därför att ta fram sätt att arbeta där fler aktörer är med och påverkar både de åtgärder som ingår i nuvarande plan och innehållet i framtidens arbete med informationssäkerhet.

Målgruppen för handlingsplanen är alla aktörer i samhället som arbetar med informationssäkerhet i sin verksamhet. För aktörer inom exempelvis transportsektorn, energisektorn, finanssektorn, samt inom vård och omsorg är det ett stöd att känna till vilken inriktning det nationella arbetet har. Handlingsplanen ger här både en grund för en aktiv dialog om mål och metoder, och en möjlighet för enskilda organisationer att samordna sitt säkerhetsarbete med det nationella säkerhetsarbetet. Planen är treårig och framtagen av MSB i samråd med övriga myndigheter som ingår i SAMFI, det vill säga Försvarets materielverk (FMV)/Sveriges certifieringsorgan för it-säkerhet (CSEC), Försvarets radioanstalt (FRA), Försvarsmakten, Post- och telestyrelsen (PTS), samt Säkerhetspolisen/Rikskriminalpolisen.

1. Följande myndigheter ingår i SAMFI: Försvarets materielverk (FMV)/Sveriges certifieringsorgan för it-säkerhet (CSEC), Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS) samt Rikspolisstyrelsen (RPS) som representeras av Säkerhetspolisen (Säpo) och Rikskriminalpolisen (RKP).
2. *Strategi för samhällets informationssäkerhet 2010-2015,* MSB (https://www.msb.se/RibData/Filer/pdf/25482.pdf)

Framtagande av nationell handlingsplan

Koppling mellan strategi, lägesbedömning och handlingsplan

Den nationella strategin för informationssäkerhet är en viktig utgångspunkt för handlingsplanens utformning. Ytterligare ett viktigt ingångsvärde är det löpande arbetet med den nationella lägesbedömningen avseende samhällets informationssäkerhet. I detta avsnitt beskrivs hur handlingsplanen relaterar till strategin och arbetet med lägesbedömning.

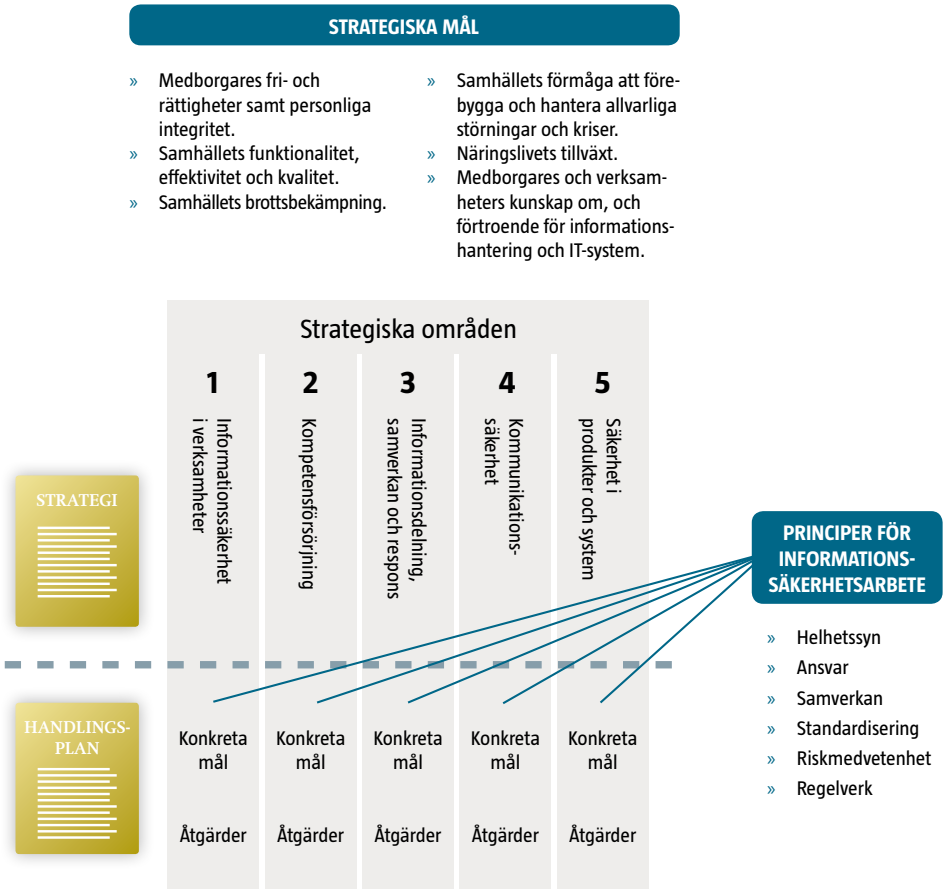
I Strategi för samhällets informationssäkerhet 2010-2015 anges att målet är att uppnå en god informationssäkerhet i samhället som främjar:

- Fri- och rättigheter samt personliga integritet.
- Samhällets funktionalitet, effektivitet och kvalitet.
- Samhällets brottsbekämpning.
- Samhällets förmåga att förebygga och hantera allvarliga störningar och kriser.
- Näringslivets tillväxt.
- Medborgares och verksamheters kunskap om, och förtroende för informationshantering och IT-system.

I strategin anges även fem strategiska områden:

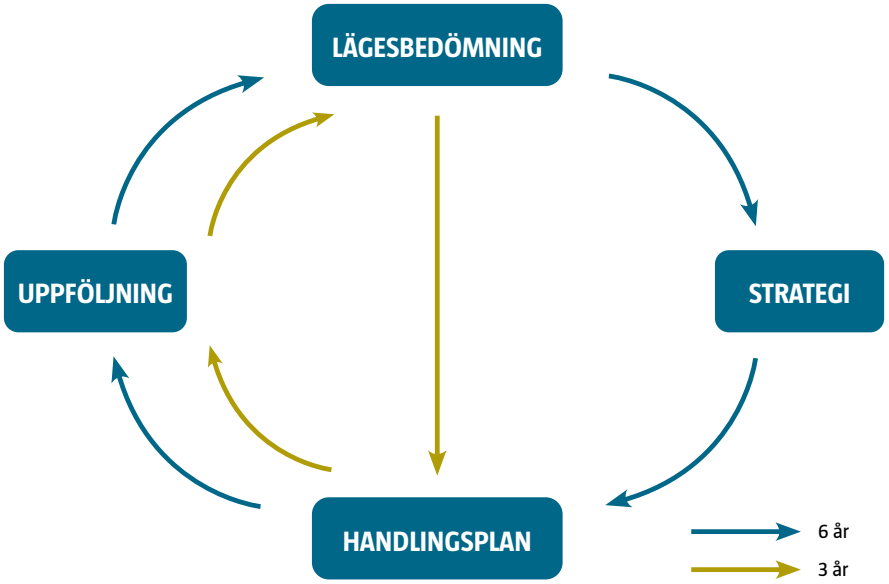
1. Informationssäkerhet i verksamheter
2. Kompetensförsörjning
3. Informationsdelning, samverkan och respons
4. Kommunikationssäkerhet
5. Säkerheter i produkter och system.

Handlingsplanen utgör ett viktigt instrument för att realisera strategin och tar därför sin utgångspunkt i de fem strategiska områdena. Samband mellan strategi och handlingsplan illustreras i figur 1.



Figur 1. *Samband mellan strategi och handlingsplan.*

Grunden för arbetet med samhällets informationssäkerhet är en god uppfattning om samhällets risker och sårbarheter. Handlingsplanens aktiviteter är baserade på MBS:s löpande lägesbedömningar, de samlade uppfattningarna hos myndigheterna i SAMFI, samt hot- och riskbilder som framkommit i dialog med andra aktörer. I figur 2 visas processen för arbetet med strategi, lägesbedömning och handlingsplan.



Figur 2. *Process för arbete med strategi, lägesbedömning och handlingsplan.*

Arbetsprocess nationell handlingsplan

Den nationella handlingsplanen har tagits fram av en arbetsgrupp under SAMFI. Arbetet har innefattat gemensamma arbetsmöten och arbete inom ramen för de i SAMFI ingående myndigheternas ordinarie verksamhet.

Arbetet med handlingsplanen har även innefattat diskussioner och samverkan med ett stort antal aktörer i samhället, exempelvis Informationssäkerhetsrådet[3]. Handlingsplanen har därigenom fortlöpande förankrats på olika nivåer i samhället.

Handlingsplanens terminologi följer i huvudsak SIS handbok Terminologi för Informationssäkerhet (SIS HB 550 utgåva 3). 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 om mer än att säkra it-system; även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

De mål och åtgärder som anges i handlingsplanen är kopplade till de strategiska områden som anges i strategin för samhällets informationssäkerhet. Arbetet ska ske i enlighet med de sex principer för informationssäkerhetsarbete som uttrycks i strategin:

Helhetssyn: För att informationshantering och it-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet. Informationssäkerhet är ett komplext och gränsöverskridande område som spänner över bland annat teknik, administration, ekonomi och juridik.

Ansvar: Allt arbete med informationssäkerhet ska utgå från det i samhället reglerade ansvaret, exempelvis ansvarsprincipen. Den innebär att den som har ansvar för en verksamhet under normala förhållanden ska ha det också vid en krissituation.

Samverkan: Informationssäkerhetens komplexitet, gränsöverskridande karaktär och snabba utvecklingstakt kräver en effektiv samverkan.

Standardisering: Standarder som stödjer informationssäkerhetsarbete bör tillämpas eftersom de bygger på erfarenhet och tar tillvara redan gjorda landvinningar. På så sätt kan en högre säkerhet uppnås och onödiga misstag undvikas.

Riskmedvetenhet: Det krävs resurser för att kunna nå en säker och trygg informationshantering i samhället. Säkerhetsaspekter ska inte ses som en ytterligare kostnadspost, utan som en självklar investering för att uppnå avsedd funktion och kvalitet.

3. https://www.msb.se/sv/Forebyggande/Informationssakerhet/Samhallets-informationssakerhet-/Informationssakerhetsradet/

Regelverk: En förutsättning för en god informationssäkerhet i samhället är att det finns regler som ligger i linje med modern informationshantering. Detta gäller för både verksamhetsnivå och samhällsnivå.

Förvaltning av handlingsplanen

Förvaltningen av handlingsplanen är nära kopplad till arbetet i SAMFI. Handlingsplanen ges ut av MSB i samråd med myndigheterna i SAMFI och är tänkt att uppdateras vart tredje år.

Handlingsplanen från 2008 omfattade 47 åtgärdsförslag. Till stor del har åtgärdsförslagen resulterat i projekt och aktiviteter. Ett stort antal åtgärdsförslag har genomförts medan andra är under genomförande. Vissa åtgärdsförslag har också, där så varit lämpligt, sammanförts med nya eller pågående aktiviteter i 2012 års handlingsplan.

Resultatet av åtgärderna i handlingsplanen från 2008 har löpande avrapporterats till regeringen.

Informationssäkerhet i verksamheter

1. Informationssäkerhet i verksamheter

Informationshantering sker i alla delar av samhället och samhällets informationssäkerhet är följaktligen beroende av ett stort antal aktörer. Statliga myndigheter, kommuner, landsting, företag och andra organisationer har olika förutsättningar, och därmed olika behov och krav på informationssäkerhet

Verksamheter hanterar information som är mer eller mindre konfidentiell, riktighets- och tillgänglighetskritisk. Att ha en god informationssäkerhet är en viktig intern fråga för de flesta verksamheter för att nå upp till de egna kvalitets- och effektivitetskraven. Samtidigt kan informationssäkerhet inte betraktas som enbart en verksamhetsintern angelägenhet. Flöden av tjänster och produkter sker i flera led, och bristande informationssäkerhet kan därför få följdverkningar långt utanför den egna verksamhetens gränser.

