KRISBEREDSKAPS
MYNDIGHETEN

Samhällets informationssäkerhet

Handlingsplan 2008

2009

2010

Sammanfattning

KBM fick i januari 2007 uppdraget av regeringen att utarbeta förslag till en handlingsplan för samhällets informationssäkerhet. Handlingsplanen består sammantaget av 47 åtgärdsförslag. Följande fyra områden har identifierats som prioriterade.

Det behövs ett förbättrat sektorsövergripande och tvärsektoriellt arbete för samhällets informationssäkerhet. Heltäckande föreskrifter på informationssäkerhetsområdet bör kunna utformas för att gälla samtliga myndigheter under regeringen. Samtidigt behöver det sektorsvisa ansvaret förtydligas. Vidare behöver det finnas möjligheter att ge ändamålsenliga rekommendationer till övriga delar av samhället.

Det behöver fastställas en grundläggande säkerhetsnivå för samhällets informationssäkerhet. En sådan basnivå är en förutsättning för att kunna säkra de informationstillgångar som blivit alltmer fundamentala för såväl näringsliv som offentlig sektor.

Samhället måste kunna hantera omfattande IT-relaterade störningar och kriser. En operativ nationell samordningsfunktion bör därför inrättas.

Det finns kompetensbrister inom informationssäkerhetsområdet på alla nivåer i samhället. Den snabba utvecklingen medför också att kompetensbrister hos den enskilde användaren får allt större konsekvenser. Därför läggs flera förslag som tillsammans utgör en bred satsning för att höja kompetensen inom området.

De förslag som lämnas i handlingsplanen avser åtgärder inom informationssäkerhetsområdet och omfattar hela samhället från normaltillstånd till kris. I handlingsplanen föreslås också en förvaltningsprocess där åtgärderna årligen följs upp och uppdateras.

Handlingsplanen föreslår åtgärder som möter de problem som redovisas i KBM:s årliga lägesbedömning. Åtgärdsförslagen tar också hänsyn till bland annat Infosäkutredningen *Säker information* (SOU 2005:42) samt till regeringens proposition, *Stärkt krisberedskap – för säkerhets skull* (prop. 2007/08:92) samt kommittédirektiv, *En ny myndighet med ansvar för frågor om samhällets krisberedskap och säkerhet* (Dir. 2008:27).

Arbetet har bedrivits i samverkan med myndigheter, kommuner, landsting samt med näringslivet. Myndigheter inom Samverkansrådet för informationssäkerhet (SAMFI) har tecknat samråd på handlingsplanen.

Innehåll

Ord- och förkortningslista

AgN – Arbetsgruppen för näringslivssamverkan. AgN är en undergrupp till *Informationssäkerhetsrådet*.

BITS – Basnivå för informationssäkerhet, utgiven av KBM.

CCRA – Common Criteria Recognition Agreement. CCRA är en samverkan mellan 24 nationer som erkänner varandras certifikat enligt standarden *Common Criteria (CC)*. Sveriges representant för CCRA är *KBM*.

CERT - Computer Emergency Response Team.

CIP – Critical Infrastructure Protection.

CIIP- Critical Information Infrastructure Protection.

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

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

Common Criteria (CC) – Standarden ISO/IEC IS 15408 *Evaluation criteria for IT security.* Common Criteria är en standard för kravställning, deklaration och evaluering av säkerhet i IT-produkter och IT-system samt i deras användningsmiljöer (se avsnitt 9.1).

Digitala kontrollsystem (SCADA) – Datorbaserade system för styrning, reglering och övervakning av fysiska processer som exempelvis el-, gas- och vattenförsörjning samt spårbunden trafik (se avsnitt 9.2).

EPCIP – European Programme for Critical Infrastructure Protection.

EU – Europeiska unionen.

FIDI – Forum för informationsdelning avseende informationssäkerhet. En modell för samverkan inom informationssäkerhet mellan privata och offentliga aktörer (se avsnitt 7.3.1).

FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems (FIPS = Federal Information Processing Standards Publications).

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

FISMA – Federal Information Security Management Act of 2002.

FOI – Totalförsvarets forskningsinstitut.

FM – Försvarsmakten.

FMV – Försvarets materielverk.

FRA – Försvarets radioanstalt.

IEC – International Engineering Consortium.

ISO – International Organization for Standardization.

ISO/IEC 27001 – Kravstandard för ledningssystem för informationssäkerhet.

ISO/IEC 27002 – Riktlinjer (s k ”best practice”) för ledningssystem för informationssäkerhet.

Informationssäkerhetsrådet - Ett råd avseende nationella informationssäkerhetsfrågor med representanter från strategiska aktörer inom området. Rådet leds av *KBM*.

KBM – Krisberedskapsmyndigheten.

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

MSB – Myndigheten för samhällsskydd och beredskap.

PP – Protection Profile.

PTS – Post- och telestyrelsen.

RKP – Rikskriminalpolisen.

RPS – Rikspolisstyrelsen.

S-BIT – Gemensam funktion hos RKP och Säpo avseende samordning av IT-relaterade brott och incidenter.

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

SCADA – Se *digitala kontrollsystem*

SGSI – Swedish Government Security Intranet. Svenskt nationellt nät som används för kommunikation mellan svenska myndigheter och med EU kommissionens nät *TESTA* (se avsnitt 8.3).

Sitic – Sveriges incidentcentrum. Drivs av *PTS*.

Säpo – Säkerhetspolisen.

TESTA – Trans-European Service for Telematics between Administrations. EU-kommissionens nät för kommunikation med EU:s medlemsstater (se avsnitt 8.3).

TSS – Totalförsvarets signalskyddsskola.

Verva – Verket för förvaltningsutveckling.

1 Inledning

Krisberedskapsmyndigheten (KBM) har det sammanhållande myndighetsansvaret för frågor rörande informationssäkerhet och har i denna roll fått uppdraget av regeringen att upprätta en handlingsplan för att genomföra och förvalta nationens strategi för informationssäkerhet. I detta avsnitt beskrivs uppdraget till KBM, tolkningen av uppdraget samt valt angreppssätt för att utföra uppdraget.

1.1 KBM:s uppdrag

I regeringens proposition *Samverkan vid kris – för ett säkrare samhälle* (prop. 2005/06:133) anges att KBM ska utarbeta förslag till en handlingsplan för informationssäkerhet. I Krisberedskapsmyndighetens regleringsbrev för 2007 anger Försvarsdepartementet följande:

> Krisberedskapsmyndigheten ska inom ramen för sitt informationssäkerhetsarbete och utifrån nuvarande ansvarsförhållanden inom området lämna förslag till en handlingsplan för genomförande och förvaltande av den nationella strategin för informationssäkerhet. Arbetet ska bedrivas i samverkan med berörda myndigheter, kommuner, landsting samt med näringslivet. Tillsyns- och sektorsmyndigheternas ansvar ska särskilt beaktas och de ska beredas möjlighet att lämna synpunkter på förslaget. En lägesrapport ska redovisas senast den 30 augusti 2007 och uppdraget ska slutredovisas i samband med årsredovisningen 2008.

1.1.1 Tolkning av uppdraget

Den nationella strategin för informationssäkerhet är en grundförutsättning för handlingsplanens utformning. Regeringens strategi för informationssäkerhet finns uttryckt i propositionerna *Samhällets säkerhet och beredskap* (prop. 2001/02:158) och *Samverkan vid kris – för ett säkrare samhälle* (prop. 2005/06:133). Ett delbetänkande i Infosäkutredningen, *Säker information – förslag till informationssäkerhetspolitik* (SOU 2005:42), innefattar ett förslag till strategi omfattande tio punkter, vilka också bör beaktas.

Genomförande innebär ett antal aktiviteter och åtgärder som syftar till att realisera strategin. Förvaltning tolkas som underhåll av de realiserade åtgärderna, till exempel uppföljning och uppdatering, men också av målen med informationssäkerhet, det vill säga strategin.

1.2 Ingångsvärden

Handlingsplanen tar hänsyn till regeringens proposition, Stärkt krisberedskap – för säkerhets skull (prop. 2007/08:92) samt kommittédirektiv, En ny myndighet med ansvar för frågor om samhällets krisberedskap och säkerhet(dir. 2008:27) från den 13 mars 2008. Propositionen föreslår att KBM, Statens räddningsverk och Styrelsen för psykologiskt försvar, ska läggas ned den 31 december 2008 samt att en ny myndighet, *Myndigheten för samhällsskydd och beredskap* (MSB) inrättas den 1 januari 2009.

1.2.1 Nationell strategi för informationssäkerhet

Den strategi som avses i regleringsbrevet föreslogs i propositionen *Samhällets säkerhet och beredskap* (prop. 2001/02:158) samt kompletterades senare i propositionen *Samverkan vid kris – för ett säkrare samhälle* (prop. 2005/06:133).

Den övergripande strategin har följande lydelse (prop. 2001/02:158):

> Målet bör vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man ska kunna förhindra eller hantera störningar i samhällsviktig verksamhet. Strategin för att uppnå detta mål bör liksom övrig krishantering i samhället utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen.
>
> Principiellt gäller att den som ansvarar för informations-behandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet ska fungera tillfredsställande. En viktig roll för staten är därför att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den enskilda systemägaren.
>
> För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas.

Inriktningen av den nationella strategin för informationssäkerhet kompletteras i prop. 2005/06:133 enligt följande:

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

1.2.2 Infosäkutredningens strategi

Infosäkutredningen delbetänkande *Säker information – förslag till informationssäkerhetspolitik* (SOU 2005:42) redovisar ett förslag till strategi för informationssäkerhet. Denna strategi, liksom utredningens övriga delar, har beaktats i framtagandet av handlingsplanen. Strategin består av följande tio punkter:

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

1.3 Metod

Handlingsplanen bygger på samverkan med andra aktörer, dokumentstudier och egna fördjupningsstudier. Dessa metoder beskrivs nedan.

En viktig utgångspunkt för handlingsplanen åtgärdsförslag är identifierade hot och sårbarheter. Dessa redovisas emellertid inte mer utförligt i handlingsplanen utan återfinns i andra dokument, bland annat KBM:s årliga lägesbedömningar samt tidigare nämnda propositioner och utredningar.

1.3.1 Samverkan

Experter på olika områden har bidragit med kunskap, kritik och textförfattande. Extern samverkan har skett genom möten, konferenser och workshops. I första hand har samverkan skett med KBM:s olika forum för samverkan inom informationssäkerhet:

- *Samverkansgruppen för informationssäkerhet (SAMFI)*. Deltagare är representanter för de sju myndigheterna KBM, Post- och telestyrelsen (PTS), Verket för förvaltningsutveckling (Verva), Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Försvarsmakten (FM) samt Rikskriminalpolisen (RKP) och Säkerhetspolisen (SÄPO). Dessa myndigheters respektive uppgifter och roll återfinns i bilaga 4.
- *Informationssäkerhetsrådet* är ett råd avseende nationella informations-säkerhetsfrågor med representanter från strategiska aktörer inom området.
- *Arbetsgruppen för Näringslivssamverkan (AgN)*. AgN är en undergrupp till Informationssäkerhetsrådet med representanter från det svenska näringslivet.