Informationssäkerhet handlar om verksamhetens kvalitet. Det innebär bland annat kartläggning av verksamhetens risker samt fördelning av ansvar för att hantera dessa. Att förbättra informationssäkerheten innebär inte enbart att tillmötesgå externa krav, utan även att förbättra verksamheten i sig. Att ha en god informationssäkerhet ska därför ses som en kvalitetsaspekt, ett sätt att uppnå god intern kontroll, ordning och reda. En god informationssäkerhet utgör också en förutsättning för en rad olika it-baserade tjänster som i sig kan vara kostnadsbesparande eller inkomstbringande för verksamheten.

1.1 Utveckla ramverk för informationssäkerhet

Grundelementet i arbetet med informationssäkerhet är ledning och styrning vilket också framgår av ISO/IEC 27000, den internationella standardfamiljen för informationssäkerhet. Stöd för att utveckla den administrativa informationssäkerheten är därför en huvudpunkt i den nationella handlingsplanen.

För att organisationers ledningar ska kunna styra informationssäkerhetsarbetet så att det motsvarar de behov som organisationen har för att kunna uppfylla sitt uppdrag på ett tillfredställande sätt krävs ett ledningssystem för informationssäkerhet (LIS). LIS är också ett effektivt verktyg för att skapa den säkerhetskultur som gör alla medarbetare aktiva i säkerhetsarbetet.

Myndigheterna i SAMFI har tillsammans med andra aktörer arbetat i projektet Stöd för verksamheters informationssäkerhetsarbete (SVISA) för att fram stöd som underlättar för olika organisationer att införa ett ledningssystem för informationssäkerhet. Projektet SVISA är nu avslutat och följs av en förvaltningsfas där ett systematiskt arbete ska bedrivas för att skapa långsiktig kvalitet och användbarhet. Sektorsanpassning av metodstödet kommer också att ske för de sektorer som bedöms som särskilt angelägna.

Under arbetets gång har ett antal prioriterade områden identifierats där ytterligare fördjupning bör ske. De prioriterade områdena är:

- Stöd för ledningsfunktioner att utöva sitt ansvar vad gäller informationssäkerhet, bland annat genom ett systematiskt arbete med riskanalyser och prioritering av skyddsåtgärder.
- Utveckla metoder för riskanalyser som också möjliggör värdering av informationssäkerhetsrisker i förhållande till andra typer av risker samt göra en bedömning av hur olika investeringar ger utdelning i form av bättre säkerhet.
- Utveckla den befintliga modellen för informationsklassning så att den stödjer processen från värdering av konsekvenser fram till användandet av systematiskt utformade skyddsnivåer. I detta arbete kan det även ingå att ta fram definitoner av vissa nationellt gemensamma skyddsnivåer.
- Utveckla stöd för styrningen inom upphandling av system, e-tjänster och andra produkter/tjänster som påverkar informationssäkerheten för verksamheter med stor betydelse för samhällets funktionalitet.
- Utveckla webbplatsen www.informationssäkerhet.se så att den tillhandahåller relevant information och tjänster kring informationssäkerhet för olika aktörer och därmed utgör ett centralt stöd för att utveckla och samordna samhällets informationssäkerhet.

Observera att utbildning och medvetandehöjning som är andra viktiga delar i den administrativa informationssäkerheten behandlas i kapitel 2.

För att kunna prioritera och samordna arbetet med administrativ informationssäkerhet kommer en åtgärdsplan att tas fram.

MÅL
Att tillhandahålla ett över tiden lättanvänt och effektivt stöd för organisationer så att de kan utveckla sin informationssäkerhet.

ÅTGÄRDER
Förvalta arbetet efter projektet SVISA och genomföra de fördjupningar som beskrivs ovan.

GENOMFÖRANDE
MSB samordnar arbetet primärt med myndigheterna inom SAMFI, samt med sektorsansvariga myndigheter, landsting, kommuner och övriga berörda aktörer.

1.2 Krav på säkerhetsanalyser när säkerhetsskyddsförordningen tillämpas

Myndigheter och andra, till exempel kommuner och landsting, som omfattas av säkerhetsskyddsförordningen (1996:633) är skyldiga att undersöka vilken verksamhet som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skydd mot terrorism (säkerhetsanalys).[4] Detta kan omfatta tillgångar i form av personal, materiel, information, anläggningar eller verksamhet. En säkerhetsanalys utgör grunden för ett väl anpassat säkerhetsskydd och är dels en undersökning som syftar till att kartlägga vilka uppgifter som omfattas av sekretess och rör rikets säkerhet i en verksamhet, och dels en handling som dokumenterar de resonemang som leder fram till bedömningen av vad som kräver ett säkerhetsskydd. Säkerhetsanalys avser såväl identifiering och prioritering av skyddsvärda tillgångar, bedömning av säkerhetshot, sårbarheter och risker, som prioritering och hantering av risker inklusive beslut om skyddsåtgärder. Resultatet av en säkerhetsanalys bör utmynna i en säkerhetsplan för att hantera de risker vilka har identifierats i säkerhetsanalysen.

MÅL
Att samtliga myndigheter och andra som säkerhetsskyddsförordningen omfattar har fått information om skyldigheten att undersöka vilken verksamhet som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skydd mot terrorism.

ÅTGÄRDER
Samtliga myndigheter ska ges särskild information om gällande skyldighet att genomföra säkerhetsanalyser enligt säkerhetsskyddsförordningen, samt kopplingen till riskhantering med utgångspunkt i MSBFS 2009:10.

GENOMFÖRANDE
Säkerhetspolisen och Försvarsmakten ansvarar för arbetet i samverkan med MSB.

4. För närvarande sker en översyn av säkerhetsskyddslagstiftningen. Syftet är främst att bättre anpassa lagstiftningen till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet och till de krav det internationella samarbetet ställer. Uppdraget ska redovisas senast den 30 april 2014. (http://www.regeringen.se/content/1/c6/18/22/43/8492cf99.pdf)

1.3 Utveckla metoder för kontinuitetsplanering

Kontinuitetsplanering är en metod för att säkerställa en organisations leveransförmåga genom att planera för fortsatt verksamhet vid förlust av operativ förmåga, det vill säga att trots avbrott kunna leverera de tjänster och produkter som är viktigast för organisationen och dess intressenter.

Idag är tillgången till information en grundförutsättning för att en organisation ska kunna upprätthålla sin verksamhet. Därför blir planering för att kunna upprätthålla system, nätverk och andra komponenter i it-arkitekturen en huvudpunkt i kontinuitetsplaneringen, det vill säga informationssäkerhetsdimensionen är särskilt viktig i planeringen. Samtidigt bör planeringen även beskriva hur vitala aktiviteter ska kunna utföras även utan it-stöd.

Kontinuitetsplaneringen kompliceras av de många beroenden som finns såväl inom som mellan organisationer. För att kunna hantera dessa beroenden, och där så är nödvändigt skapa en samordnad kontinuitetsplanering, bör det finnas gemensamma modeller som kan användas av olika aktörer i respektive organisation. Detta kan också ses som ett underlag för olika typer av avtalsrelationer mellan aktörer samt för samförstånd i olika eskaleringssteg även på det nationella planet.

MÅL

Det ska finnas en generisk modell för kontinuitetsplanering med väldefinierade begrepp som går att anpassa till olika verksamheters behov.

ÅTGÄRDER

En analys genomförs som beskriver dels behoven av kontinuitetsplanering ur informationssäkerhetssynpunkt, dels hur området relaterar till exempelvis krisberedskap och samordning vid allvarliga it-incidenter. Därefter utarbetas förslag på generiska metoder för kontinuitetsplanering ur denna aspekt som också går att synkronisera med en organisations övergripande kontinuitetsplanering.

GENOMFÖRANDE

MSB ansvarar för att en analys av kontinuitetsplanering genomförs och sedan stäms av med SAMFI och övriga intressenter.

1.4 Stödja arbetet med säker e-förvaltning och säkra e-tjänster

Under mer än ett decennium har det funnits en stark intention att utveckla den svenska offentliga förvaltningen mot det som idag kommit att kallas e-förvaltning. Detta innebär bland annat att myndigheterna i allt högre grad erbjuder medborgare och andra intressenter att sköta sina myndighetskontakter via internet.

God informationssäkerhet är en nödvändig förutsättning för en effektiv och förtroendeingivande e-förvaltning. I en så avancerad hantering av information som e-förvaltning är det viktigt att säkerhetsfrågorna inte enbart hanteras med

tekniska lösningar. Tyngdpunkten i säkerhetsarbetet bör vara ledning, styrning och analys i samklang med utvecklingsarbetet för att åstadkomma bra säkerhetslösningar. Då e-förvaltningen bygger på en samverkan mellan olika myndigheter och även andra aktörer måste också E-delegationens arbete bidra till bra styrning av informationssäkerhet.

En grundförutsättning för ett systematiskt informationssäkerhetsarbete är att ha kontroll över informationen. För att identifiera vilken information som skapas och kommuniceras i en organisation är en kartläggning av organisationens processer och den information som genereras den mest effektiva metoden. Ett näraliggande intresse finns hos Riksarkivet som föreskriver en processbaserad redovisning av statliga myndigheters information[5], något som med fördel kan tillämpas även av andra organisationer.

I många e-tjänster som statliga myndigheter och kommuner tillhandahåller behöver motparten identifieras elektroniskt på ett säkert sätt. Det behövs också metoder för att signera handlingar elektroniskt, så att det kan avgöras vem handlingen härrör från och att den inte kan förvanskas. I E-delegationens betänkande SOU 2010:62 påpekas att Sverige har använt samma tekniska lösning sedan 1990-talet när det gäller kryptografisk säkerhet för e-legitimationer och elektroniska underskrifter.[6]

MÅL

Att E-delegationens intentioner och andra initiativ inom e-förvaltningsområdet ska genomföras med informationssäkerhet avpassad efter identifierade och bedömda risker.

ÅTGÄRDER

Ett initiativ för att stödja en säker e-förvaltning ska tas. Initiativet ska bland annat leda fram till en strategi för säker e-förvaltning samt mer specifika åtgärder som stöd för processorienterad kartläggning av information och utredning om ökad kryptografisk säkerhet för e-legitimation och elektronisk signering.

GENOMFÖRANDE

MSB tar inom ramen för arbetet med E-delegationen initiativ till bland annat framtagandet av en strategi för informationssäkerhet inom e-förvaltning samt ansvarar för att initiera övriga åtgärder. I det praktiska arbetet med framtagandet av strategin kommer andra aktörer som myndigheterna i SAMFI och Sveriges kommuner och landsting (SKL) att involveras.

5. RA-FS 2008:4 Föreskrifter om ändring i Riksarkivets föreskrifter och allmänna råd (RA-FS 1991:1) om arkiv hos statliga myndigheter.
6. *Så enkelt som möjligt för så många som möjligt: Under konstruktion – framtidens e-förvaltning,* SOU 2010:62 (http://www.regeringen.se/content/1/c6/15/27/07/2744b8f7.pdf).

1.5 Utveckla stöd till särskilda verksamheter

Samhällets funktioner bygger på att ett stort antal aktörer förmår att skapa och förvalta god informationssäkerhet i sina organisationer. Stöd i informationssäkerhetsfrågor ska därför erbjudas till aktörer som upprätthåller för samhället viktig verksamhet. MSB har för den närmaste treårsperioden i sitt arbete prioriterat följande tre områden:

- Kommunal verksamhet
- Vård och omsorg
- Små och medelstora företag

Prioriteringen bygger både på verksamhetens betydelse och på bedömningen av behovet av stöd. Sveriges kommuner bedriver en verksamhet som är varierad och komplex, samt av stor betydelse för medborgarnas liv och hälsa. Verksamhetens komplexitet ställer höga krav på kommunernas informationssäkerhet. Samtidigt är många kommuner relativt små organisationer som är hårt pressade ekonomiskt och har därför sällan möjlighet att själva bygga upp alla de förutsättningar som krävs för ett systematiskt arbete med informationssäkerhet.

Vård och omsorg fyller en mycket viktig roll både då det gäller människors liv och hälsa och då det gäller samhällets funktionalitet. Därför är det mycket viktigt både ur ett samhällsperspektiv och ur den enskildes perspektiv att vård och omsorg fungerar på ett säkert sätt vilket innebär att kunna motstå och snabbt återhämta sig från oönskade händelser, olyckor och kriser. För att vård och omsorg ska kunna fylla sin viktiga samhällsroll krävs också att medborgare och andra aktörer känner stor tillit till de olika organisationer som levererar olika typer av vård. Samtliga dessa aspekter förutsätter god informationssäkerhet.

Samhällets viktiga funktioner upprätthålls inte bara av offentliga utan i allt högre grad även av privata aktörer. De privata aktörernas behov av säkerhet i sina lösningar för informationshantering är inte mindre än de offentligas och det är därför viktig att näringslivet får stöd för sitt säkerhetsarbete. Stödet bör i första hand riktas till små och medelstora företag då de största aktörerna kan antas ha mer resurser att själva utveckla nödvändiga säkerhetslösningar.

MÅL

Att tillhandahålla ett samordnat stöd för ett systematiskt informationssäkerhetsarbete för prioriterade verksamheter, som samtidigt möjliggör en bättre möjlighet till samordning i händelse av en mer omfattande kris.

ÅTGÄRDER

Aktiviteter ska genomföras för att öka informationssäkerheten inom vård och omsorg, kommuner samt små och medelstora företag. I detta ingår att utveckla nätverk för informationsdelning och samverkan inom respektive verksamhetsområde.

GENOMFÖRANDE

MSB samordnar prioriterade aktiviteter i samarbete med centrala aktörer såsom Socialstyrelsen, SKL samt Svenskt Näringsliv.

1.6 Självmätning av informationssäkerhet

En verksamhets nivå av informationssäkerhet bör minst motsvara dess interna och externa krav. Det är viktigt att en verksamhet kan jämföra sin informationssäkerhetsnivå med andra, liknande, verksamheter för att kunna bedöma sin egen nivå. Att kunna bedöma sin egen verksamhets nivå av informationssäkerhet bidrar i hög grad till verksamhetsledningars medvetande och motivation.

Uppskattningar av nivån på vidtagna säkerhetsåtgärder är viktigt för att den enskilda organisationen ska kunna göra rätt prioriteringar men också för att kunna skapa en översiktlig förmågebedömning. Bedömningen av olika verksamheters nivå av informationssäkerhet är också en viktig faktor för de risk- och sårbarhetsanalyser som ska genomföras inom offentlig sektor.[7]

Det finns heller ingen möjlighet att bedöma informationssäkerheten i en sektor för att få en samlad bild av samhällets informationssäkerhet.
Det är mycket angeläget att det inom offentlig sektor finns ett verktyg där berörda aktörer kan få ett mått på graden av informationssäkerhet i den egna organisationen. Med hjälp av ett antal konkreta frågor går det att skapa en mätning (självmätning) som organisationen kan ställa i jämförelse med andra organisationer (benchmarking). Detta gäller även om verksamheterna självfallet skiljer sig åt från myndighet till myndighet, från kommun till kommun etcetera. Standardiserade självmätningar ger också möjlighet att ge underlag för bedömningar av säkerhetsnivån inom olika sektorer och även för en samlad bild av samhällets informationssäkerhet.

MÅL

Verksamheter kan bedöma sin egen nivå av informationssäkerhet i jämförelse med andra verksamheter i samma sektor. Det ska också vara möjligt att skapa en samlad bild av nivån på verksamheters informationssäkerhet i sektorer och i samhället i stort.

ÅTGÄRDER

Ta fram ett verktyg för självmätning av informationssäkerhet för myndigheter, landsting och kommuner. De olika aktörerna ska på ett säkert sätt kunna föra in uppgifter om sin säkerhetsnivå, samt kunna jämföra sin nivå med andra, i verktyget. Det ska även vara möjligt att i verktyget sammanställa olika avidentifierade rapporter för att kunna skapa en bild av samhällets informationssäkerhet.

GENOMFÖRANDE

MSB samordnar arbetet och tar fram ett verktyg för självmätning av informationssäkerhet som kan användas från och med 2013.

7. *MSBFS 2010:7 föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser, samt MSBFS 2010:6 föreskrifter om kommuners och landstings risk- och sårbarhetsanalyser.*

1.7 Förbättra skyddet av personlig integritet som en del i informationssäkerheten

Ett av de strategiska målen i Strategi för samhällets informationssäkerhet 2010-2015 är att skydda fri- och rättigheter samt personliga integritet. Flera verksamheter hanterar idag stora mängder av personuppgifter och annan information som är av känslig karaktär. Förutsättningen för att dessa organisationer ska kunna upprätthålla en hög grad av tillit bland medborgarna är att de kan skydda den känsliga informationen från otillbörlig åtkomst. Integritetsaspekten har identifierats som central för att kunna utveckla fungerande säkerhetslösningar inom områden som vård och omsorg, men är också en grund i det nya e-förvaltningsarbetet.

Integritet som begrepp är inte entydigt och kan inte enbart hänföras till legala definitioner. I den mån det uppstår en konflikt emellan exempelvis tillgänglighet och integritet måste denna situation lyftas fram och diskuteras öppet för att väl förankrade prioriteringar ska kunna göras. Ur ett samhällsperspektiv måste det också vara tydligt att integritet är den centrala faktorn för att medborgare och andra aktörer ska känna tillit till samhällets funktioner. Saknas denna tillit kommer det att leda till samma konsekvenser som vid avbrott av tillgänglighet, det vill säga funktionen upphör att fungera.

Inom informationssäkerhetsområdet används ofta begreppet integritet i betydelsen egenskap hos en informationstillgång. Detta sätt att använda begreppet är inte synonymt med ”personlig integritet”. För att underlätta informationssäkerhetsarbetet är det viktigt att förtydliga centrala begrepp, och detta gäller i synnerhet begrepp som integritet.

MÅL

Det finns tillgängligt stöd för systematiskt informationssäkerhetsarbete som även inkluderar integritetsaspekterna på ett sätt som skapar tillit för väsentliga funktioner i samhället.

ÅTGÄRDER

Utreda och förtydliga hur personlig integritet ska värnas inom informationssäkerhetsarbetet. Personlig integritet ska vara en drivande faktor vid till exempel val av skyddsnivåer och åtgärder.

Förtydliga hur balans kan skapas mellan å ena sidan personlig integritet och å andra sidan säkerhetsåtgärder som kan vara kränkande, till exempel loggning och annan övervakning.

GENOMFÖRANDE

MSB genomför arbetet i samarbete med Datainspektionen.

1.8 Nationell terminologi för informationssäkerhet

En enhetlig terminologi inom informationssäkerhetsområdet blir allt viktigare i takt med att fler organisationer arbetar aktivt med att förbättra och förvalta sin informationssäkerhet. Det allt mer ökade informationsutbytet över organisationsgränser kräver att det finns enhetliga definitioner som går att använda i avtal och andra typer av överenskommelser. Terminologin är också av stor betydelse för att strategiskt kunna bygga kunskap och kommunicera kring informationssäkerhet inom olika samhällssektorer. Detta gäller inte enbart i det praktiska arbetet med informationssäkerhet inom enskilda organisationer utan är också en förutsättning för en rad andra punkter i handlingsplanen som exempelvis för medvetandehöjande åtgärder, forskning och stöd för e-förvaltning.

SIS HB 550 Terminologi för informationssäkerhet är ett grunddokument för en gemensam och enhetlig terminologi som nu bör revideras med stöd av experter från myndigheterna i SAMFI och andra relevanta parter. En genomgripande begreppsmodellering bör ligga som grund för arbetet för att säkerställa konsistenta begrepp och relationer mellan begrepp.

Arbetet med en reviderad terminologi måste bedrivas långsiktigt och med starkt fokus på tillgänglighet. Därför bör det också tas fram ett förslag på hur terminologin ska förvaltas och fortlöpande revideras på ett kvalitetssäkrat sätt. Den bör också finnas tillgänglig elektroniskt.

MÅL

En kvalitetssäkrad terminologi för informationssäkerhetsområdet som fortlöpande utvecklas och finns tillgänglig för de som arbetar med informationssäkerhet.

ÅTGÄRDER

Att i samarbete med relevanta specialister, SIS/TK 318 Informationssäkerhet och SIS förlag AB ta fram en reviderad version av SIS HB 550 Terminologi för informationssäkerhet, samt säkerställa att det finns en långsiktig förvaltning av terminologin.

GENOMFÖRANDE

FMV/CSEC leder arbetet i samverkan med SIS och övriga myndigheter i SAMFI.

Kompetensförsörjning

2. Kompetensförsörjning

Utvecklingen inom it-området har inneburit och kommer även i fortsättningen att innebära en stark positiv kraft i samhället. Tekniken ger möjlighet till kommunikation, kunskapsutveckling, ekonomisk tillväxt och ökade möjligheter till delaktighet i samhällets demokratiska processer. För att samhället på bästa sätt ska kunna tillvarata utvecklingens positiva effekter krävs både kompetens och medvetenhet rörande de risker som är förknippade med it-användningen. Kunskaper om riskerna med it och elektronisk kommunikation via exempelvis internet bör läras in tidigt och vara en integrerad och naturlig del av den första it-användningen. Därefter ska kunskaperna och färdigheterna följa med under hela skolgången och finnas med i högre utbildningar, inte minst som en integrerad del i utbildningar som leder till yrken med betydande inslag av informationshantering.

I många verksamheter är den mänskliga faktorn kritisk. Stora incidentkostnader kan härledas till brister i medvetenhet och kompetens hos ledning, användare och it-personal. Det är människor som utvecklar, installerar, konfigurerar och använder tekniska system. Det är människor som formulerar, kommunicerar och efterföljer administrativa system. En särskilt viktig grupp ur ett informationssäkerhetsperspektiv är verksamhetsledningar, eftersom det är de som i slutändan ansvarar för kvalitet och säkerhet samt beslutar om skyddsåtgärder. Det finns därmed ett stort behov av kunskap om informationssäkerhet där kompetenshöjande åtgärder måste anpassas för olika roller och verksamheter.

Ett så mångfacetterat område som informationssäkerhet behöver studeras djupare. Forskning och forskarutbildning är nödvändig för att upprätthålla såväl en generell kunskap som spetskompetens inom området. En nationell forskning och forskarutbildning förbättrar dessutom lärarkompetensen inom området – från grundskola till högskolor och universitet.