Förutom dessa forum har enskilda möten med svenska aktörer genomförts; dels aktörer som återfinns i de ovan nämnda grupper, och dels möten med andra strategiskt viktiga aktörer. Internationella kontakter har förts genom bilaterala möten med till exempel tyska och norska myndigheter, samt genom deltagande på konferenser och workshops. Samtliga aktörer som KBM samverkat med redovisas i Bilaga 3.

1.3.2 Dokumentstudier

Infosäkutredningen har varit en viktig utgångspunkt i utformningen av handlingsplanen eftersom den är aktuell, är omfattande och har remitterats på bred basis. I övrigt har både nationella och internationella rapporter använts som underlag. Samtliga dokument som legat till grund för handlingsplanen återfinns i avsnittet referenser.

1.3.3 Fördjupade studier

Tre fördjupande studier har genomförts:

1. Studie av hur Sverige ska bli bättre på att agera i informationssäkerhetsfrågor inom EU. Studien har genomförts av Försvarets forskningsinstitut (FOI).
2. Analys av vårdsektorn och finanssektorn i syfte att identifiera pågående arbete med informationssäkerhet och framtida svagheter (beroenden, sårbarheter) och planerade åtgärder (Meile AB).
3. Observationsstudie av IT-attackerna mot Estland våren 2007. Utredningen har genomförts av informationssäkerhetsenheten på KBM.

1.4 Definition av informationssäkerhet

Handlingsplanens terminologi följer 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 informations-tillgångar. 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 informationssystem; även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

1.5 Disposition

Dokumentet inleds med detta introduktionskapitel och fortsätter med kapitel två som ger en beskrivning av informationssäkerhetens karaktäristik.
Kapitel tre behandlar genomförandet av handlingsplanen. Här återfinns de mest centrala åtgärdsförslag som kräver beslut av regeringen samt förslag på hur handlingsplanen ska förvaltas.

Kapitel fyra till nio behandlar sakområden (exempelvis kompetensförsörjning) med underavsnitt (till exempel forskning). Varje underavsnitt består av bakgrund, målbeskrivning och åtgärdsförslag.

2 Informationssäkerhet i samhället

Informationssäkerhet omfattar hela samhället, och är därför en angelägenhet för alla. Informationssäkerhet handlar om förtroende, med målsättningen att samtliga aktörer i samhället kan lita på informationssystemen. Informationssäkerhet bidrar till att IT-utvecklingen i samhället kan fortskrida med hög kvalitet.

Informationssäkerhet är en stödjande verksamhet för att öka kvaliteten hos samhällets funktioner. Ytterst handlar det om att slå vakt om en mängd olika värden och målsättningar i samhället, såsom demokrati, personlig integritet, tillväxt samt ekonomisk och politisk stabilitet. I och med den ökande IT-användningen i samhället är informationssäkerhet en förutsättning för att nya företeelser i samhället som till exempel e-förvaltning ska kunna fungera.

Genom god informationssäkerhet i samhället kan man främja:

- Samhällets effektivitet och kvalitet i informationshantering
- Näringslivets lönsamhet och tillväxt
- Samhällets brottsbekämpning och beredskap mot allvarliga störningar och kriser
- Medborgares fri- och rättigheter samt personliga integritet
- Medborgares och verksamheters förtroende för informationshantering och IT-system

2.1 Informationssamhällets hot och sårbarheter

Det pågår en samhällsutveckling där informationshantering i allt högre grad utförs med stöd av IT. Detta ökade beroende innebär även ökade risker för enskilda och organisationer. Det sker också en entydig ökning av informationssäkerhetsrelaterade hot såsom dataintrång, bedrägerier och spridning av skadlig kod. Bakomliggande aktörer utgörs av såväl organiserad brottslighet, terrorister som statsmakter.

Brister i informationssystem kan också påverka fysiska tillgångar. Skador på den kritiska infrastrukturen kan få ödesdigra följder. Incidenter som leder till oförmåga eller förstörelse av sådana system och tillgångar kan leda till allvarliga kriser som drabbar de finansiella systemen, allmänhetens hälsa, den nationella säkerheten, eller kombinationer av dessa.

Brister i hantering av information leder till ett försämrat förtroende för aktuella tjänster och bakomliggande aktörer, och kan därför äventyra aktörens verksamhet och användningen av dess tjänster. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till fler aktörer och tjänster och även till andra sektorer. Exempelvis kan ett försämrat förtroende för Internetbanker smitta av sig till andra sektorer i samhället som erbjuder Internetbaserade tjänster.

2.2 Aspekter på informationssäkerhet

För att uppnå en god informationssäkerhet i samhället krävs att man särskilt beaktar följande viktiga aspekter:

- Helhetssyn
- Standardisering
- Kompetens och medvetenhet
- Samverkan
- Resurser
- Regelverk

2.2.1 Helhetssyn

Informationssäkerhet är ett komplext och gränsöverskridande område som spänner över bland annat teknik, administration, ekonomi och juridik. Vid arbete med att förbättra informationssäkerheten i organisationer och på nationell nivå krävs att hänsyn tas till dessa områden.

Skyddsåtgärder bör både syfta till att skapa en mer robust informationshantering vid samhällets normaltillstånd och för att hantera mer allvarliga störningar och kriser. En god vardagssäkerhet är ofta likställd med att ha en god förberedelse för allvarligare händelser. Exempelvis kan en god internkontroll i verksamheter, kompetens inom informationssäkerhet samt god samverkan innebära en grund för en god operativ förmåga i händelse av ett krisläge.

Det behövs en helhetssyn som är sektorsövergripande och tvärsektoriell utöver det som hanteras av respektive sektor. Utifrån en bred syn på informationssäkerhet syftar denna handlingsplan till att bidra med att IT och informationshanteringen i samhället utvecklas på ett tryggt och säkert sätt i syfte att främja såväl normaltillståndet som krishanteringsförmågan. Åtgärderna i handlingsplanen knyter därför på olika sätt an till de båda nivåerna.

2.2.2 Standardisering

En viktig aspekt vid säkerhetshöjande åtgärder är att arbeta utifrån beprövade tekniker och arbetssätt. Olika former av standarder erbjuder verksamheter att tillämpa något som är beprövat och byggt på erfarenheter och därför skapar förutsättningar för bättre säkerhet. Tillämpning av standarder innebär att man kan anpassa något som är genomtänkt till det egna behovet. Man vinner dessutom stordriftsfördelar när fler använder samma lösningar och tidskrävande tjänste- och produktutveckling blir snabbare, enklare och billigare när man på förhand vet vilka ramar som tillämpas. Genom spridning av standarder förenklas utbildning och därmed förbättras utbudet av kompetens. Standarder ökar också transparensen mellan organisationer vilket underlättar kravställning och bedömning av säkerhetsnivåer i produkter, system och hela verksamheter.

2.2.3 Kompetens och medvetenhet

IT-användning är idag en integrerad del i de flesta verksamheter och i samhället i stort. Brister i kompetens leder till sårbarheter och kunskapsbehoven är därför stora. En mängd insatser i form av information, utbildning och övning behövs därför i samhället med målsättningen att på sikt skapa en *informationssäkerhetskultur*. Man behöver genomföra utbildningsinsatser i verksamheter och inom utbildningsväsendet och dessutom bör man satsa på att öka informationssäkerhetsmedvetandet i samhället i stort, exempelvis genom att stödja folkbildning inom området.

2.2.4 Samverkan

På grund av informationssäkerhetens komplexitet, gränsöverskridande karaktär och snabba utvecklingstakt krävs en effektiv informationsdelning och samverkan för att nå goda resultat. Det handlar om samverkan mellan olika aktörer i Sverige, såsom statliga myndigheter, kommuner och landsting, näringsliv och intresseorganisationer, och internationell samverkan. En god samverkan kring informationssäkerhet i samhället är viktigt under ett normaltillstånd, men också en nödvändighet för att kunna skapa en god operativ förmåga i krissituationer.

2.2.5 Resurser

För att lyckas med att nå en säker och trygg informationshantering i samhället måste resurser läggas på informationssäkerhet. Säkerhetsaspekter ska inte ses som en ytterligare pålaga, utan som en självklar investering för att uppnå avsedd funktion och kvalitet. Investeringar inom informationshanteringar görs inte sällan i syfte att effektivisera och rationalisera tjänster i samhället. Det är därför rimligt att en del av besparingarna satsas på att uppnå kvalitet och robusthet genom ökade säkerhetsinsatser. Kostnader för att bygga in och förbättra säkerhet bör alltid jämföras med vad det kan kosta att inte göra detta.

2.2.6 Regelverk

En förutsättning för en god informationssäkerhet i samhället är att det finns regler som ligger i linje med aktuell informationshantering. Det behövs författningsstyrning för att nå detta mål. Dessa författningar bör vara generiska och teknikoberoende för att kunna fungera under lång tid även vid den snabba teknikutvecklingen.

3 Genomförande

De förslag som lämnas i handlingsplanen avser uppgifter och ansvar, tidsförhållanden och kostnadsuppskattning inom informationssäkerhetsområdet och omfattar hela samhället från normaltillstånd till kris. Genomförandefasen kommer att involvera många aktörer som ensamma eller tillsammans med andra genomför åtgärderna. Det ansvarsförhållande som anges syftar på den aktör som bär ansvaret för genomförandet av ett åtgärdsförslag. Utgångspunkten för att genomföra det som anförs i handlingsplanen är baserat på ansvarsprincipen.

Vidare varierar tidsförhållanden för de olika åtgärdsförslagen. Tidsförhållanden anges inom ramen för vilket år åtgärden bör påbörjas eller inom vilken tid en åtgärd planeras vara genomförd, ett till fem år. Handlingsplanen innehåller 47 förslag som bör realiseras inom en femårsperiod.

En del kan genomföras omgående och till låga kostnader medan andra kan genomföras först på lång sikt och föranleda stora kostnader. Under kostnad anges en kostnadsuppskattning för de föreslagna åtgärderna. Kostnadsuppskattningen görs med avseende på följande indelning:

Kostnadsneutral: Ringa kostnader eller kostnader som ryms inom myndighets ordinarie verksamhet
Låg: Under 5 miljoner
Medel: 5-10 miljoner
Hög: Över 10 miljoner

Kostnaden för åtgärdsförslagen är uppskattad på årsbasis för berörd myndighet.

3.1 Beslut om åtgärdsförslag

Handlingsplanen består av 47 åtgärdsförslag. De förslag som bedöms som särskilt viktiga och övergripande beskrivs i detta avsnitt. I övriga avsnitt presenteras ett antal andra förslag som också bedöms som viktiga att genomföra. KBM föreslår att regeringen beslutar om:

Åtgärdsförslag 4: Översyn av lagstiftningen på informationssäkerhetsområdet (kap. 4)
Regeringen bör tillsätta en utredning som gör en heltäckande analys av författningar som berör informationssäkerhetsområdet.

Kostnad: Förslaget medför medelstor kostnad
Tid: Bör påbörjas under år 2008
Ansvar: Statlig utredning (SOU)

Åtgärdsförslag 5: Föreskriftsrätt inom informationssäkerhetsområdet (kap. 4)
Regeringen bör ge MSB rätt att utfärda föreskrifter och allmänna råd för att myndigheter ska kunna uppnå grundläggande och särskilda tilläggskrav på informationssäkerhet. Förslag till bemyndigande framgår av bilaga 2.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Under år 2009
Ansvar: Regeringen

Åtgärdsförslag 6: Myndighetsledningars formella ansvarstagande för hantering av informationssäkerhetsrisker (kap. 5)
Regeringen bör besluta att det ställs krav på myndigheter att i sin årsredovisning redovisa på vilket sätt gällande krav på informationssäkerhet uppfylls.