2.1 Utreda samhällets utbildnings- och kompetensbehov inom informationssäkerhetsområdet

För att samhällets informationssäkerhet ska kunna utvecklas krävs ett stort antal aktörer med olika typer av kompetens inom området. Här finns en skala från expertkompetens till den kompetens som enskilda hemanvändare behöver för att kunna sköta sin informationshantering på ett säkert sätt.

Idag finns olika typer av utbildningar som exempelvis kurser på universitet och högskolor, myndigheter och privata utbildningsföretag samt de internutbildningar som många organisationer själva bedriver. Eftersom informationssäkerhetsområdet i sig är så stort innefattar detta allt från utbildningar som rör ledning och styrning av informationssäkerhet till tekniska säkerhetsåtgärder. Ur ett samhällsperspektiv är det viktigt att skapa, och utgå från, en helhetsbild av både behov och tillgängliga utbildningar för att det ska vara möjligt att prioritera utbildnings- och forskningsinsatser på ett ändamålsenligt och långsiktigt sätt.

Av särskild betydelse är att kunna göra prioriteringar av kompetensbehovet inom samhällsviktiga verksamheter som till exempel vård och omsorg liksom inom branscher med särskilda uppgifter som till exempel internetoperatörer. Även yrkesgrupper med stor betydelse för informationssäkerheten som lärare på olika nivåer, jurister och systemvetare samt professionellt verksamma inom informationssäkerhetsområdet är viktiga uppmärksamma då det gäller kompetensbehov.

Hur utbildningsinsatser av tvärsektoriell karaktär riktade till ledningsfunktioner ska utvecklas är ett annat område som bör analyseras närmare. Detta ska ske samtidigt som arbetet med att utveckla den så kallade CIAO-utbildningen[8] fortsätter.

MÅL

Att på ett effektivt och samordnat sätt kunna höja kompetensen inom området informationssäkerhet utifrån en gemensam behovsbild i samhället.

ÅTGÄRDER

Utreda samhällets behov av kompetens inom informationssäkerhetsområdet i ett femårigt perspektiv.

FRA, PTS och MSB samarbetar med Försvarshögskolan (FHS) om utveckling av CIAO-utbildningen under 2012.

GENOMFÖRANDE

MSB tar initiativ till en utredning om utbildnings- och kompetensbehov inom informationssäkerhetsområdet. Utredningen genomförs i nära samverkan med övriga myndigheter i SAMFI, och andra relevanta aktörer.

8. Chief Information Assurance Officer (CIAO)

2.2 Öka medvetandet om informationssäkerhet i samhället

Samhällsutveckling ställer höga krav på säkerhetsmedvetande. Den offentliga sektorn bör här ta ansvar genom att informera och utbilda i säkerhetsfrågor. Informationssäkerhet är ett stort och komplext område och inbegriper många olika delar och funktioner i samhället. Vid sidan av de tekniska förutsättningarna spelar individen och hur denna väljer att hantera sin information en stor roll i arbetet med att uppnå en god informationssäkerhet.

Många säkerhetsincidenter har idag inte en teknisk utan en mänsklig orsak som i många fall har sin grund i okunskap. Trots detta satsas ofta mer resurser och forskning på utveckling av den tekniska miljön än på förståelse för individens överväganden. Kunskap och medvetande hos den breda allmänheten om varför informationssäkerhet behövs och hur man skyddar sin information är centrala delar i ett informationssäkerhetsarbete. Strategiska överväganden och målmedvetenhet krävs för att bygga upp medvetande och kunskap om informationssäkerhetsfrågor i samhället. Kunskap om hur medvetandet om informationssäkerhetsfrågor ser ut idag i samhället är då i det närmaste en förutsättning för ett effektivt arbete med kunskapshöjande åtgärder.
Det vidtas löpande olika åtgärder för att höja medvetandenivån vad avser informationssäkerhet, till exempel informationsinsatser riktade mot särskilt utvalda målgrupper och utveckling av utbildningsverktyg som exempelvis Datorstödd informationssäkerhetsutbildning för användare (DISA). För att uppnå en långsiktig effekt bör dessa åtgärder samordnas i ett program med strategisk inriktning.

MÅL
Att en relevant och aktuell uppfattning om de risker som finns för olika typer av it-användning är allmänt spridd. Detta gäller både för användning i arbete och på fritid.

ÅTGÄRDER
Ta fram och genomföra ett program för att höja medvetenheten kring informationssäkerhet i samhället.

GENOMFÖRANDE
MSB ansvarar för att ett program för att samordna medvetandehöjande åtgärder tas fram tillsammans med myndigheterna i SAMFI, samt andra relevanta aktörer.

2.3 Utlysning av ramforskningsprogram kring informationssäkerhet

En nationell satsning på forskning och forskarutbildning inom informationssäkerhet är nödvändig för att upprätthålla såväl en generell kunskap som spetskompetens inom området. En utökad nationell forskning och forskarutbildning förbättrar dessutom lärarkompetensen inom området på högskolor och universitet.

Forskning inom informationssäkerhet ska – direkt eller indirekt – leda till nytta för samhället, och därför är det viktigt att den forskning som bedrivs är förankrad i samhället i stort. Forskning inom informationssäkerhet bör ske ur ett brett perspektiv och inte ensidigt fokusera på teknisk forskning, även om detta

naturligtvis är en viktig komponent. Sociala, kulturella, juridiska, ekonomiska och kriminologiska aspekter är exempel på andra områden som behöver studeras inom informationssäkerhetsområdet för att nå en helhetskunskap. Områdets mångfacetterade karaktär medför att kunskapsutveckling bör ske i tvärvetenskapliga miljöer och i samverkan med det omgivande samhället.

Forskning bör stimuleras till att ske i internationell samverkan. Detta motsäger dock inte att det behöver finnas en tydligare nationell samling bakom den forskning som bedrivs i Sverige.

Kartläggning och samordning krävs för att de resurser som läggs på forskning ska ge maximal nytta. Det är därför viktigt att arbeta för fortsatt samverkan kring finansiering av forskning inom informationssäkerhetsområdet.

MÅL
Ökad samverkan mellan forskningsfinansiärer och samhället i stort när det gäller informationssäkerhetsforskning. På lång sikt är målet att svensk forskning inom informationssäkerhetsområdet är samordnad nationellt och internationellt samt har en tydlig inriktning mot samhälleliga behov.

ÅTGÄRDER
Utveckla ramforskningsprogram kring informationssäkerhet och ökad samverkan kring informationssäkerhetsforskning och utveckling i samhället. Ett första steg är att genomföra en utlysning av forskningsmedel inom informationssäkerhetsområdet under 2012.

GENOMFÖRANDE
MSB ansvar för arbetet som genomförs i samverkan med berörda myndigheter.

2.4 Informationsinsats om signalskydd

Signalskydd definieras traditionellt som åtgärder syftande till att förhindra obehörig insyn i och påverkan av vårt lands telekommunikationer. Dessa åtgärder kan utgöras av system med inbyggd kryptering eller system för skydd mot signalunderrättelsestjänst, störsändning eller falsk signalering. För att ett system ska kunna benämnas signalskyddssystem ska det vara godkänt av Försvarsmakten. Signalskyddssystem är konstruerade och anpassade för att möta en hotbild från andra länders samlade underrättelsetjänster och kräver därför omfattande skyddsåtgärder, regelverk, utbildning och hantering. Systemen används framförallt för att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet men kan även användas för att skydda andra uppgifter där man ser en stark hotbild.

I Sverige finns en stor kunskap och kompetens vid de myndigheter som har ansvar inom signalskydds- och kryptoområdet samt vid de företag som utvecklar kryptoprodukter. Denna kunskap kan användas bredare i samhället. Genom rådgivning från ansvariga myndigheter kan säkerhetsnivån i samhällsviktiga verksamheter höjas. Vidare kan arbete göras för att säkerställa att dessa verksamheter har förmåga att skydda sina informationstillgångar och uppnå säkert

tvärsektoriellt informationsutbyte av information som omfattas av sekretess och rör rikets säkerhet. Detta kan ske på central, regional och lokal nivå.

Ett informationsunderlag som vänder sig till relevanta aktörer inom offentlig verksamhet bör utarbetas och spridas för att öka medvetenheten, användningen och visa på vinsten med att använda signalskydd. Informationsunderlaget ska visa på hur information kan skyddas från insyn och påverkan, främst för skydd av information som omfattas av sekretess och som rör rikets säkerhet, med hjälp av signalskydd.

MÅL
Myndigheter, landsting och kommuner ska ha kunskap om vad signalskydd är och hur det kan användas.

ÅTGÄRDER
Ta fram ett informationsunderlag om signalskydd och sprida detta till myndigheter, kommuner och landsting.

GENOMFÖRANDE
Arbetet genomförs i samverkan mellan Försvarsmakten, MSB och FRA, samt övriga berörda myndigheter.

Informationsdelning, samverkan och respons

3. Informationsdelning, samverkan och respons

Att dela information är viktigt för att ta till vara och sprida kunskap och erfarenhet inom informationssäkerhetsområdet. Sådana kunskaper och erfarenheter finns överallt i samhället; både inom offentlig och privat sektor. För att öka samhällets informationssäkerhet är det viktigt att det finns väl fungerande nätverk inom och mellan den privata och offentliga sektorn. Detta är särskilt viktigt när det gäller samhällsviktig verksamhet och kritisk infrastruktur som bedrivs i såväl offentlig som privat regi.[9] Både offentlig sektor och näringsliv har därför nytta av ett ökat informations- och erfarenhetsutbyte.

It-baserade störningar och angrepp sprider sig inte sällan över organisations- och nationsgränser med hög hastighet. Samhället behöver ha en god förmåga att förebygga dessa händelser, och om de ändå inträffar, kunna hantera dem på ett bra sätt. En viktig förutsättning när det gäller samhällsviktig verksamhet och kritisk infrastruktur är det finns en tillräcklig resiliens – det vill säga en förmåga att snabbt återhämta sig efter it-incidenter. Det finns ett behov av ökad samverkan och samordning inom, och mellan, alla samhällssektorer och ansvarsnivåer. En global värld med gränsöverskridande risker och hot kräver även ökad internationell samverkan. Sverige medverkar därför aktivt i internationella samarbeten på flera plan; inom EU, med de nordiska länderna och med enskilda stater.

Den traditionella brottsligheten som bedrägeri, utpressning, förtal och sabotage finns i dag även på internet. Det är ett hot mot samhället, och dessa nya former av brottslighet måste motverkas. It-incidenter som innefattar brottsliga handlingar faller inom polisens ansvarsområde och ska efter polisanmälan hanteras av polisen. Hanteringen av konsekvenserna – det vill säga inte den brottsutredande verksamheten – är dock en fråga för den drabbade organisationen och andra aktörer i samhället. Utgångspunkt för detta arbete är de så kallade Ansvars-, Likhets- och Närhetsprinciperna.[10]

Storskaliga it-incidenter kan ytterst komma att hota Sveriges säkerhet och svenska intressen. I det fall det rör kvalificerade antagonistiska angrepp, har de svenska säkerhets- och underrättelsetjänsterna, samt i de flesta fall Rikskriminalpolisen, ett ansvar.

9. Se även ”Nationell strategi för skydd av samhällsviktig verksamhet” som MSB har tagit fram på regeringens uppdrag.
10. *Ansvarsprincipen:* Den som har ansvar för en verksamhet under normala förhållanden ska ha det också under en krissituation. *Likhetsprincipen:* Under en kris ska verksamheten fungera på liknande sätt som vid normala förhållanden – så långt det är möjligt. Verksamheten ska också, om det är möjligt, skötas på samma plats som under normala förhållanden. *Närhetsprincipen:* Med närhetsprincipen menas att en kris ska hanteras där den inträffar och av dem som är närmast berörda och ansvariga. Det är alltså i första hand den drabbade kommunen och det aktuella landstinget som ansvarar för insatsen. Först om de lokala resurserna inte räcker till blir det aktuellt med regionala och statliga insatser.

3.1 Ökad samverkan för att förebygga och hantera allvarliga it-incidenter

En storskalig it-incident kan få allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur. För att förbättra samhällets förmåga att förebygga och hantera allvarliga it-incidenter anser regeringen att ”det krävs en mer sammanhållen struktur på området. Ett viktigt medel för att uppnå detta är inrättandet av en nationell samverkansfunktion för informationssäkerhet. Regeringen anser därför att MSB i samverkan med berörda myndigheter bör verka för en sådan funktion”.[11]

Regeringen gav den 14 april 2010 MSB i uppdrag att ta fram en nationell plan som klargör hur allvarliga it-incidenter ska hanteras (Fö2010/701/SSK). Den 1 mars 2011 redovisade MSB uppdraget. Syftet med Nationell hanterandeplan för allvarliga it-incidenter är att, genom samverkan och ett koordinerat beslutsfattande, förbättra förutsättningarna för att begränsa och avvärja de direkta konsekvenserna av en allvarlig it-incident i samhället. För att lösa den uppgiften kommer det att krävas ett brett samarbete mellan olika aktörer. Hanterandeplanen fokuserar uteslutande på hanteringen av allvarliga it-incidenter. Den utgår från de grundförutsättningar som finns inom det svenska krishanteringssystemet, det vill säga styrande principer och de enskilda aktörernas ansvar. Hanterandeplanen är interimistisk tills dess att den övats och reviderats i linje med resultaten.

MÅL

Att öka förmågan att förebygga och hantera allvarliga kriser med it-inslag. Allvarliga it-incidenter skall bemötas genom effektiv samordning av samhällets resurser utan att rådande ansvarsförhållanden förändras.

ÅTGÄRDER

Fortsatt arbete med nationell samverkan inom informationssäkerhetsområdet, inom ramen för gällande ansvar och roller.

Fortsatt utveckling av en nationell samverkansfunktion för informationssäkerhet.

Fortsatt arbete mellan säkerhets- och underrättelsetjänsterna för att ytterligare stärka förmågan att hantera allvarliga antagonistiska it-angrepp.

Fastställa den nationella hanterandeplanen för allvarliga it-incidenter efter övning och revidering.

11. Proposition 2010/11:1 utgiftsområde 6, sid. 83, samt *It i människans tjänst – en digital agenda för Sverige* (Näringsdepartementet).

GENOMFÖRANDE

Myndigheterna i SAMFI fortsätter arbete med nationell samverkan för att förebygga och hantera it-incidenter inom ramen för gällande ansvar och roller.

MSB, i samverkan med SAMFI och andra aktörer i samhället, fortsätter arbetet med att utveckla en nationell samverkansfunktion för informationssäkerhet.

MSB, i samverkan med SAMFI och berörda aktörer, reviderar vid behov hanterandeplanen i anslutning till övningen NISÖ 2012 och fastställer hanterandeplanen.

Säkerhets- och underrättelsetjänsterna fortsätter arbetet med att stärka sin förmåga att hantera allvarliga antagonistiska it-angrepp.

3.2 It-incidentrapportering

En viktig del i ett effektivt informationssäkerhetsarbete är att kontinuerligt samla kunskap om vilka incidenter som inträffar eftersom de kan påverka informationstillgångar av betydelse för verksamhetens kontinuitet. Många aktörer har redan insett vikten av att analysera inträffade it-incidenter och föra tillbaka kunskapen till den egna organisationen. Konkret innebär detta att många organisationer idag har infört någon form av rapporterings- och hanteringssystem för it-incidenter. Det finns stora vinster i att inte bara lära av sina egna misstag och incidenter, utan även av andras. Detta gäller såväl inom den enskilda organisationen som på nationell nivå. Därför är det viktigt att skapa förutsättningar för ett väl utvecklat informationsflöde mellan enskilda aktörer och den centrala nationella nivån. En mer systematisk it-incidentrapportering i samhället ersätter dock inte rutinen att anmäla brott till polisen och det är viktigt att rapporteringen inte sker på ett sådant sätt att den kan försvåra brottsutredningar.

Regeringen gav den 14 april 2010 MSB i uppdrag att lämna förslag beträffande ett system för obligatorisk it-incidentrapportering för statliga myndigheter. Den 1 mars 2011 redovisade MSB sitt förslag på hur en sammanhållen struktur för sådan it-incidentrapportering kan utformas. Förslaget kan kortfattat beskrivas som en dubbelriktad rapporteringsprocess för inrapportering till MSB/CERT-SE och återkoppling till berörda parter. Systemet föreslogs bli obligatoriskt för statliga myndigheter och frivilligt för andra aktörer i samhället. I redovisningen av uppdraget bedömde MSB att det krävs en noggrann analys av de rättsliga förutsättningarna för att samla in, lämna vidare och hantera informationen.

I proposition 2011/12:1 (Utgiftsområde 6) skriver regeringen att det är nödvändigt att närmare analysera vilken typ av information en myndighet ska åläggas att samla in och rapportera, vilken myndighet som rapportering ska ske till, samt hur förslaget ska finansieras. De rättsliga förutsättningarna behöver också förtydligas. Regeringen skriver även att ”förutom MBS:s behov av it-incidentinformation utifrån myndighetens samordnande roll vid olyckor och kriser och vid hantering av it-incidenter, kan även Rikspolisstyrelsen (RPS) ha behov av it-incidentrapportering”. I propositionen betonar regeringen även att en it-incident som innefattar en brottslig handling faller inom polisens ansvarsområde. Den 12 april 2012

fick MSB i uppdrag av regeringen att göra en fördjupad analys av obligatorisk it-incidentrapportering för statliga myndigheter. Uppdraget ska redovisas senast den 1 december 2012.

MÅL
Att skapa en god uppfattning om omfattning och inriktning av it-incidenter hos statliga myndigheter och andra aktörer i samhället.

ÅTGÄRDER
Genomföra en fördjupad analys av obligatorisk it-incidentrapportering för, primärt, statliga myndigheter.

GENOMFÖRANDE
MSB genomför en fördjupad analys av obligatorisk it-incidentrapportering i enlighet med uppdrag från regeringen.

3.3 Tekniska detekterings- och varningssystem

Många aktörer använder skyddsmekanismer såsom intrångsdetekteringssystem, brandväggar och antivirussystem för att öka sin informations- och it-säkerhet. It-intrångsdetekterings- och varningssystem är ett viktigt verktyg i arbetet med att bygga upp en nationell lägesbild över verkliga och potentiella it-incidenter samt avvikelser från normalläget. En sådan informationssäkerhetsrelaterad lägesbild är en förutsättning för ett samordnat hanterande av allvarliga it-incidenter. Det är av stor vikt att snabbt kunna detektera och presentera händelseförloppet vid en it-incident. Visar den nationella informationssäkerhetsrelaterade lägesbilden att en rad centrala aktörer i samhället samtidigt drabbats av samordnade intrång, verkliga eller potentiella, ställer det krav på ett annat agerande än om endast någon enstaka aktör är drabbad. Att bygga upp en nationell informationssäkerhetsrelaterad lägesbild, och även skydda samhällsviktiga verksamheter mot angrepp, kan kräva flera olika detekterings- och varningssystem, med olika uppgifter och förutsättningar.

Regeringen gav den 14 april 2010 FRA i uppdrag att lämna förslag på hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan utformas och införas. MSB fick samma dag i uppdrag av regeringen att ta fram ett förslag på hos vilka aktörer ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur skulle kunna införas.

FRA och MSB redovisade sina uppdrag den 1 mars 2011. I propositionen 2011/12:1 skriver regeringen att både MBS:s och FRA:s redovisningar utgör underlag för det fortsatta arbetet och att utgångspunkten bör vara att ”de myndigheter som har ett särskilt ansvar vad gäller krisberedskap enligt bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap i första hand bör delta i ett nationellt detekterings- och varningssystem”.

Den 10 november 2011 fick FRA i uppdrag av regeringen att inkomma med ytterligare information avseende det tekniska detekterings- och varningssystem som myndigheten redovisade 1 mars 2011. FRA redovisade sin fördjupande utredning om tekniska detekterings- och varningssystem den 2 april 2012. Uppdraget genomfördes i samråd med Säkerhetspolisen och omfattade även att ta fram en pilotversion av det föreslagna systemet.

MÅL

Att genom införande av olika typer av tekniska detekterings- och varningssystem i samhället skapas en bättre nationell lägesbild över it-incidenter samt avvikelser från normalläget – en informationssäkerhetsrelaterad lägesbild. Detta skapar förutsättningar för ett samordnat agerande på nationell nivå, vilket i sin tur ger möjligheter att avvärja, eller begränsa konsekvenserna av, allvarliga it-incidenter.

ÅTGÄRDER

Arbetet med tekniska detekterings- och varningssystem fortsätter inom ramen för ordinarie verksamhet hos myndigheterna i SAMFI och andra aktörer. Ett särskilt behov är att utveckla system som på ett säkert sätt kan tillvarata och hantera information från säkerhets- och underrättelsetjänsterna.

GENOMFÖRANDE

FRA fortsätter arbetet med att utveckla ett tekniska detekterings- och varningssystem i enlighet med det förslag som redovisades för regeringen den 2 april 2012.

Övriga aktörer fortsätter arbetet med teknisk detektering av it-incidenter och varningssystem inom ramen för ordinarie verksamhet.

3.4 Nationell samverkan kring arbetet med informationssäkerhet i EU

I den digitala agendan för Sverige anger regeringen att ”Sveriges medverkan i internationella samarbeten inom informationssäkerhetsområdet bör vidare stödjas och utvecklas”.[12]

I arbetet med att förbättra det svenska samhällets informationssäkerhet är det arbete som sker inom ramen för EU av stor vikt. Eftersom Sverige är medlem i EU utgör unionen en viktig arena bland annat när det gäller forskning och teknikutveckling samt normering, det vill säga olika former av lagstiftning och andra styrmedel såsom till exempel standardisering. Det är därför viktigt att Sverige kan utöva ett konstruktivt inflytande på EU:s arbete med informationssäkerhet. För att myndigheter ska kunna stödja det svenska agerandet krävs både sakkunskap och erfarenhet av hur EU:s politik utformas och införs. För att skapa ett inflytande på EU:s arbete med informationssäkerhet är det nödvändigt att välja vilka frågor och processer som ska prioriteras. Det är dessutom viktigt att koordinera de tillgängliga resurserna för att erhålla bästa möjliga effekt.

12. *IT i människans tjänst – en digital agenda för Sverige* (Näringsdepartementet), sid. 41.

MÅL
Genom en ökad nationell samverkan och ett aktivt deltagande i det informationssäkerhetsarbete som sker inom EU, kan Sverige utöva ett konstruktivt inflytande på EU:s arbete inom informationssäkerhetsområdet.

ÅTGÄRDER
Ett aktivt deltagande i det informationssäkerhetsarbete som sker inom ramen för EU och en ökad nationell samverkan kring EU:s arbete med informationssäkerhet.