Kostnad: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: Samtliga myndigheter

Åtgärdsförslag 16: Nationellt kunskapscentrum för informationssäkerhet (kap. 6)
Regeringen bör ge i uppdrag till MSB att närmare utreda hur ett nationellt kunskapscenter för informationssäkerhet kan upprättas. Syftet med kunskapscentret ska vara att öka och samordna kvalificerad kunskapsutveckling, samt utgöra ett expertcentrum inom området. Kunskapscentret kan organiseras i form av en stiftelse med en styrgrupp inkluderande intressenter från såväl staten, näringslivet som akademin. Centrumet kan delfinansieras genom statliga anslag.

Kostnad: Förslaget medför låg kostnad
Tid: Under år 2009
Ansvar: MSB i samverkan med näringslivet och universitet och högskolor

Åtgärdsförslag 26: Operativ nationell samordning (kap. 7)
Regeringen bör ge KBM och berörda myndigheter i uppdrag att lämna underlag till regeringen om hur man kan skapa en administrativ och teknisk infrastruktur för informationsdelning och respons inom informationssäkerhet för hela samhället. Förslaget bör omfatta gemensam kunskapsdelning, gemensam lägesbildsfunktion och operativ förmåga vid omfattande IT-incidenter. Verksamheten ska fungera under såväl normala förhållanden som vid en kris.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2008
Ansvar: KBM i samverkan med berörda myndigheter och näringsliv

Åtgärdsförslag 28: Obligatorisk incidentrapportering (kap. 7)
Regeringen bör införa krav på att statliga myndigheter ska rapportera inträffade informationsrelaterade incidenter, utom för den typen av incidenter som är undantagna genom lagstiftning. Krav på omedelbar rapportering ska gälla större incidenter som gett eller kunnat ge allvarliga konsekvenser. Se även åtgärdsförslag 26.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2010
Ansvar: Samtliga myndigheter

Åtgärdsförslag 29: Utveckling av förmågan att förebygga och bekämpa IT-relaterad brottslighet (kap. 7)
Regeringen bör besluta att tilldela Rikspolisstyrelsen särskilda medel för att utveckla förmågan att förebygga och bekämpa IT-relaterad brottslighet.

Kostnad: Förslaget medför medelstor till hög kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Regeringen

Åtgärdsförslag 36: Etablera ett forum för samverkan inom ramen för EPCIP (kap. 7)
Regeringen bör ge MSB med stöd av PTS i uppdrag att inför Sveriges ordförandeskap i EU hösten 2009, utveckla ett EU-forum för sektorsövergripande samverkan inom informationssäkerhet och skydd av kritisk informationsinfrastruktur. Ett sådant forum bör utgå från det befintliga EPCIP-samarbetet (European Programme for Critical Infrastructure Protection).

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB med stöd av PTS

Åtgärdsförslag 47: Statlig samordnad satsning på säkerhet i digitala kontrollsystem inom samhällsviktiga verksamheter (kap. 9)
Regeringen bör ge MSB i uppdrag att genomföra en statlig satsning på säkerhet i digitala kontrollsystem. Avsikten med ett sådant initiativ är att skapa en ökad nationell förmåga att förebygga och hantera störningar i de informations- och kommunikationssystem som används för styrning, övervakning och kontroll av samhällsviktiga verksamheter.

Kostnad: Förslaget medför hög kostnad
Tid: 2009-2011
Ansvar: MSB i samverkan med berörda myndigheter och näringsliv

3.2 Förvaltning av handlingsplanen

3.2.1 Bakgrund

I förvaltningen ingår att följa upp hur förslagen genomförs samt att revidera och konkretisera handlingsplanen utifrån behov och förändrade förutsättningar. Därmed kan handlingsplanen kontinuerligt anpassas utifrån samhällsutvecklingen. Handlingsplanen bör uppdateras på årsbasis med start 2009. Förvaltningen av handlingsplanen bör ske i bred samverkan med samhällets aktörer, på ett liknande sätt som skett vid framtagningen av den. Uppdaterade versioner av handlingsplanen bör lämnas till regeringen i samband med den lägesbedömning som idag tas fram av KBM. Därmed får man en tydlig koppling mellan å ena sidan hot, sårbarheter, trender och å andra sidan åtgärdsförslag som möter dessa. I samband med revidering av handlingsplanen till 2009 bör också den nationella strategin uppdateras. Eftersom att en mängd händelser inträffat inom informationssäkerhetsområdet under den senaste tiden, bör en ny strategi formuleras. Efter att en uppdaterad strategi är formulerad bör denna revideras i en cykel på tre till fem år.

3.2.2 Åtgärdsförslag

Målsättning förvaltning

- *Den övergripande målsättningen med förvaltningen är att åstadkomma en kontinuerlig process där både strategin och handlingsplanen på regelbunden basis uppdateras.*

Åtgärdsförslag 1: Förvaltning av handlingsplanen under 2008
Regeringen bör ge KBM i uppdrag att i samverkan med berörda myndigheter förvalta handlingsplanen till och med den 31 december 2008.

Kostnad: Förslaget är kostnadsneutralt
Tid: Under 2008
Ansvar: KBM i samverkan med berörda myndigheter

Åtgärdsförslag 2: Fortsatt förvaltning av handlingsplanen
Regeringen bör ge MSB i uppgift att från och med 2009 förvalta handlingsplanen och årligen redovisa hur genomförandet av åtgärdsförslagen fortskrider samt behov av nya åtgärder. Förvaltningen av handlingsplanen bör ske i samverkan med samhällets aktörer.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB i samverkan med berörda myndigheter

Åtgärdsförslag 3: Uppdatering av strategin
Regeringen bör ge MSB i uppgift att lämna förslag på uppdatering av den nationella strategin utifrån den rådande samhällsutvecklingen. Efter att strategin är formulerad därefter bör denna uppdateras i en cykel på tre till fem år.

Kostnad: Förslaget medför medelstor kostnad
Tid: år 2009
Ansvar: MSB i samverkan med berörda myndigheter

4 Författningsöversyn och föreskriftsrätt

4.1 Bakgrund

Den snabba utvecklingen inom informationssäkerhetsområdet under de senaste åren har inneburit att de författningar som påverkar informationssäkerhetsområdet behöver anpassas därefter. Det är svårt att uppnå en god informationssäkerhet på övergripande samhällsnivå i Sverige utan stöd av en lagstiftning som så långt möjligt är anpassad till aktuella former för informationshantering. De bestämmelser som tas fram inom informationssäkerhetsområdet bör vara generiska och teknikoberoende för att inte snabbt bli inaktuella.

Informationssäkerhet har kopplingar till ett stort antal rättsområden bland annat offentlig förvaltning, redovisning, arkivering, personuppgiftsbehandling, skydd av rikets säkerhet, skydd mot terrorism, elektroniska kommunikationer och krisberedskap.

I Infosäkutredningen (delbetänkandet Säker information SOU 2005:42, sidan 229) framhålls att det är nödvändigt med författningsändringar (se bilaga 2). Det behövs ett utvidgat, mer sammanhållet och heltäckande regelverk som motsvarar den bredare definition av begreppet informationssäkerhet som presenteras i utredningen. I likhet med utredarens uppfattning anser KBM att regeringen bör tillsätta en utredning som gör den omfattande och genomgående analys som krävs för att kunna genomföra en sådan lagöversyn.

Det finns för närvarande ingen myndighet som har bemyndigande att utfärda föreskrifter och rekommendationer för informationssäkerhet på en övergripande och strategisk nivå. I Infosäkutredningen, (SOU 2005:42, s 33 ff.), föreslogs att regeringen skulle utse en myndighet med rätt att meddela föreskrifter om administrativa och tekniska åtgärder för att uppfylla grundläggande och särskilda krav på informationssäkerhet för statliga myndigheter. I regeringens proposition, Stärkt krisberedskap – för säkerhets skull (prop. 2007/08:92) framkommer det att regeringen avser att ge MSB rätten att utfärda generella föreskrifter.

När det specifikt gäller säkerhetsskyddslagstiftningen och säkerhetsskyddsförordningen kan följande behov av uppdatering identifieras. Den nuvarande lagstiftningens starka koppling till sekretesslagen och inriktning på begreppet rikets säkerhet medför att vissa rättssubjekt endast i viss utsträckning omfattas av säkerhetsskyddslagstiftningen och att säkerhetsskydd för skydd mot terrorism är begränsat. En annan fråga som har uppmärksammats vid tillämpningen av säkerhetsskyddslagstiftningen är den föråldrade beskrivningen av vad som är skyddsvärt i ett modernt samhälle. Det har visat sig att många skyddsvärda verksamheter utformar sitt säkerhetsskydd och informationssäkerhetsskydd utifrån termer av beredskapsplanering och uppfyller därmed inte kraven på rimligt säkerhetsskydd. Lagstiftningen bör ha en enkel struktur och en modern syn på sårbarhet och vad som är skyddsvärt i samhället. Bestämmelserna skall tillförsäkra ett gott säkerhetsskydd och informationssäkerhetsskydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda.

4.2 Åtgärdsförslag

Målsättningar författningsfrågor

- *Den svenska lagstiftningen ska vara harmoniserad med utvecklingen inom IT och informationssäkerhet*
- *En myndighet ska ha föreskriftsrätt gällande grundläggande och särskilda krav på statliga myndigheters administrativa och tekniska informationssäkerhet*

Åtgärdsförslag 4: Översyn av lagstiftningen på informationssäkerhetsområdet
Regeringen bör tillsätta en utredning som gör en heltäckande analys av författningar som berör informationssäkerhetsområdet.

Kostnad: Förslaget medför medelstor kostnad
Tid: Bör påbörjas under år 2008
Ansvar: Statlig utredning (SOU)

Åtgärdsförslag 5: Föreskriftsrätt inom informationssäkerhetsområdet
Regeringen bör ge MSB rätt att utfärda föreskrifter och allmänna råd för att myndigheter ska kunna uppnå grundläggande och särskilda tilläggskrav på informationssäkerhet. Förslag till bemyndigande framgår av bilaga 2.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Under år 2009
Ansvar: Regeringen

5 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 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 deras kvalitets- och effektivitetskrav. Samtidigt kan informationssäkerhet inte betraktas som enbart en verksamhetsintern angelägenhet. Flöden av tjänster och produkter sker i flera led. Bristande informationssäkerhet kan få följdverkningar långt utanför den egna verksamhetens gränser. I slutänden handlar det om att skapa och upprätthålla ett förtroende för hela informationssamhället och dess tjänster. Förtroendeproblem som drabbar en verksamhet kan via branschen eller sektorn spridas till övriga delar av samhället.

Det är viktigt att poängtera att informationssäkerhet handlar om verksamhetens kvalitet. Att förbättra informationssäkerheten innebär inte enbart att tillmötesgå externa krav, utan 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.

För att uppnå god informationssäkerhet i särskilt skyddsvärda verksamheter (rikets säkerhet och skydd mot terrorism) finns det krav i säkerhetsskyddsförordningen (1996:633) på att dessa verksamheter skall genomföra en säkerhetsanalys för att tillskapa ett lämpligt säkerhetsskydd (informationssäkerhet, fysisk säkerhet och skydd mot insiders) för dessa skyddsvärda verksamheter. Dock finns det inget uttalat krav på med vilket intervall som säkerhetsanalyser skall genomföras. Det är viktigt med tanke på olika skyddsvärda verksamheters snabba utveckling att det i framtiden ställs krav på att säkerhetsanalysen genomförs på årlig basis.

5.1 Informationssäkerhetsansvar

5.1.1 Bakgrund

Som nämnts ovan bör informationssäkerhet betraktas som en kvalitetsaspekt. Att uppnå en erforderlig informationssäkerhetsnivå är därför en del i varje verksamhetsansvar och bör betraktas som en integrerad del i verksamhetens kvalitets- och säkerhetsarbete. Flera rapporter har emellertid pekat på att myndighetsledningarna ibland har svårigheter att hantera detta ansvar. Detta kan bero på att området är relativt nytt och att det fortfarande saknas tillräcklig kunskap. Det finns en tendens till att myndighetsledningarna betraktar informationssäkerhetsfrågorna som en angelägenhet som enbart berör IT-avdelningar.

Det bör ytterligare tydliggöras att informationssäkerhet ska integreras i verksamheternas kvalitets- och effektivitetskrav och vara en självklar del av verksamhetsansvaret. Teknikskiften, till exempel övergång från analog telefoni till IP-telefoni, eller andra omfattande investeringar bör föregås av kontinuitetsplaneringar,

risk- och sårbarhetsanalyser, och säkerhetsanalyser för att förstå vad förändringarna innebär för den egna verksamheten och för att få fram rätt kravspecifikationer.

Vissa av de problem som kan uppstå vid teknikskiften går att härleda till brister i kravställande och beställarkompetens. Det är därför av stor vikt att upphandlingen av ny teknik sker på ett professionellt sätt. Det måste därvid finnas tillräcklig kompetens för att kunna ställa relevanta säkerhetskrav.

Vidare är det viktigt att efter genomförandet regelbundet utföra tredjepartsgranskningar för att säkerställa att kraven upprätthålls. Eftersom övergång till ny teknik främst drivs av ekonomiska skäl är det rimligt att kräva att en del av de kostnadsreduktioner investeringarna leder till används till sådan granskning.

5.1.2 Åtgärdsförslag

Målsättningar informationssäkerhetsansvar

- *Det ska tydligt framgå att informationssäkerhet är en del av organisationers kvalitetskriterier. Organisationsledningar ska vara medvetna om att ansvaret för informationssäkerhet är en del i verksamhetsansvaret och säkra en tillräcklig kompetensnivå i den egna organisationen.*
- *Organisationer ska ha kontroll på vilka risker som föreligger för den egna verksamheten och ha vidtagit åtgärder för att möta dessa risker.*
- *För särskilt skyddsvärda verksamheter, som lyder under säkerhetsskyddsförordningen (1996:633), bör det ställas krav på årliga säkerhetsanalyser. Dessa säkerhetsanalyser bör särskilt fokuseras på informationssäkerhetsaspekter.*

Åtgärdsförslag 6: Myndighetsledningars formella ansvarstagande för hantering av informationssäkerhetsrisker
Regeringen bör besluta att det ställs krav på myndigheter att i sin årsredovisning redovisa på vilket sätt gällande krav på informationssäkerhet uppfylls.

Kostnad: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: Samtliga myndigheter

Åtgärdsförslag 7: Förtydligande av informationssäkerhet i vägledningar för risk- och sårbarhetsanalyser
Information och rekommendationer för risk- och sårbarhetsanalyser gällande informationssäkerhet bör förtydligas i vägledningar som grundas på lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och vid höjd beredskap och på förordningen (2006:942) om krisberedskap och höjd beredskap som reglerar myndigheters risk- och sårbarhetsanalyser. Uppgiften bör läggas på MSB eftersom detta är en uppgift som för närvarande ligger på KBM.

Kostnad: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: MSB

Åtgärdsförslag 8: Rekommendationer för kravställning vid upphandlingar
Det bör tas fram information och rekommendationer om hur informationssäkerheten bör beaktas i samband med upphandlingar. Information och rekommendationer bör omfatta:

- Riskanalys
- Kontinuitetsplanering
- Kravställning vid upphandling
- Tredjepartsgranskning

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: FMV och Verva

Åtgärdsförslag 9: Informationsmaterial till myndighetsledningar
Det bör tas fram informationsmaterial till myndighetsledningar som ger en introduktion till informationssäkerhet och beskriver myndighetsledningars ansvar inom området.

Kostnad: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: MSB

5.2 Ledningssystem för informationssäkerhet

5.2.1 Bakgrund

Ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter. Den internationella standardserien ISO/IEC 27000 är ett sådant ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys, och där informationssäkerhetsarbetet följer en tydlig process. Tillämpning av standarderna i denna serie underlättar arbetet med informationssäkerhet inom organisationer och förbättrar också möjligheterna att externt bedöma säkerhet och revidera denna på ett enhetligt sätt.

Sedan den 1 januari 2008 gäller Vervas föreskrift för myndigheters tillämpning av informationssäkerhetsstandarder (VERVAFS 2007:2). Föreskriften innebär att tillämpning av standarderna ISO/IEC 27001 och 27002 är obligatoriska för statliga myndigheter. Föreskriften är begränsad till statliga myndigheter, men även andra verksamheter i samhället bör rekommenderas att tillämpa dessa standarder. På sikt bör ambitionen vara att även kommuner och landsting tillämpar dem, samt även näringsliv med samhällsviktig verksamhet.

Ett problem som ofta förs fram är att standarder är dyra och kan vara svåra att tillgodogöra sig. Speciellt kännbart är det för mindre organisationer och i utbildningssammanhang. Stödmaterial för arbete med dessa standarder bör därför tas fram och tillgängliggöras, vilket leder till ökad spridning och bättre genomslag.

Standardserien för ett ledningssystem för informationssäkerhet kan emellertid vara svår att förstå för den som inte är insatt i informationssäkerhet. Detta kan leda till kommunikationsproblem mellan verksamhetsledningar och informationssäkerhets-

ansvariga. För att få en bättre överblick av tillståndet i ett ledningssystem kan man skapa metoder för värdering och mätning. Dessa kan sedan användas vid självvärderingar eller vid interna och externa revisioner. Genom en distribuerad lösning kan metoderna användas för att konsolidera flera verksamheters tillstånd. Det kan också användas omvänt, för att jämföra enskilda verksamheters nivåer med andra verksamheter.

Verva motiverar sin föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte med att en organisationsintern informationssäkerhet är en förutsättning för ett säkert informationsutbyte mellan organisationer. Detta gäller också för vårdsektorn där kritisk information kommuniceras elektroniskt. Bland annat av detta skäl behöver den interna informationssäkerheten i verksamheter inom vårdsektorn styras upp på ett enhetligt sätt. I likhet med statliga myndigheter bör vårdsektorn därför tillämpa standarderna ISO/IEC 27001 och 27002. I vilken mån dessa standarder bör anpassas till vårdsektorn, alternativt kompletteras med riktlinjer för tillämpning inom vårdsektorn, bör ses över.

5.2.2 Åtgärdsförslag

Målsättningar ledningssystem för informationssäkerhet

- *Informationssäkerhetsarbete i verksamheter ska följa gällande standarder för ledningssystem på området.*
- *Aktörer och funktioner inom vårdsektorn ska ha en mycket god förmåga att klara allvarliga störningar och kriser.*

Åtgärdsförslag 10: Rekommendationer för tillämpning av standarderna ISO/IEC 27001 och 27002
Det bör utfärdas rekommendationer för de verksamheter som inte omfattas av Vervas föreskrift om att de ska tillämpa standarderna ISO/IEC 27001 och 27002.

Kostnad: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: Verva

Åtgärdsförslag 11: Stödmaterial för införande av ledningssystem för informationssäkerhet
Det bör tas fram utförligt material som stödjer tillämpningen av standarderna ISO/IEC 27001 och 27002. Redan befintligt material kan fungera som utgångspunkt och anpassats till standarderna ISO/IEC 27001 och 27002.

Finansiering: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: Återstår att klarlägga

Åtgärdsförslag 12: Utveckling och införande av ett värderingssystem för informationssäkerhet
Det bör tas fram och införas ett system för värdering av myndigheters informationssäkerhet. Systemet ska underlätta självvärdering samt vid intern och extern revision hur ställda krav på myndigheters informationssäkerhet uppfylls.

Finansiering: Förslaget medför låg kostnad
Tid: Under år 2009
Ansvar: MSB i samverkan med berörda myndigheter

5.3 Ramverk för statens informationssäkerhet

5.3.1 Bakgrund

Informationssäkerhetsåtgärder som införs eller planeras inom statlig verksamhet behöver sättas in i ett gemensamt ramverk. Säkerhetskraven på verksamheter varierar beroende på vilka informationstillgångar de förfogar över och de dimensionerande hot som föreligger. För att nå ett adekvat skydd av informationstillgångar och tjänster måste åtgärder väljas så att det finns en balans mellan kostnaderna för åtgärderna och de konsekvenser som incidenter kan leda till. Att finna balansen mellan kostnader för skydd och kostnader som uppstår vid incidenter är en mycket central del av informationssäkerhetsarbetet.

Standarderna i ISO/IEC 27000-serien innehåller ingen metod eller modell för klassificering av informationstillgångar, vilket är en viktig förutsättning för att på ett likartat sätt kunna värdera behovet av informationssäkerhet i verksamheter. Här finns i Sverige och på andra håll i världen goda förebilder för hur en sådan klassning kan ske. Exempelvis finns i USA en modell baserad på den federala standarden, Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199), och ett antal kompletterande publikationer inom ramen för det federala arbetet med att införa regelverket Federal Information Security Management Act (FISMA). En generell klassningsmodell för information har även tagits fram av KBM, inom ramen för analysverktyget BITS Plus (basnivå för informationssäkerhet).

Det arbete som beskrivs ovan är långsiktigt. En stor del av det bör i högre grad än hittills samordnas och struktureras inom staten. Detta för att minska statens utgifter, undvika att arbete dubbleras samt samordna och utnyttja expertisen på bästa möjliga sätt.

Ett ramverk som möjliggör en sådan samordning av informationssäkerhetsarbetet kan bestå av en standardmodell för hur information och informationssystem klassificeras. Klassificeringen av tillgångar baseras dels på vilka typer av skydd som är nödvändiga (konfidentialitet, riktighet och tillgänglighet), dels på hur allvarliga konsekvenserna blir i händelse av en incident.

För respektive informationsklass enligt ovan, kan råd, anvisningar och föreskrifter ges för skyddsåtgärder baserade på standarder (LIS, Common Criteria med flera). Dessa kan kompletteras med anpassade anvisningar för särskilda sektorer, till exempel finanssektorn, vårdsektorn och energisektorn. Verksamheter kan därvid nivåbestämma sitt säkerhetsarbete genom att:

- Identifiera och definiera sina informationstillgångar och system.
- Klassificera dessa i enlighet med ovan nämnda standard.
- Tillämpa skyddsåtgärder för varje klass utifrån exempelvis råd, anvisningar eller föreskrifter

Vid tillämpning av ramverket i en specifik verksamhet kan anpassningar göras. Genom utveckling av ett sådant ramverk kan samhällets resurser samordnas och ett ”lärande system” skapas där erfarenheter från en verksamhet kan samlas och leda till förbättringar som kommer andra till del.