GENOMFÖRANDE
Myndigheterna i SAMFI verkar för en ökad samverkan kring sitt deltagande i det informationssäkerhetsarbete som bedrivs av EU. Arbetet med dessa frågor sker i en nära dialog mellan berörda myndigheter och departement i Regeringskansliet.

3.5 Planera, genomföra och utvärdera informationssäkerhetsövningar

Regelbundna informationssäkerhetsövningar, inom och mellan olika sektorer och på olika ansvarsnivåer, är en förutsättning för att utveckla och utvärdera de strukturer som finns för att hantera it-incidenter. Övningarna kan exempelvis syfta till att utveckla privat-offentlig samverkan och undersöka hur gemensamma lägesbilder skapas och upprätthålls. EU-kommissionen uppmanar EU:s medlemsstater att anordna regelbundna övningar för insatser och återställning efter storskaliga it-incidenter.[13]

Informationssäkerhetsövningar är en viktig del av nationell och internationell samverkan i syfte att förebygga och hantera allvarliga it-incidenter. I november 2011 genomfördes övningen Cyber Atlantic som ett samarbete mellan EU och USA. I november 2010 genomfördes den paneuropeiska övningen Cyber Europe 2010. Även inom ramen för Nato/PFP genomförs informationssäkerhetsövningar. I maj 2010 och i februari 2008, genomfördes tekniska informationssäkerhetsövningar, så kallade Cyber Defence Exercises (CDX), som en samverkan mellan aktörer i Sverige (SAMFI, Totalförsvarets forskningsinstitut (FOI), FHS med flera) och utlandet. Den 29-30 september 2010 genomförde MSB i samverkan med SAMFI, Svenska kraftnät och privata aktörer från energisektorn den första nationella informationssäkerhetsövningen, benämnd NISÖ 2010.

13. EU-kommissionens meddelande KOM(2011)163.

MÅL

Att genom regelbundna informationssäkerhetsövningar, inom och mellan olika sektorer, på olika ansvarsnivåer nationellt och internationellt, utveckla Sveriges förmåga att hantera allvarliga it-incidenter.

ÅTGÄRDER

Planera, genomföra och utvärdera den nationella informationssäkerhetsövningen NISÖ 2012 och en teknisk informationssäkerhetsövning under 2013, samt kommande övningar.

Delta aktivt i det arbete som sker med informationssäkerhetsövningar inom EU och Nato/PFP.

GENOMFÖRANDE

MSB ansvarar för övningen NISÖ 2012 samt den tekniska informationssäkerhetsövningen under 2013. Arbetet sker i samverkan med SAMFI, sektorsmyndigheter och privata aktörer.

Arbetet med övningar relaterade till skydd av kritisk informationsinfrastruktur (CIIP) och cybersäkerhet inom EU sker i nära samverkan mellan PTS och MSB.

Övningar inom ramen för Nato/PFP sker primärt i samverkan mellan Försvarsmakten och MSB.

Kommunikationssäkerhet

4. Kommunikationssäkerhet

Informationshantering sker regelmässigt mellan fler aktörer vilket ställer krav på säker kommunikation över tele- och datanät. Exempelvis är internet bärare av en stor andel av samhällets informationsflöde. Det är viktigt i detta sammanhang att ha robusta kritiska funktioner i infrastrukturen för elektronisk kommunikation och att det finns säkra kryptografiska funktioner och signalskydd. För förtroendefullt informationsutbyte är det också nödvändigt att elektroniska tjänster bygger på väl fungerande och säkra system.

4.1 Förebyggande åtgärder för att öka säkerheten i de elektroniska kommunikationerna

Det är tele- och internetoperatörernas ansvar att kommunikationsnäten fungerar och är säkra, men ibland kräver samhället ännu högre driftsäkerhet än vad som är affärsmässigt motiverat för företagen, efter att de har uppfyllt lagkraven. Då kan samhället agera för att finansiera förebyggande åtgärder som stärker elektronisk kommunikation mot allvarliga störningar och kriser, exempelvis sabotage, olyckor och naturkatastrofer. Arbetet med förebyggande verksamhet är i många fall exempel på framgångsrik privat-offentlig samverkan. Under de senaste åren finns en rad exempel där finansiering ordnats av till exempel mobila basstationer, reservelkraft, dubbla förbindelser och bergrum. De åtgärder som genomförs ligger i linje med den nationella strategin för robust elektronisk kommunikation.

MÅL

Antalet driftsstörningar inom elektronisk kommunikation minskar och aktörerna inom sektorn stärker sin förmåga att hantera allvarliga driftstörningar.

ÅTGÄRDER

Följande förebyggande åtgärder vad avser fysiska och logiska hot, utbildningar och informationssystem, ska vidtas för att öka driftsäkerheten i elektronisk kommunikation.

- Kartläggningar av sårbarheter i stödsystem och nätdelar hos operatörer inom sektorn för elektronisk kommunikation genomföras.
- Funktionskontroller på skyddade anläggningar inom sektorn för elektronisk kommunikation genomförs.
- Tillträdesskydd vid anläggningar för elektronisk kommunikation stärks.
- En nationell krisledningsövning (Telö) för aktörer inom sektorn för elektronisk kommunikation planeras, genomförs och utvärderas.
- Det nationella systemet för robust och spårbar tid vidareutvecklas.
- Informationssystemen Ledningskollen, Gemensam lägesuppfattning (GLU) och Driftinformation för operatörer (DIO) vidareutvecklas.
- Särskilda utbildningsinsatser inom området driftsäkerhet i stadsnät genomförs.
- En pilotstudie av samhällsviktiga verksamheters behov av elektronisk kommunikation genomförs.

GENOMFÖRANDE

PTS ansvarar för arbetet i samverkan med berörda myndigheter och andra aktörer.

4.2 Åtgärder för att följa upp säkerheten i sektorn elektronisk kommunikation

Genom de ändringar som trädde i kraft i Lagen om elektronisk kommunikation (LEK) den 1 juli 2011 har nytt verktyg i tillsynsverksamheten tillkommit. Operatörerna ska nu till PTS rapportera driftsäkerhets- och integritetsincidenter av betydande omfattning. Inom ramen för detta har PTS utfärdat föreskrifter för att åstadkomma ett tydligt regelverk för rapporteringen av dessa händelser.[14] På detta sätt skapas ett förbättrat underlag för tillsynsarbetet i sektorn.

MÅL

Antalet driftsstörningar inom elektronisk kommunikation minskar och aktörerna inom sektorn stärker sin förmåga att hantera allvarliga driftstörningar.

ÅTGÄRDER

Viktiga åtgärder som ska vidtas för att öka säkerheten i elektronisk kommunikation är:

- En kontinuerlig vidareutveckling av rutiner för daglig bevakning av driftstörningar och hantering av incidentrapporter.
- En analys av tillsynsmetodik genomförs då nya mandat och verktyg har tillkommit.
- En planlagd tillsyn av driftsäkerheten vid den svenska toppdomänen .SE genomförs.
- Allmänna råd ersätts med föreskrifter om driftsäkerhet.
- Föreskrift om säkerhetsskydd för elektronisk kommunikation tas fram.

GENOMFÖRANDE

PTS ansvarar för arbetet i samverkan med berörda myndigheter och andra aktörer.

4.3 Särskild satsning på införande av DNSSEC

En central funktion i internet är det så kallade domännamnssystemet (DNS). Förenklat uttryckt översätter det de adresser som används (till exempel www.myndigheten.se) till IP-adresser för de servrar där den efterfrågade informationen finns, där mottagaren av e-post finns etcetera.

När DNS ursprungligen designades var det andra frågor än säkerhet som var i fokus, bland annat fanns krav att det skulle vara enkelt att snabbt ansluta ytterligare datorer till internet. På senare år har kraven på säkerhet förts fram och ett särskilt tillägg till DNS, kallat DNSSEC, har utvecklats. DNSSEC bygger på att det svar i form av bland annat en IP-adress som domännamnsystemet lämnar signeras med ett certifikat. Detta förhindrar att felaktiga adresser skickas in obehörigen av någon, vilket är en risk i det ursprungliga DNS. En säker DNS inom all offentlig verksamhet är ett fundament för att säkerställa krishanteringsförmågan i en digital värld.

14. Se *PTSFS 2012:01* och *PTSFS 2012:02*.

DNSSEC anses idag vara en självklarhet för den som driver en webbplats där kraven på informationens trovärdighet är höga. Trots detta, och trots de vägledningar som bland annat E-delegationen tillsammans med SKL tagit fram, är andelen webbplatser som använder DNSSEC inom offentlig sektor förvånansvärt låg. Under 2011 har kommuner, via länsstyrelserna, kunnat söka medel ur det så kallade krisberedskapsanslaget i statsbudgeten för att få hjälp med att införa DNSSEC i sin it-infrastruktur. Arbetet har fått starkt genomslag och cirka en tredjedel av landets kommuner har önskat delta. Arbetet kommer att utvärderas under år 2012, men redan nu står det klart att ytterligare steg behöver tas för att införa DNSSEC hos resterande kommuner, men också hos statliga myndigheter, landsting och regioner.

MÅL
Att DNSSEC är infört hos merparten av de offentliga verksamheterna vid utgången av 2014.

ÅTGÄRDER
Följa upp insatserna som gjordes under 2011 och fortsätta arbetet med att införa DNSSEC för återstående domäner inom offentlig sektor.

GENOMFÖRANDE
MSB och PTS i samverkan med .SE (Stiftelsen för internetinfrastruktur) och SKL.

4.4 Krypto för skyddsvärda uppgifter

Det finns behov av att skydda känslig och skyddsvärd information hos myndigheter, kommuner, landsting och organisationer. Om informationen rör rikets säkerhet ska den skyddas med signalskyddssystem godkända av Försvarsmakten.[15] För annan skyddsvärd information finns exempelvis Krypto för skyddsvärda uppgifter (KSU). KSU-system godkänns av Försvarsmakten efter genomförd granskning. Målsättningen med KSU är att kvalitetssäkrade och kommersiellt tillgängliga produkter, tillsammans med ett av Försvarsmakten framtaget regelverk och en för organisationen anpassad hantering, ska kunna höja säkerhetsnivån jämfört med i dag. Genom att använda av Försvarsmakten godkända KSU-system kan organisationer på ett enkelt sätt försäkra sig om att ingående komponenter samt rekommenderad hantering ger ett säkert och effektivt skydd för de uppgifter som organisationen avser att skydda.

För närvarande finns ett filkrypto godkänt som KSU. Det bör utvecklas ytterligare av Försvarsmakten godkända kryptosystem för nivån KSU avsedda för till exempel mobil, tal- och datakommunikation, förbindelsekryptering över Virtuella Privata Nät (VPN), samt för kryptering av USB-minnen.

15. Enligt 13 § Säkerhetsskyddsförordningen (1996:633)

MÅL
Att KSU ska byggas ut och få sådan spridning att skyddsvärd information som hanteras i myndigheter, landsting, kommuner och andra organisationer skyddas med krypto för skyddsvärda uppgifter.

ÅTGÄRDER
Föreslå lösningar på ekonomiska och juridiska aspekter vid införande av KSU.

GENOMFÖRANDE
Försvarsmakten i samverkan med MSB, FRA, samt andra berörda myndigheter.