5.3.2 Åtgärdsförslag

Målsättningar ramverk för statens informationssäkerhet

- *Det bör finnas ett för staten ett gemensamt ramverk för klassificering av informationstillgångar.*

Åtgärdsförslag 13: Gemensam modell för klassificering av informationstillgångar
Det bör utvecklas fram en gemensam modell för klassificering av informationstillgångar. Till modellen ska en metod utvecklas som stödjer identifiering, värdering och klassificering av informationstillgångar. Metoden kan användas som vägledning till verksamheter för klassificering av informationstillgångar, och kan därigenom fungera som ett stöd vid prioritering och beslut om skyddsåtgärder.

Finansiering: Förslaget medför medelstor kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB i samverkan med berörda myndigheter

5.4 Grundläggande säkerhetsnivå för informationssäkerhet

5.4.1 Bakgrund

Som ett led i att åstadkomma en robust informationsinfrastruktur i samhället behöver en gemensam lägsta informationssäkerhetsnivå fastställas. En sådan grundläggande nivå för informationssäkerhet ska inte ta hänsyn till den specifika hotbilden för en verksamhet, utan svara mot den generella hotbilden i form av till exempel skadlig kod, intrång och interna hot. För att på sikt uppnå ett gemensamt förtroende för samhällets informationssäkerhet måste tillämpningen av ledningssystem för informationssäkerhet kompletteras med en grundläggande säkerhetsnivå. Denna ska så tydligt som möjligt anpassas till standarderna ISO/IEC 27001 och 27002 och tillsammans med dessa erbjuda ett samlat ramverk för styrning av informationssäkerhet.

Staten bör i detta sammanhang vara ett föredöme för övriga samhället. Alla statliga myndigheter ska som minst nå upp till den grundläggande säkerhetsnivån. Föreskrifter ska därför utfärdas som utgör krav för myndigheter under regeringen. Övriga organisationer i samhället ska rekommenderas att som minst uppnå den grundläggande säkerhetsnivån för informationssäkerhet. För kommuner, landsting och näringsliv ska föreskrifterna utgöra rekommendationer som måste uppfyllas för att elektroniskt kunna

kommunicera och utbyta information med de statliga myndigheter vilka har att följa föreskrifterna.

Eftersom föreskrifterna och rekommendationerna handlar om en definierad grundläggande säkerhetsnivå måste denna uppdateras kontinuerligt för att kunna svara mot den snabba utvecklingen inom informationssäkerhetsområdet.

5.4.2 Åtgärdsförslag

Målsättningar grundläggande säkerhetsnivå för informationssäkerhet

- *Varje organisation har en grundläggande informationssäkerhet som möter den generella hotbilden mot verksamhetens informationstillgångar.*

Åtgärdsförslag 14: En grundläggande säkerhetsnivå för informationssäkerhet i samhället
Det bör definieras en grundläggande säkerhetsnivå för informationssäkerhet i samhället. Den ska tillämpas utifrån den modell för klassificering av informationstillgångar som anges i återgärdsförslag 13 och bör kopplas till standarderna ISO/IEC 27001 och ISO/IEC 27002. Under övergångstiden till en beslutad grundläggande säkerhetsnivå är det lämpligt att följa den basnivå för informationssäkerhet (BITS) som finns framtagen.

Kostnad: Förslaget medför medelstor kostnad
Tid: Bör påbörjas under år 2008
Ansvar: KBM i samverkan med berörda myndigheter

Åtgärdsförslag 15: Rekommendationer för grundläggande säkerhetsnivå
MSB i samverkan med berörda myndigheter bör ta fram rekommendationer för kommuner, landsting och näringsliv, baserade på den grundläggande informations-säkerheten som gäller för myndigheter.

Kostnad: Förslaget är kostnadsneutralt
Tid: Bör påbörjas under år 2009
Ansvar: MSB i samverkan med berörda myndigheter

6 Kompetensförsörjning

Kunskaper om riskerna med hantering av IT och Internet måste tillföras tidigt och vara en integrerad och naturlig del av den första IT-användningen. Därefter ska den 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. Ett flertal undersökningar visar att en majoritet av incidentkostnaderna kan härledas till brister i medvetenhet och kompetens hos ledning, användare och IT-personal. I verksamheter behövs olika typer av kunskap i en mängd olika roller. Det är människor som utvecklar, installerar, konfigurerar och använder tekniska system. Det är människor som formulerar, kommunicerar och efterföljer administrativa system. En särskild viktig grupp ur ett informationssäkerhetsperspektiv är organisationsledningar, eftersom det är dessa som i slutändan ansvarar för verksamhetens kvalitet och säkerhet och beslutar om skyddsåtgärder.

Ett så mångfacetterat område som informationssäkerhet behöver studeras djupare. Det kan ske genom forskning. En nationell satsning på forskning och forskarutbildning 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.

6.1 Kunskapscentrum för informationssäkerhet

6.1.1 Bakgrund

Det finns behov av att etablera ett nationellt kunskapscentrum för informationssäkerhet med nationella och internationella experter. Centrumet kan utgöra ett expertstöd, en tankesmedja och en gemensam mötesplats för såväl akademiker som praktiker inom informationssäkerhetsområdet.

Ett nationellt kunskapscentrum för informationssäkerhet innebär ett tydligare gränssnitt till det omgivande samhället och kan exempelvis underlätta rekrytering av lärare, studenter och forskare. Ett samlat kunskapscentrum kan dessutom leda till synergieffekter och en kritisk massa av studenter, lärare, praktiker och forskare med exempelvis en ökad nyetablering av företag som följd. Kunskapscentrumet skulle kunna upprätta stipendier till akademiker och eller praktiker inom informationssäkerhet för att stimulera kvalificerad kunskapsutveckling.

6.1.2 Åtgärdsförslag

Målsättningar kunskapscentrum

- *Skapa förutsättningar för att samla och koordinera den kvalificerade kunskapsutvecklingen inom informationssäkerhet*

Åtgärdsförslag 16: Nationellt kunskapscentrum för informationssäkerhet
Regeringen bör ge i uppdrag till MSB att närmare utreda hur ett nationellt kunskapscenter för informationssäkerhet kan upprättas. Syftet med kunskapscentret ska vara att öka och samordna kvalificerad kunskapsutveckling, samt utgöra ett expertcentrum inom området. Kunskapscentret kan organiseras i form av en stiftelse med en styrgrupp inkluderande intressenter från såväl staten, näringslivet som akademin. Centrumet kan delfinansieras genom statliga anslag.

Kostnad: Förslaget medför låg kostnad
Tid: Under år 2009
Ansvar: MSB i samverkan med näringslivet och universitet och högskolor

6.2 Informationssäkerhetsmedvetande i samhället

6.2.1 Bakgrund

Idag använder de flesta medborgarna IT i hemmet. Utvecklingen av e-tjänster i samhället innebär att vi använder Internet till en rad olika tjänster såsom banktjänster, inköp, resebeställningar och liknande. Utbyggnaden av e-förvaltningen innebär att en mängd samhällstjänster kommer att kunna utföras hemifrån via datorn, exempel inom utbildning och omvårdnad. Samtidigt ökar riskerna för att bli utsatt för skadlig kod och IT-relaterad brottslighet. Denna utveckling ställer höga krav på säkerhetsmedvetandet i samhället. Den offentliga sektorn bör här ta ansvar genom att informera och utbilda i säkerhetsfrågor.

Det är viktigt att kompetens- och medvetandehöjande åtgärder inte begränsas till individer inom utbildningsväsendet och yrkeslivet. Tekniskpridningen innebär att åtgärder måste riktas även till dem som inte nås via skolan eller arbetsplatsen. Som exempel kan kampanjen *Surfa lugnt* nämnas. Kampanjen riktar sig till hemanvändare, småföretagare och ungdomar (inklusive föräldrar och pedagoger). Kampanjen spelar därför en viktig roll i strävan mot ett ökat informationssäkerhetsmedvetande i det svenska samhället. Kampanjen arbetar också med folkbildningen i Sverige som har en viktig roll i sammanhanget.

6.2.2 Åtgärdsförslag

Målsättningar informationssäkerhetsmedvetande i samhället

- *Alla medborgare som använder IT ska ges möjlighet att bli förtrogna med de hot, risker, sårbarheter som är förknippade med IT samt att förstå hur man bör skydda sig och vart man kan vända sig för rådgivning.*

Åtgärdsförslag 17: Utökning av kampanjen Surfa lugnt
Den medvetandehöjande kampanjen Surfa lugnt bör utvecklas och få ökat stöd för att denna ska kunna intensifiera och bredda sin verksamhet.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: 2009-2012
Ansvar: Berörda myndigheter

Åtgärdsförslag 18: Stimulera folkbildning inom informationssäkerhet
Berörda myndigheter bör ytterligare utveckla konkreta förslag om hur folkbildningsverksamheten inom informationssäkerhet kan stimuleras och få ett ökat utbud och tillgänglighet av utbildningar (kurser, cirkelverksamhet, fortbildning av lärare m.m.) som ett led att höja säkerhetsmedvetandet på bred front i samhället.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Berörda myndigheter

6.3 Grundskola och gymnasium

6.3.1 Bakgrund

Informationssäkerhet bör finnas med från ett tidigt skede i grundskolan och genom hela skolgången. Utbildning av elever på grundskola och gymnasium kräver kompetens hos lärarna. Därför bör lärare på olika nivåer erbjudas fortbildning inom informationssäkerhet. Av speciell betydelse är etikfrågor i anslutning till användning av IT och Internet. Etikfrågor kan ses som en viktig aspekt av informationssäkerhet.

6.3.2 Åtgärdsförslag

Målsättningar grundskola och gymnasium

- *Utbildning i informationssäkerhet och IT-etik ska finnas med under hela skoltiden med start från lågstadiet.*
- *Informationssäkerhet och IT-etik ska finnas med på ett integrerat sätt i samtliga utbildningar där IT används eller som leder till yrkesroller där informationshantering är en viktig del.*

Åtgärdsförslag 19: Rekommendationer till grundskola och gymnasium
Framtagande av rekommendationer till grundskola och gymnasium avseende hur informationssäkerhet och IT-etik bör integreras i olika typer av utbildningar.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Återstår att klarlägga

6.4 Universitet och högskolor

6.4.1 Bakgrund

Inom universitet och högskolor finns för närvarande en mängd utbildningar inom informationssäkerhet. Universitet och högskolor avgör själva detta utbud baserat på efterfrågan på utbildning och tillgång till lärarkompetens. Två sätt att stärka lärarkompetensen är att 1) staten erbjuder fortbildning av lärare inom informationssäkerhet och 2) det sker en ökad satsning på forskarutbildning inom informationssäkerhet.

Förutom specifika kurser inom informationssäkerhet är det av vikt att informationssäkerhetsaspekter finns med i utbildningar där IT ingår eller som leder till yrkesroller med hög grad av informationshantering, till exempel för utbildningsprogram för ingenjörer och systemvetare, medicinska informatiker, samhällsvetare, jurister och ekonomer.

6.4.2 Åtgärdsförslag

Målsättningar universitet och högskolor

- *Informationssäkerhet ska finnas med på ett integrerat sätt i samtliga utbildningar där IT används eller som leder till yrkesroller där informationshantering är en viktig del.*

Åtgärdsförslag 20: Rekommendationer till högskolor och universitet
Framtagande av rekommendationer till högskolor och universitet avseende hur informationssäkerhet bör integreras i olika typer av utbildningar.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2010
Ansvar: Återstår att klarlägga

6.5 Yrkesverksamma

6.5.1 Bakgrund

Eftersom IT och informationshantering är en integrerad del av en mängd olika arbetsuppgifter ställs det krav på IT-kompetens för åtskilliga roller i en organisation. Kunskaperna om informationssäkerhet får inte vara avgränsade till organisationens IT-avdelning utan grundregeln är att kompetens måste gå hand i hand med arbetsuppgift och ansvar. Informationssäkerhetsansvaret återfinns på flera nivåer i en organisation: från ledningen och mellanchefer till den enskilda medarbetaren som ansvarar för sina egna arbetsuppgifter. Det behövs också djupare och specifik kunskap för dem som konkret arbetar med informationssäkerhet. I likhet med andra yrkesgrupper, till exempel jurister och ekonomer, tillhör de professionella inom informationssäkerhets-området en specifik yrkesgrupp, ett skrå, på vilka det ställs höga kompetenskrav. Utvecklingen av yrkesorienterade certifieringar inom området bör därför främjas för att stärka yrkesområdets status och underlätta kompetensbedömningar, till exempel i samband med rekryteringar och tjänsteupphandlingar. Till yrkesverksamma räknas också lärare på olika nivåer i utbildningssystemet.

6.5.2 Åtgärdsförslag

Målsättningar yrkesverksamma

- *Yrkesverksamma ska ha kunskaper inom informationssäkerhet som motsvarar deras arbetsuppgifter och ansvar.*

Åtgärdsförslag 21: Identifiering av kompetensbehov hos yrkesverksamma
Det bör identifieras kunskapsbehov hos särskilda kategorier av yrkesverksamma och tas fram kravspecifikationer för utbildningar. Exempel på kategorier kan vara:

- Grundskolelärare
- Gymnasielärare
- Lärare inom folkbildning
- Högskolelärare (i flera olika ämnen)
- Verksamhetsledningar i offentlig sektor
- Professionella inom informationssäkerhet
- Beställare och projektledare

Kostnad: Förslaget är kostnadsneutralt
Tid: Under år 2009
Ansvar: Berörda myndigheter

Åtgärdsförslag 22: Utbildningar i informationssäkerhet
Det bör initieras utbildningar och tas fram utbildningsmaterial inom informationssäkerhet utifrån kravspecifikationerna i åtgärdsförslag 21. Utbildningar, med eventuellt tillhörande certifieringar, bör särskilt beakta nya kunskapsbehov som uppkommer till följd av föreskrifter och rekommendationer i åtgärdsförslag 5 och 10.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2010
Ansvar: Berörda myndigheter i samverkan med näringsliv och utbildningsväsendet

6.6 Forskning

6.6.1 Bakgrund

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 och kriminologiska aspekter är exempel på andra områden som behöver studeras inom informationssäkerhet 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.

6.6.2 Åtgärdsförslag

Målsättningar forskning

- *Det finns en nationell strategi för forskning inom informationssäkerhet som är förankrad i samhället*
- *Det finns forskning och forskarutbildning inom informationssäkerhet som tillgodoser samhällets behov*
- *Samverkan mellan forskningsaktörer och mellan akademin och övriga samhället är god*
- *Svensk forskning har en god internationell samverkan*

Åtgärdsförslag 23: Nationell forskningsstrategi
Det bör utformas en långsiktig nationell forskningsstrategi dels för att i högre grad styra forskningen mot samhälleliga behov och dels för att öka forskningssamverkan nationellt och internationellt. Se även åtgärdsförslag 16.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB i samverkan med berörda myndigheter och på sikt även i samverkan med det nya kunskapscentrumet

Åtgärdsförslag 24: Koordinering av forskningsmedel
Baserat på forskningsstrategin bör MSB i samverkan med berörda myndigheter koordinera forskningsmedel inom informationssäkerhet. Koordineringen bör ske i samverkan med statliga myndigheter och organ inom EU.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2010
Ansvar: MSB i samverkan med berörda myndigheter

Åtgärdsförslag 25: Inrättande av forskarskola
Det bör upprättas en nationell forskarskola i informationssäkerhet med syfte att få fram djupare kunskap inom området. Ytterligare ett syfte med forskarskolan är att stimulera samverkan inom forskarsamhället och mellan detta och det omgivande samhället. Forskarskolan bör ha en tvärvetenskaplig prägel och arrangeras av flera lärosäten. Exempelvis kan ämnen som företagsekonomi, juridik och sociologi förekomma vid sidan av ämnen där informationssäkerhet traditionellt studeras. En forskarskola innebär en skola för doktorander som delvis har gemensam kursplan men individuella avhandlingsprojekt.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2010
Ansvar: Berörda universitet eller högskolor

7 Informationsdelning, samverkan och respons

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

Som ett led i att öka samverkan i samhället föreslås åtgärder för att stimulera nationella nätverk inom informationssäkerhet samt privat-/offentlig samverkan. Det senare är mycket betydelsefullt eftersom en hel del av den svenska kritiska informations-infrastrukturen återfinns i privat ägo och ett förbättrat erfarenhetsutbyte kommer såväl stat och offentlig sektor som näringsliv till godo. En global värld med gränslösa hotbilder kräver naturligtvis även internationell samverkan. Sverige bör aktivt medverka i internationella samarbeten på flera plan: inom EU, med de nordiska länderna och med enskilda stater.

7.1 Operativ nationell samordningsfunktion

7.1.1 Bakgrund

Det behöver formaliseras hur information om hot, sårbarheter och incidenter rapporteras, tas om hand, förs vidare och hur informationen kan leda till förbättringsåtgärder. Den nuvarande underrättelse- och säkerhetstjänsten bör därför kompletteras med en utökad informationsdelning och en förbättrad operativ förmåga att genom samverkan agera mot hot och inträffade incidenter på nationell nivå. Detta innebär att arbetet inte kan avgränsas till staten utan måste även inbegripa näringsliv och andra organisationer. Exempelvis kan näringslivet förmedla viktig information till staten och vice versa.

Det behövs en administrativ och teknisk infrastruktur för informationsdelning och respons i vid mening inom informationssäkerhet i det svenska samhället, där samtliga aktörer av betydelse för samhällets kritiska informationsinfrastruktur finns representerade. Infrastrukturen ska fungera under normala förhållanden men också innefatta en krisledningsorganisation som kan fungera som stöd under allvarliga störningar och kriser. En sådan organisation och infrastruktur måste därför självfallet ha en hög grad av robusthet för att inte slås ut vid allvarliga störningar. För att nå kostnadseffektivitet och att på bästa sätt ta till vara befintlig kompetens och organisation bör infrastrukturen bygga på nuvarande struktur. En övergång från normalläge till krisläge ska inte innebära stora förändringar i aktörer och arbetssätt som försvårar och fördröjer arbetet i en redan pressad situation. Utgångspunkten bör därför vara att utgå från och ta tillvara nuvarande verksamhet, såsom CERT-verksamheten hos Sitic och befintlig underrättelseverksamhet inom polisen, säkerhetspolisen, försvarsmakten och FRA. En samverkansgrupp bör bildas med representation från dessa

aktörer samt den myndighet som har det sammanhållande sektorsövergripande och tvärsektoriella inriktningsansvaret för samhällets informationssäkerhet.

Som framkommit i Kapitel 6 finns det i dagsläget ett underskott i samhället på kompetens inom informationssäkerhet. Denna kompetensbrist kan medföra allvarliga svårigheter i samband med kriser i samhället. Större IT-attacker mot samhällsviktiga verksamheter kan innebära att kvalificerad kompetens behöver flyttas till de mest utsatta sektorerna. En sådan omflyttning kan vara mycket svår att organisera när ett skarpt läge föreligger, både av praktiska och juridiska skäl. En beredskap för en sådan situation kräver därför förberedelser i form av en samövad IT-beredskapsorganisation, där kompetensmässiga och juridiska spörsmål är klargjorda. Samverkan mellan staten och det övriga samhället är centralt när det handlar om IT-beredskap.

7.1.2 Åtgärdsförslag

Målsättningar operativ nationell samverkansfunktion

- *Det ska finnas en effektiv informationsdelning inom informationssäkerhet i samhället i stort, i syfte att berörda parter ska kunna nå en samlad kunskapsnivå och lägesbedömning och nå en operativ förmåga att kunna kommunicera och agera i samband med incidenter och kriser.*
- *Kompetent och övad personal ska finnas tillgänglig i händelse av kris.*

Åtgärdsförslag 26: Operativ nationell samordning
Regeringen bör ge KBM och berörda myndigheter i uppdrag att lämna underlag till regeringen om hur man kan skapa en administrativ och teknisk infrastruktur för informationsdelning och respons inom informationssäkerhet för hela samhället. Förslaget bör omfatta gemensam kunskapsdelning, gemensam lägesbildsfunktion och operativ förmåga vid omfattande IT-incidenter. Verksamheten ska fungera under såväl normala förhållanden som vid en kris.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2008
Ansvar: KBM i samverkan med berörda myndigheter och näringsliv

Åtgärdsförslag 27: Upprättande av en IT-beredskapsorganisation
Det bör tas fram ett förslag till en IT-beredskapsorganisation som ska kunna användas i händelse av allvarliga störningar i den svenska informationsinfrastrukturen. Viktiga delar i detta arbete är att identifiera relevant kompetens, skapa nätverk, utforma avtal och se över gällande bestämmelser.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB i samverkan med berörda myndigheter

Åtgärdsförslag 28: Obligatorisk incidentrapportering
Regeringen bör införa krav på att statliga myndigheter ska rapportera inträffade informationsrelaterade incidenter, utom för den typen av incidenter som är undantagna genom lagstiftning. Krav på omedelbar rapportering ska gälla större incidenter som gett eller kunnat ge allvarliga konsekvenser. Se även åtgärdsförslag 26.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2010
Ansvar: Samtliga myndigheter

7.2 Bekämpning av IT-relaterad brottslighet

7.2.1 Bakgrund

Den traditionella brottsligheten som bedrägeri, utpressning, förtal och sabotage finns idag även på Internet. Det är också enkelt att snabbt få tillgång till erforderlig information och verktyg för att begå kriminella handlingar på Internet. I jämförelse med den fysiska världen kan tröskeln till att begå brott på Internet vara lägre, och därmed riskerar brottsligheten att sprida sig till traditionellt icke-kriminella grupper.

Denna trend hotar IT-utvecklingen i landet i stort. IT-kriminaliteten utgör ett av de största hoten mot att myndigheternas e-tjänster utvecklas vidare och att fler medborgare utnyttjar dem. Det är svårt att bedöma omfattningen idag och än svårare hur framtiden ser ut. Ett problem med att bedöma IT-kriminalitetens konsekvenser för samhället är det stora mörkertalet. Företag och organisationer drar sig fortfarande för att anmäla brott i rädsla för att skada sitt eget rykte. Därmed är det ytterst svårt att veta omfattningen av de olika typer av IT-brott som kan påverka samhället.