4.5 Utveckla Swedish Government Secure Intranet (SGSI)

För att uppnå säker kommunikation via EU-kommissionens nät TESTA (Trans-European Service for Telematics between Administrations) med EU:s medlemsstater och organ har det i Sverige etablerats ett nationellt nät, SGSI (Swedish Government Secure Intranet). SGSI kan också användas för säkert informationsutbyte mellan svenska myndigheter. Kommunikationen mellan myndigheterna är krypterad med ett nationellt godkänt signalskyddssystem. MSB är systemägare för SGSI.

SGSI ger idag ett mervärde för anslutna myndigheter. Antalet myndigheter anslutna till SGSI bör öka, dock utan att kostnaderna ökar. Det senare bör kunna förverkligas genom effektivare styrning av förvaltningen av nätet.

MÅL
Att antalet myndigheter som är anslutna till SGSI ska öka, samt att driften av nätet ska effektiviseras och säkerheten i nätet säkerställs över tiden.

ÅTGÄRDER
Vidmakthålla och i vissa avseenden utveckla säkerhetsarbetet i SGSI.
Utveckla tjänster i nätet som efterfrågas av användarna.

GENOMFÖRANDE
MSB ansvarar för genomförandet, delvis i samverkan med berörda myndigheter i SAMFI.

4.6 Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor

Sedan något decennium är det grundläggande för svenska myndigheter att kunna skapa och utbyta digital information i allt större omfattning. Kännetecknande för den digitala utvecklingen är att förändringarna sker i en stegvis upptrappning från lokala lösningar till mer gemensamma lösningar. För den svenska e-förvaltningen blir det allt mer tydligt att lokala lösningar inte är tillräckliga vare sig för funktion eller för säkerhet.

Varje myndighet ska enligt lag och förordning eftersträva hög effektivitet och god hushållning med statens medel i sin verksamhet. Enligt myndighetsförordningen ska myndigheten också utveckla verksamheten och verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Omvärldens förändringar skapar dessutom ett starkt tryck på statsförvaltningen och med den stora effektiviseringskrav.[16]

E-delegationen verkar för att ta fram underlag för gemensamma lösningar där en väsentlig utgångspunkt är att se statlig förvaltning som en helhet. Efter hand som e-förvaltningen slår igenom kommer vissa myndigheter att behöva förmedla stora mängder känslig information elektroniskt mellan sig. Detta ställer inte bara krav på konfidentialitet och sekretess, utan även krav på tillgänglighet, riktighet och spårbarhet.[17]

Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor bör utgå från existerande förutsättningar i samhället. Det handlar bland annat om att nyttja befintlig infrastruktur, anpassa sig till en livskraftig marknad i snabb utveckling och ta tillvara den höga tekniska kompetens som finns inom såväl privat som offentlig sektor.

MÅL
Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

ÅTGÄRDER
Fortsatt arbete med tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

GENOMFÖRANDE
Arbetet med tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor fortsätter inom ramen för de olika aktörernas mandat, och i enlighet med kommande uppdrag från regeringen.[18]

16. *IT inom statlig förvaltning – har myndigheterna på ett rimligt sätt prövat om outsourcing bidrar till ökad effektivitet?* RiR 2011:4, Riksrevisionen, 2011.
17. *Strategi för myndigheternas arbete med e-förvaltning.* Betänkande av E-delegationen, SOU 2009:86.
18. I prop 2011/12.1 (Utgiftsområde 6) anger regeringen att Statskontoret kommer att få i uppdrag att redovisa behovsbilden vad gäller tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

Säkerhet i produkter och system

5. Säkerhet i produkter och system

En långsiktig försörjning av säkra it-produkter ställer krav på formella ramverk för evaluering och certifiering av säkerhetsegenskaper. Sådana ramverk bör vara nationellt och internationellt accepterade.

Inom exempelvis el- och vattendistribution samt spårbunden trafik och petrokemisk industri, används it-system för att styra och övervaka de fysiska processerna. Det är av stor vikt att industriella styrsystem har en hög informationssäkerhet.

5.1 Utveckla ett kryptogranskningsregelverk för kommersiella produkter

Sveriges Certifieringsorgan för it-säkerhet (CSEC) vid FMV har ett system för evaluering och certifiering av it-säkerhet i produkter och system inom ramen för den internationella överenskommelsen CCRA. Vidare har Försvarsmakten ett särskilt ansvar vad gäller godkännande av krypto för skyddsvärda uppgifter (KSU) för den egna myndigheten, totalförsvaret och internationellt samarbete.

FMV/CSEC har på Försvarsmaktens uppdrag utvecklat kompletterande regler för hur krypto kan granskas inom ramen för CSEC:s certifieringsordning. Detta kryptogranskningsregelverk kan utgöra grunden för hur kommersiella produkter genom certifiering vid CSEC enligt dessa kryptoregler kan utgöra grund för KSU-godkännande från Försvarsmakten.

MÅL

Att skapa ett Common Criteria-baserat system för kryptogranskning i Sverige, vilket kan utgöra grund för att fler kommersiella produkter kan erhålla KSU-godkännande från Försvarsmakten.

ÅTGÄRDER

Utveckla ett kryptogranskningsregelverk inom FMV/CSEC certifieringsordning. Ta fram uppgifter och dokumentation, exempelvis protokoll, som kan användas inom ramen för KSU-godkännande från försvarsmakten. Licensiera evalueringsföretag att genomföra kryptogranskning enligt de av FMV/CSEC utvecklade, och av Försvarsmakten godkända, kryptoregelverket.

GENOMFÖRANDE

FMV/CSEC genomför arbetet med stöd av Försvarsmakten och MSB.

5.2 Ökad användning av CC-evaluerade produkter

En ökad tillämpning av Common Criteria (CC) som metodstöd vid kravställande kan bidra till säkrare it-produkter och system. Detta förutsätter dock att standardens metodpaket också utvecklas på ett sätt som så långt som möjligt förenklar användningen.

Det är rimligt att det ställs krav på tillämpning av certifierade produkter, till exempel inom kritiska områden i it-infrastrukturen med stor betydelse för kommunikationssäkerheten eller för säkerhetsprodukter som används i verksamheter med höga krav på konfidentialitet. En stegvis upptrappning av kravmetoderna vid upphandling kan vara en väg mot tillämpning av CC. Bara att ställa krav på att de myndigheter som deltar vid upphandling ska definiera den egna organisationens säkerhetskrav kopplat till det som ska upphandlas kan vara värdefullt som en inledande ansats. I övrigt är målinriktade informationsinsatser av stort värde. Idag finns ett stort antal CC-evaluerade skyddsprofiler (så kallade Protection Profiles, PP) offentliggjorda. En ökad tillgång till skyddsprofiler för efterfrågade säkerhetsprodukter bör öka förutsättningarna för god säkerhet i it-produkter och system.

MÅL
Att svenska myndigheter, och andra verksamheter, ska få stöd vid upphandling av it-säkerhetsprodukter, genom att myndigheterna i SAMFI utvecklar en serie skyddsprofiler. Skyddsprofilerna utgör grund för minimikrav på säkerhetsfunktioner och granskning av sådana produkter som har stor betydelse för verksamheters informationssäkerhet.

ÅTGÄRDER
Utveckla och certifiera skyddsprofiler. Ta fram föreskrift från MSB med krav på it-produkters säkerhetsegenskaper, baserade på kraven i certifierade skyddsprofiler. Ta fram råd och anvisningar för hur verksamheter kan använda produkter som certifieras för att uppnå god informationssäkerhet.

GENOMFÖRANDE
Arbetet med skyddsprofiler genomförs av MSB med stöd av FMV/CSEC och experter från övriga myndigheter i SAMFI.

Arbetet med föreskrifter med krav på it-produkters säkerhetsegenskaper genomförs av MSB i samverkan med FMV/CSEC och Försvarsmakten, samt andra berörda aktörer.

5.3 Nationellt evalueringslaboratorium

En av de stora utmaningarna inom informationssäkerhetsområdet idag är de oerhört stora mängder information som kan lagras i olika former av bärbar datautrustning, till exempel USB-minnen, mobiltelefoner och bärbara datorer. En av de vanligaste orsakerna till stora sekretessförluster är stöld eller förlust av sådan utrustning. Genom kryptering av information som lagras på bärbar datautrustning kan sekretessförlust i flertalet fall förebyggas. Ett sådant krypteringsskydd förutsätter dock att det kan motstå angripare som får fysisk tillgång till upphittad utrustning. En sådan angripare kan genom olika former av fysiska attacker röja kryptonyckeln och därigenom få åtkomst till den krypterade informationen.

Eftersom tillgången till kunskap om hur dessa fysiska attacker kan genomföras får ökad spridning, samtidigt som den utrustning som behövs för att genomföra attackerna i många fall blivit mycket billigare, så har risken för sådana attacker ökat markant. Om det fysiska skyddet av kryptonycklarna inte är korrekt utformat finns det en tilltagande risk att en motiverad angripare framgångsrikt kan forcera skyddet hos upphittad eller stulen bärbar datorutrustning, trots att informationen är krypterad. Det finns en lång rad exempel där olika former av skydd av information i bärbara enheter haft allvarliga brister vilket fått till följd att informationen kunnat läsas utan större insatser.

Till skillnad från andra ledande it-säkerhetsländer (exempelvis Storbritannien, Tyskland, Nederländerna och Spanien) saknar Sverige idag ett nationellt kompetenscentrum för att analysera hur sådana attacker genomförs och hur sådana attacker kan förhindras genom lämpliga tekniska lösningar, även i det fall angriparen har tillgång till datorutrustningen. Konsekvensen av detta är att svenska myndigheter och leverantörer i många fall måste vända sig till andra länder för

att få produkter prövade. Bristen på nationell kompetens inom området innebär även en väsentlig risk att information i bärbar utrustning inte har det skydd som utlovats.

Ett nationellt kompetenscenter bör etableras inom området. Detta kompetenscenter bör även kunna genomföra evaluering av specifika produkter för att tillse att de har ett tillräckligt fysiskt skydd av lagrad information. Genomförda evalueringar ska genom certifiering kunna nå internationellt erkännande.

MÅL
Sverige ska ha egen förmåga att analysera hur fysiska attacker mot information i bärbar datorutrustning kan genomföras och förebyggas. Det ska även finnas nationell kompetens och förmåga att evaluera och certifiera produkter för att visa att dessa har ett adekvat skydd mot fysiska attacker. Sverige ska samverka med andra länder i Europa inom området och kunna genomföra certifieringar av denna typ som erkänns internationellt.

ÅTGÄRDER
Analysera förutsättningarna för ett nationellt evalueringslaboratorium med nödvändig kompetens och utrustning för att analysera fysiska attacker mot information i datorutrustning.

GENOMFÖRANDE
FMV/CSEC utreder förutsättningarna för ett nationellt evalueringslaboratorium i samverkan med Försvarsmakten och FRA.

5.4 Ökad säkerhet i industriella informations- och styrsystem (SCADA)

Industriella informations- och styrsystem (SCADA) används i samhällsviktiga verksamheter och kritisk infrastruktur för att styra och övervaka fysiska processer. Informations- och styrsystem görs i en allt högre utsträckning tillgängliga via publika nätverk (exempelvis internet), bygger allt mer på kommersiellt framtagna och tillgängliga standardprodukter och integreras i högre grad med affärssystem. Den rådande utvecklingen medför en starkt förändrad riskbild i samhället. Sammanfattningsvis krävs därför en ökad nationell förmåga att förebygga och hantera it-relaterade risker och hot mot industriella informations- och styrsystem i samhällsviktig verksamhet och kritisk infrastruktur. Säkerhet i industriella informations- och styrsystem är ett tvärsektoriellt område där det svenska myndighetsansvaret ligger på flera sektors- och tillsynsmyndigheter, samt omfattar både normal verksamhet och krislägen. Säkerhetsproblemen är liknande i alla samhällssektorer och det finns inte någon naturlig sektorsfinansiering.