Bekämpning av IT-brott är därtill resurskrävande. För att hålla jämna steg med de kriminella krävs kunskap och personal. Materialet i beslagtagna datorer är en stor källa till information i förundersökningar, men det krävs stora resurser för att bearbeta data. En ökad användning av kryptering och antiforensiska metoder gör utredningsarbetet allt svårare och mer tidskrävande. Resurserna för att bekämpa IT-brottsligheten bör därför ökas kraftigt för att bromsa den negativa utvecklingen och för att inte samhällets satsningar på Sverige som en framgångsrik IT-nation ska äventyras.

Under normalförhållanden behöver den polisiära verksamheten dessutom delta i samverkande förberedelser och planering med andra aktörer i samhället för att vara förberedd för krissituationer eller höjd beredskap (som beskrivs i avsnitt 6.1). Rikskriminalpolisen (RKP) och Säkerhetspolisen (Säpo) startade 2004 en funktion – S-BIT – avseende samordning av IT-relaterade brott och incidenter. Denna funktion har inte de resurser som krävs i en situation där resursläget redan är ansträngt och tid saknas för utbildning och omorganisation av befintlig verksamhet. Det långsiktiga, brottsförebyggande arbetet i normalverksamheten behöver omriktas, förstärkas och förberedas för hastigt uppkommande situationer i samband med kris eller höjd beredskap.

7.2.2 Åtgärdsförslag

Målsättningar Bekämpning av IT-relaterad brottslighet

- *Det ska finnas en effektiv bekämpning av IT-relaterad brottslighet*
- *Polisen ska aktivt delta i samverkansarbetet inför allvarliga IT-relaterade störningar och kriser*

Åtgärdsförslag 29: Utveckling av förmågan att förebygga och bekämpa IT-relaterad brottslighet
Regeringen bör besluta att tilldela Rikspolisstyrelsen särskilda medel för att utveckla förmågan att förebygga och bekämpa IT-relaterad brottslighet.

Kostnad: Förslaget medför medelstor till hög kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Regeringen

Åtgärdsförslag 30: Polisiärt deltagande i samverkan inför krissituationer
Det bör tilldelas ökade resurser så att Rikspolisstyrelsens funktion för samordning av IT-relaterade brott och incidenter (S-BIT) har möjlighet att aktivt bidra i samverkan med andra samhällsaktörer inför allvarliga störningar och kriser.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Rikspolisstyrelsen

Åtgärdsförslag 31: Informationsdelning kring IT-relaterade brott
Polisen bör, genom Rikskriminalpolisen och Säkerhetspolisen, vara en aktör i informationsdelningen kring IT-relaterade brott mellan berörda myndigheter.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Rikspolisstyrelsen i samverkan med berörda myndigheter

7.3 Nationell samverkan

7.3.1 Bakgrund

Nationell samverkan är viktig, inte minst på grund av statens organisation av informationssäkerhetsarbetet och områdets tvärsektoriella karaktär. Viktigt arbete sker idag isolerat inom respektive sektor eller bransch. Området innefattar emellertid många generella problemställningar varför ökat erfarenhetsutbyte bör eftersträvas.

En stor del av arbetet med informationssäkerhet i Sverige sker i nätverksform. Dessa nätverk är ibland övergripande eller har en viss profil, exempelvis i form av koppling till en viss sektor eller bransch, ett forskningsområde eller någon speciell aspekt av informationssäkerhet. Gemensamt för nätverken är att de är viktiga kunskaps-generatorer och förmedlare inom området samt bidrar till utvecklingen av informationssäkerhet i samhället i stort. Staten bör bättre ta till vara denna kunskap.

Genom ett givande och tagande kan ett ömsesidigt lärande ske mellan nätverk och statlig verksamhet.

En stor del av Sveriges kritiska informationsinfrastruktur drivs i näringslivet regi. Där återfinns även en betydande del av kompetensen och de internationella kontakterna. Att stimulera privat-/offentlig samverkan inom informationssäkerhetsområdet innebär därför att öka ett ömsedigt lärande i samhället och öka förutsättningarna för en förbättring av samhällets informationssäkerhet i stort. Forum för privat-/offentlig samverkan bör vara informella, eftersom publiceringar och andra former av offentlighet kan äventyra deras integritet och förtroendet mellan aktörerna.

En beprövad samverkansform är konceptet FIDI (Forum för Informationsdelning avseende Informationssäkerhet). FIDI har lyckosamt använts av KBM inom SCADA-området under cirka tre års tid (FIDI-SC). FIDI-konceptet baseras på riktlinjer och erfarenheter från den brittiska myndigheten Centre for the Protection of National Infrastructure (CPNI). FIDI-konceptet innebär att myndigheter och industrin delar på information om risker och sårbarheter. Målet med samverkan är bland annat att skapa en mekanism där en enskild organisation kan ta lärdom av andras erfarenheter, misstag och framgångar för att höja sin egen säkerhetsnivå, vilket i förlängningen förmodas komma samhället till godo. Det ska kunna ske utan rädsla för att behöva exponera den egna organisationens blottor för till exempel konkurrenter eller media. Modellen baseras på ett antal begrepp vilka anses vara generella för privat-/offentlig samverkan:

- Förtroende
- Mervärde
- Strukturerade former för informationsutbyte
- Aktivt deltagande och engagemang
- Konkurrensneutralt
- Jämlikt deltagande
- Statlig drivkraft utan tillsyn och kontroll

Av dessa anses det personliga förtroendet mellan deltagarna vara den enskilt viktigaste framgångsfaktorn. Förtroende är ett tillstånd som infinner sig först efter en viss tid och förutsätter deltagarnas aktiva medverkan.

Informationsutbyte och samarbete mellan den offentliga sektorn och näringslivet bör utvecklas för att på ett kostnadseffektivt sätt bygga upp informationssäkerhets-kompetensen i samhället på bredden. Genom att använda erfarenheterna från FIDI-SC bör staten stimulera att FIDI-konceptet sprids till fler områden.

Finanssektorn har av tradition ett välutvecklat säkerhetstänkande och har generellt en hög informationssäkerhetsnivå. Den ökande brottsligheten på Internet i samband med ett utökat tjänsteutbud och en ökad internationalisering innebär dock en förändrad hotbild. Staten har ett naturligt intresse av att upprätthålla en ständigt fungerande bank- och finansmarknad. Eftersom en förändrad hotbild är ett branschgemensamt problem borde alla aktörer ha nytta av ett samarbete i säkerhetsfrågor, åtminstone till den del säkerheten gäller den gemensamma infrastrukturen. Därför kan det vara intressant både för branschen och för staten om en utökad samverkan, bland annat för att diskutera branschgemensamma säkerhetskrav.

7.3.2 Åtgärdsförslag

Målsättningar nationell samverkan

- *Staten ska ha en kontinuerlig samverkan med i landet existerande nätverk för informationssäkerhet.*
- *Det ska finnas en god privat-offentlig samverkan i de sektorer och tvärsektoriella områden där för samhället kritisk informationsinfrastruktur befinns i privat ägo.*
- *Att finanssektorn har ett fördjupat samarbete med staten i informationssäkerhetsfrågor, och tillämpar branschgemensamma säkerhetskrav som är framtagna i samverkan med staten.*

Åtgärdsförslag 32: Nätverkssamverkan
Berörda myndigheter bör utveckla samverkan med befintliga nätverk och intresse-organisationer inom informationssäkerhet.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2010
Ansvar: Berörda myndigheter

Åtgärdsförslag 33: Samverkan mellan offentlig och privat sektor
Staten bör stimulera och utveckla samarbetet mellan offentlig sektor och näringsliv avseende samhällsviktig verksamhet inom informationssäkerhetsområdet. Arbetet bör ske sektorsvis såväl som tvärsektoriellt.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Berörda myndigheter

Åtgärdsförslag 34: Upprättande av FIDI-Finans
KBM och finanssektorn bör tillsammans initiera ett privat-/offentligt samverkansforum i form av ett FIDI (Forum för Informationsdelning avseende Informationssäkerhet). Samverkan har bl a som syfte att diskutera former av branschgemensamma säkerhets-krav.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2008
Ansvar: KBM i samverkan med berörda myndigheter

7.4 Samverkan inom EU

7.4.1 Bakgrund

I arbetet med att förbättra det svenska samhällets informationssäkerhet är det självklart att förhålla sig till EU. Eftersom Sverige är medlem i EU utgör unionen en viktig arena främst 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 informationssäkerhetsarbete som ligger i linje med svenska intressen. För att

myndigheter ska kunna stödja det svenska agerandet krävs både sakkunskap och erfarenhet av hur EU:s politik utformas och införs.

Som liten nation måste Sverige välja inom vilka frågor och processer man aktivt ska försöka utöva inflytande och det är därför nödvändigt att prioritera bland ansträngningarna att påverka EU. Det är dessutom viktigt för en liten aktör att koordinera resurserna för att erhålla maximalt inflytande. Den svenska koordineringen och prioriteringen bör göras med utgångspunkt i en gemensam svensk ståndpunkt.

7.4.2 Åtgärdsförslag

Målsättningar samverkan inom EU

- *Stödja utformningen av EU:s informationssäkerhetspolitik i linje med Sveriges viljeinriktning inom informationssäkerhetsområdet.*

Åtgärdsförslag 35: Bevaka EU:s informationssäkerhetsarbete
Det bör utvecklas en formaliserad bevakning och uppföljning av EU:s informationssäkerhetsarbete för att upprätthålla aktuella kunskaper om hur området utvecklas och tillämpning sker.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under 2008
Ansvar: Berörda myndigheter

Åtgärdsförslag 36: Etablera ett forum för samverkan inom ramen för EPCIP
Regeringen bör ge MSB med stöd av PTS i uppdrag att inför Sveriges ordförandeskap i EU hösten 2009, utveckla ett EU-forum för sektorsövergripande samverkan inom informationssäkerhet och skydd av kritisk informationsinfrastruktur. Ett sådant forum bör utgå från det befintliga EPCIP-samarbetet (European Programme for Critical Infrastructure Protection).

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB med stöd av PTS

7.5 Övrig internationell samverkan

7.5.1 Bakgrund

Vid sidan av EU behövs självfallet internationell samverkan med en rad andra länder. Det är naturligt att Sverige har ett nära samarbete med våra nordiska grannländer. Här finns infrastrukturella kopplingar och samarbeten vilket exempelvis innebär att viss kritisk infrastruktur delas mellan de nordiska länderna. Även vissa andra länder betraktas som särskilt viktiga att samverka med.

Standardiseringsarbete i olika former är ett område där internationell samverkan är grundläggande. Här bedrivs från svensk sida aktiviteter på flera håll, och Sverige är mycket aktivt i det internationella standardiseringsarbetet inom informationssäkerhet. Sverige har även en framskjuten position inom andra internationella forum för

informationssäkerhet, exempelvis Meridian (Critical Information Infrastructure Protection – CIIP) och First (Cert-verksamhet) och inom Internetsäkerhet.

Grundprincipen är att internationell samverkan är av godo och inte kan utvecklas för mycket. Flera av de områden som berörs i handlingsplanen, såsom forskning, kompetensförsörjning, standardisering och lagstiftning, har mycket att vinna på en aktiv internationell samverkan som därför bör stimuleras ytterligare. Viss internationell samverkan kan göras av aktörer på eget initiativ medan annan samverkan kräver en nationell samordning, exempelvis där det är av vikt att Sverige tar en officiell ställning. När en samordning är nödvändig, och hur den ska gå till, är det viktigt att tydliggöra detta så att ingen osäkerhet råder för berörda aktörer.