Samverkan mellan det privata och det offentliga är en grundförutsättning för att öka säkerheten i industriella informations- och styrsystem. Den privata sektorn kommer att få bära huvuddelen av kostnaderna då praktiska åtgärder för att öka säkerheten måste anses vara en del av ett naturligt kommersiellt åtagande hos användare och ägare av systemen. De mer kvalificerade säkerhetsfrågorna har dock bäring på den nationella säkerheten och här har den centrala statsmakten en avgörande roll.

I dagsläget finns få svenska aktörer med djupare kompetens inom området och det fordras ett tydligt statligt engagemang för att säkerställa tillräckliga resurser och kompetens. Nationell och internationell informationsdelning och samverkan förutsätter en svensk statlig förmåga att ta fram egen unik kunskap, såväl som en förmåga att värdera och anpassa kunskap som tagits fram av andra aktörer. Tidigare erfarenheter, både nationella och internationella, visar att det behövs en praktiskt inriktad verksamhet för att skapa det nödvändiga partnerskapet mellan det offentliga och det privata. För att den centrala statsmakten ska kunna vara en ledande aktör och samarbetspartner krävs ett samordnat ledarskap, teknisk kompetens och kontinuitet.

MÅL

Att skapa en ökad nationell förmåga att förebygga och hantera it-relaterade risker och hot mot industriella informations- och styrsystem i samhällsviktig verksamhet och kritisk infrastruktur.

ÅTGÄRDER

Fortsätta att genomföra det program för ökad säkerhet i industriella informations- och styrsystem (SCADA) som initierades av MSB 2010 och kommer att löpa till slutet av 2012. Programmet utgör en samordnad nationell, tvärsektoriell, satsning vilket möjliggör ett effektiv resursutnyttjande och ökar förutsättningarna för att tillvarata de satsningar som görs inom olika sektorer av ansvariga myndigheter. Särskilt viktiga områden är informationssäkerhet i elförsörjningen och i transportsystem.

Planera, genomföra och utvärdera ett program för ökad säkerhet i industriella informations- och styrsystem 2013-15.

GENOMFÖRANDE

MSB fortsätter att genomföra det pågående arbetet i samverkan med myndigheterna i SAMFI, sektors- och tillsynsmyndigheter, samt privata aktörer som äger och driver samhällsviktig verksamhet och kritisk infrastruktur.

Under 2012 tar MSB, i samverkan med berörda, fram ett förslag till program för 2013-15.

Bilaga 1: Samverkansgruppen för informationssäkerhet (SAMFI)

Samverkansgruppen för informationssäkerhet (SAMFI) ska genom att samverka och utbyta information stödja de aktuella myndigheternas uppdrag inom informationssäkerhetområdet. Visionen är att verka för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet. I SAMFI ingår följande myndigheter:

- Försvarets materielverk
- Försvarets radioanstalt
- Försvarsmakten
- Myndigheten för samhällsskydd och beredskap
- Post- och telestyrelsen
- Rikspolisstyrelsen som representeras genom Rikskriminalpolisen och Säkerhetspolisen.

I tabellen nedan sammanfattas de uppdrag som myndigheterna i SAMFI har, särskilt när det gäller informationssäkerhet. Informationen kommer från instruktioner och andra författningar.

MYNDIGHETER MED SÄRSKILT ANSVAR FÖR INFORMATIONSSÄKERHET

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Försvarets materielverk	**Förordning (2007:854) med instruktion för Försvarets materielverk** 5 § Vid Försvarets materielverk finns ett certifieringsorgan som ska upprätta och driva en certifieringsordning för säkerhet i IT-produkter och system. Försvarets materielverk ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat.
Försvarets radioanstalt	**Förordning (2007:937) med instruktion för Försvarets radioanstalt** 4 § Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet. Försvarets radioanstalt får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt ska särskilt kunna 1. stödja insatser vid nationella kriser med IT-inslag, 2. medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system, 3. genomföra IT-säkerhetsanalyser, och 4. ge annat tekniskt stöd. Försvarets radioanstalt ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. **Förordning (2006:942) om krisberedskap och höjd beredskap** 32 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 31 § ska ha säkra kryptografiska funktioner tilldelas sådana.

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Försvarsmakten	**Förordning (2007:1266) med instruktion för Försvarsmakten** 3 b § Försvarsmakten ska särskilt 2. leda och bedriva militär säkerhetstjänst 3. leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information, 4. biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet, 33 § Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret, förutom i fråga om verkställigheten av 33 § förordningen (2006:942) om krisberedskap och höjd beredskap. **Säkerhetsskyddslag (1996:627)** 33 § Regeringen eller den myndighet som regeringen utser meddelar de närmare föreskrifter som behövs för lagens tillämpning. (1996:627) **Säkerhetsskyddsförordning (1996:633)** 13 § Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten 44 § Rikspolisstyrelsen och Försvarsmakten får meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) för sina respektive tillsynsområden enligt 39 §. Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket. 45 § Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Om det behövs skall myndigheterna innan dess samråda med den myndighet som enligt 43 och 44 §§ meddelar föreskrifter för myndighetens område. Myndigheternas föreskrifter får avvika från föreskrifterna enligt 43 och 44 §§ endast om detta har medgivits av den myndighet som har meddelat dessa föreskrifter. **Förordning (2006:942) om krisberedskap och höjd beredskap** 32 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 31 § ska ha säkra kryptografiska funktioner tilldelas sådana.

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Myndigheten för samhällsskydd och beredskap	**Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap** 1 § Myndigheten för samhällsskydd och beredskap har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris. 7 § Myndigheten ska ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att 1. samordna krishanteringsåtgärderna, 2. samordna information till allmänhet och media, 3. effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och 4. samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder. Myndigheten ska ha förmågan att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser. 11 a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället. Myndigheten ska vidare svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. Myndigheten ska i detta arbete: 1. agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade, 2. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och 3. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa. Förordning (2010:1901). *Fortsättning på nästa sida.*

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Myndigheten för samhällsskydd och beredskap	**Förordning (2006:942) om krisberedskap och höjd beredskap** 30a § Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. 31 § Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut, Fortifikationsverket, Totalförsvarets rekryteringsmyndighet, Myndigheten för samhällsskydd och beredskap och Regeringskansliet ska ha säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap beslutar vilka övriga myndigheter som ska ha säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap beslutar även vilka företag som efter överenskommelse ska få tillgång till säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap får därutöver ingå avtal om tilldelning med kommuner och organisationer som har behov av säkra kryptografiska funktioner. 34 § Myndigheten för samhällsskydd och beredskap får 1. meddela de ytterligare föreskrifter som behövs för verkställigheten av 9 § om risk- och sårbarhetsanalyser, 2. meddela föreskrifter om sådana säkerhetskrav som avses i 30 a § med beaktande av nationell och internationell standard, samt 3. meddela de ytterligare föreskrifter som behövs för verkställigheten av 16-20 samt 33 §§, utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket. I 3 § finns undantag från 34 §. 3 § Bestämmelserna i 5-22 och 33-34 §§ gäller för statliga myndigheter under regeringen, med undantag av Regeringskansliet, kommittéväsendet och Försvarsmakten. För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet.

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Post och telestyrelsen	**Förordning (2007:951) med instruktion för Post- och telestyrelsen** 1 § Post- och telestyrelsen är förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. 4 § Post- och telestyrelsen har till uppgift att 1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att tillse att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster, 7. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker, 10. meddela föreskrifter enligt förordningen (2003:396) om elektronisk kommunikation, 14. utöva tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer samt meddela föreskrifter enligt förordningen (2000:833) om kvalificerade elektroniska signaturer, 15. utöva tillsyn enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet, och 16. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, samt verka för ökad krishanteringsförmåga. 17. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer, och 18. lämna råd och stöd till myndigheter, kommuner och landsting samt företag, organisationer och andra enskilda i frågor om nätsäkerhet. Förordning (2010:1913). 7 § Post och telestyrelsen ska 3. vara det behöriga organ som får begära råd och stöd enligt Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet. 5. delta i arbetet i internationella organ i frågor som rör internets förvaltning genom att vid behov företräda Sverige i dessa organ och genom att bereda ärenden med intressenter på nationell nivå. 8 § Post- och telestyrelsen får genom upphandling 4. stärka samhällets beredskap mot allvarliga störningar av elektronisk kommunikation och posttjänster i fred.

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Rikspolis-styrelsen och Säkerhetspolisen	**Förordning (1989:773) med instruktion för Rikspolisstyrelsen** 3 § Rikspolisstyrelsen svarar för samordningen av 5. Polisens beredskap för åtgärder vid incidenter i informationstekniska system (IT-incidenter) **Förordning (2002:1050) med instruktion för Säkerhetspolisen** 2 § Säkerhetspolisen har till uppgift att inom Rikspolisstyrelsen leda och bedriva polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet. Säkerhetspolisen skall även, utöver vad som anges i första stycket, inom Rikspolisstyrelsen leda och bedriva polisverksamhet när det gäller 1. terrorismbekämpning 3 § Säkerhetspolisen skall också 1. fullgöra de uppgifter som Rikspolisstyrelsen har att utföra enligt Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) **Polislag (1984:387)** 2 § Till polisens uppgifter hör att 1. förebygga brott och andra störningar av den allmänna ordningen eller säkerheten, 3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal, 4. lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen, Andra myndigheter ska ge polisen stöd i dess arbete. **Säkerhetsskyddslag (1996:627)** 5 § I verksamhet där lagen gäller skall det säkerhetsskydd finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Säkerhetsskyddet skall utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar. 6 § Med säkerhetsskydd avses 1. skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, 2. skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, och 3. skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet. Lag (2009:464). 7 § Säkerhetsskyddet skall förebygga 1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet), Säkerhetsskyddet skall även i övrigt förebygga terrorism. 9 § Vid utformningen av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt. 33 § Regeringen eller den myndighet som regeringen utser meddelar de närmare föreskrifter som behövs för lagens tillämpning. *Fortsättning på nästa sida.*

Aktör	*Uppgift och föreskriftsrätt med koppling till informationssäkerhet enligt instruktion eller annan författning*
Rikspolis-styrelsen och Säkerhetspolisen	**Säkerhetsskyddsförordning (1996:633)** 43 § Rikspolisstyrelsen får meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om förfarandet vid registerkontroll. Sådana föreskrifter som avser kontroll av personal vid Försvarsmakten skall beslutas efter samråd med Försvarsmakten. 44 § Rikspolisstyrelsen och Försvarsmakten får meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) för sina respektive tillsynsområden enligt 39 §. Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket. 44 a § Rikspolisstyrelsen får, utöver vad som sägs i 43 §, meddela föreskrifter om verkställighet av säkerhetsskyddslagen (1996:627) för sitt tillsynsområde enligt 40 a §. Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket. 45 § Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskydds-lagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Om det behövs skall myndigheterna innan dess samråda med den myndighet som enligt 43 och 44 §§ meddelar föreskrifter för myndighetens område. Myndigheternas föreskrifter får avvika från föreskrifterna enligt 43 och 44 §§ endast om detta har medgivits av den myndighet som har meddelat dessa föreskrifter.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr: MSB423 - augusti 2012 ISBN 978-91-7383-254-0