7.5.2 Åtgärdsförslag

Målsättningar övrig internationell samverkan

- *Intensifiering av internationell samverkan inom informationssäkerhet.*
- *Tydlighet i vilka sammanhang Sverige behöver ha en nationell samordning för internationell samverkan.*

Åtgärdsförslag 37: Internationell samverkan
Sveriges nationella samordning för internationell samverkan bör tydliggöras. Sveriges medverkan i internationella sammanhang inom informationssäkerhetsområdet bör stimuleras och utvecklas.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB i samverkan med berörda myndigheter

8 Kommunikationssäkerhet

Den svenska marknaden för elektronisk kommunikation styrs av lagen (2003:389) om elektronisk kommunikation (LEK). Lagen utgör den svenska implementeringen av EU-direktiv vars främsta syfte är att bryta upp de nationella monopolen, skapa en konkurrensutsatt marknad med sänkta priser för köparna och lika villkor för operatörer inom hela EU-området. I inledningen av LEK framgår att lagen bland annat syftar till att enskilda och myndigheter ska få tillgång till säker och effektiv elektronisk kommunikation och största möjliga utbyte vad gäller urvalet av tjänster och kvalitet.

I LEK kapitel 5, § 6a står det att operatörer ska se till ”att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid.” PTS har 2007 utgivit ett allmänt råd (PTSFS 2007:2), som tillsammans med lagen lägger en grund för den nivå av robusthet som alla operatörer ska följa.

Staten arbetar genom PTS med flera metoder för att öka robustheten och säkerheten inom sektorn elektronisk kommunikation. Metoderna innefattar säkerhet och robusthet som konkurrensmedel, upphandling av robusthets- och säkerhetshöjande åtgärder, samarbete och partnerskap mellan staten och näringslivet samt författningsreglerad säkerhet inklusive förebyggande tillsyn. Dessa fyra metoder kompletterar varandra och är beroende av omständigheterna.

Det finns en strategi för ökad robusthet för sektorn elektronisk kommunikation (PTS-ER-2006:19). Strategin innehåller ett antal åtgärdsområden:

- Stimulans till ett ökat användaransvar inom elektroniska kommunikationer
- Ökad redundans och flexibilitet i nätverk
- Förbättrat skydd mot både fysiska och elektromagnetiska hot
- Ökad kunskap om informationssäkerhet
- Mer robust elförsörjning för de elektroniska kommunikationerna och fördjupat samarbete mellan el- och teleområdena
- Utveckla samverkan
- Fördjupat internationellt samarbete
- Förbättrad förmåga till krishantering inom elektroniska kommunikationer
- Ökad robusthet i näten

8.1 Internetsäkerhet

8.1.1 Bakgrund

Internets uppbyggnad är i grunden robust och har stora möjligheter att kunna fungera även under svåra förhållanden och vid störningar i de elektroniska kommunikationerna. Även om Internet i grunden är ett robust system för elektronisk kommunikation går det inte att en gång för alla lösa de säkerhetsproblem som finns på Internet. Därför är det angeläget att ha ett långsiktigt arbete för att följa, främja och, där det är lämpligt, påverka säkerhetsarbetet. Eftersom Internet även nyttjar infrastrukturen i de underliggande nivåerna, till exempel mobilmaster och transmissionsnät, beror den

fysiska robustheten delvis på det arbete som görs på dessa nivåer och som även ger effekt på den svenska delen av Internet.

Internet är ett världsomspännande logiskt nät som bildats genom att ett stort antal nät som ägs och förvaltas av olika privata och offentliga aktörer, fysiskt och logiskt länkats samman. Lägre nivåer i nätinfrastrukturens hierarki, till exempel fiber, koppar, radio och transmissionsutrustning som används för Internettrafik, utnyttjas i de flesta fall även för trafik för andra tillämpningar, exempelvis fast och mobil telefoni, virtuella privata nät samt diverse IP-baserade kvalitativa tjänster. På grund av att nät och nätutrustning som används för Internet delas med andra tjänster, som har garanterad tillgänglighet och kvalitet enligt avtal, är resurserna för överföring av Internettrafik från ändpunkt till ändpunkt varierande och med oförutsägbar tillgänglighet.

Regeringen har beslutat om en strategi för ökad säkerhet i Internets infrastruktur (N2006/5335/ITFoU). Strategin är inriktad mot infrastruktur som är unik för Internet. Strategin innehåller följande strategiska ställningstaganden:

- Internets fysiska infrastruktur bör skyddas mot olyckor, störningar, avlyssning och manipulation av information under överföring
- Motståndskraften mot störningar i domännamnssystemet bör öka
- Motståndskraften mot störningar i trafikutbyte mellan Internetoperatörer bör öka
- Användare och beställare bör utbildas och informeras för ökat säkerhetsmedvetande
- Ansvarstagandet för användares säkerhet bör öka hos Internetoperatörer samt tillhandahållare av program och utrustning
- Den nationella kunskapsutvecklingen avseende Internets infrastruktur bör främjas. Det bör ske i ett bredare sammanhang rörande informationssäkerhet
- Det svenska deltagandet i internationella forum bör fördjupas. Detta bör ske i samverkan mellan privat och offentlig sektor
- Förmågan att hantera kriser relaterade till Internets infrastruktur bör utvecklas

För närvarande finns en handlingsplan tillhörande regeringens strategi för ökad säkerhet i Internets infrastruktur (PTS-ER-2006:12). Åtgärderna i handlingsplanen behöver genomföras. Handlingsplanen förvaltas av Post- och telestyrelsen och myndigheten ansvarar för uppdatering i enlighet med den förvaltningsplan som finns i strategin.

8.1.2 Åtgärdsförslag

Målsättningar Internetsäkerhet

- *Kritiska funktioner i Internets infrastruktur ska vara robusta. Kritiska funktioner är sådana som om de inte upprätthålls ger omfattande störningar eller avbrott och på så sätt försvårar eller förhindrar användning av Internet för stora grupper av enskilda användare eller för samhällsviktiga företag, myndigheter och organisationer.*

Åtgärdsförslag 38: Genomföra åtgärder och utveckla handlingsplanen från Strategin för ökad säkerhet i Internets infrastruktur
Åtgärderna i handlingsplanen tillhörande regeringens strategi för ökad säkerhet i Internets infrastruktur (PTS-ER-2006:12) behöver genomföras av berörda aktörer. Ansvaret för åtgärderna i handlingsplanen ska ligga i linje med hur regeringen framöver väljer att organisera det statliga arbetet med informationssäkerhet.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Under 2008
Ansvar: PTS i samverkan med berörda myndigheter

8.2 Signalskydd

8.2.1 Bakgrund

Det finns i samhället ett behov av att skydda känslig information som hanteras i elektroniska kommunikationsnät från otillbörlig insyn, avtappning och förvanskning. Detta gäller då informationen bearbetas elektroniskt eller då den förmedlas via elektronisk kommunikation. Vilken information som med hänsyn till rikets säkerhet ska skyddas av nationellt godkända signalskyddssystem är reglerat i sekretesslagen (1980:100) i kombination med säkerhetsskyddslagen (1996:627), säkerhetsskydds-förordningen (1996:633) och RPS föreskrifter (RPSFS 2004:11 FAP 244-1).

Vid myndigheter och företag hanteras även information som omfattas av sekretess som inte rör rikets säkerhet. Denna information samt annan information som hanteras i samhället kan dock värderas som känslig eller skyddsvärd. Det är önskvärt att också sådan information erhåller tillräckligt skydd. Detta kan i många fall ske med hjälp av nationellt godkända kryptografiska funktioner, vilket innebär att obehörig insyn i, och påverkan av, information som hanteras i elektroniska kommunikationsnät förhindras. Kryptografiska funktioner används för att uppnå konfidentialitet, autenticitet och riktighet. För att kryptografiska funktioner ska uppnå avsedd skyddseffekt måste dessa också omgärdas med administrativa regelverk, utbildad personal, metoder för försörjning av kryptonycklar samt IT-säkerhetsåtgärder. För nationellt godkända kryptografiska funktioner och signalskyddssystem, det vill säga de signalskyddssystem och kryptografiska funktioner som godkänts av Försvarsmakten, finns en helhetssyn som omfattar även dessa delar. Nationellt godkända signalskyddssystem och kryptografiska funktioner kan nyttjas av myndigheter för säkert sektorövergripande informationsutbyte.

Staten bör erbjuda sin kunskap vad avser nationellt godkända kryptografiska funktioner och signalskydd till övriga samhället genom rådgivning för att därigenom höja säkerhetsnivån i samhällsviktiga informationssystem och för att öka medvetenheten om risker och sårbarheter. Generella råd och rekommendationer bör utarbetas som riktar sig till statliga myndigheter men även till kommuner, företag m.fl. Genom att följa de gemensamma råden och rekommendationerna erhålls en likartad säkerhetsnivå som också underlättar möjligheten till informationsutbyte mellan myndigheter och mellan olika funktionssystem.

Det finns inom många myndigheter en otillräcklig kunskap om vilka möjligheter och resurser som finns för säkert informationsutbyte mellan myndigheter. Att underlåta att skydda sin information, att använda produkter som är osäkra på grund av att de inte är säkerhetsgranskade eller genom att nyttja att bristfälliga administrativa rutiner kan få omfattande konsekvenser för myndigheter eller organisation vad avser effektivitet och tillit. Ett informationspaket som vänder sig till all personal inom statsförvaltningen bör utarbetas och spridas för att öka medvetenheten och användningen av godkända signalskyddssystem och säkra kryptografiska funktioner.

Det är främst brister i utbildning samt medvetna eller omedvetna avsteg från de administrativa rutinerna eller bristfällig hanteringen av kryptonycklar som banar väg för att kryptosystem kan forceras. Detta visar på vikten av att ha ett högt säkerhetsskydd, säkra rutiner samt kunnig personal med ett högt säkerhetsmedvetande. För hantera eller använda ett signalskyddssystem krävs behörighet som erhålls genom utbildning. Ansvarig för signalskyddsutbildning är Försvarsmakten, Totalförsvarets signalskyddsskola (TSS), som utbildar signalskyddspersonal inom försvarsmakten och för krishanteringssystemets behov. Efter godkänd utbildning vid TSS ges eleverna behörighet att nyttja systemet samt att utbilda användare inom den egna organisationen.

Sverige har ett gott anseende internationellt vad avser kryptofrågor. Svenska företag har en hög kompetens inom området och har utvecklat produkter för vilka det finns ett internationellt intresse. För att nyttja nationens samlade resurser bör ett samverkansorgan bildas för informationsutbyte om samhällets behov av skydds-mekanismer samt om nya metoder och ny teknik som nyttjar nationellt godkända kryptografiska funktioner. Samverkansorganet bör omfatta myndigheter med kunskaper inom kryptoområdet samt företag som arbetar med utveckling inom området. Denna samverkan medför att staten kan nyttja företagens djupa tekniska kunskaper. För företagen kan samarbetet innebära en större möjlighet att delta i upphandlingar av kryptoprodukter inom EU eller för andra internationella organ.

8.2.2 Åtgärdsförslag

Målsättningar signalskydd

- *Hög kunskap och medvetenhet inom myndigheter om vilka möjligheter och resurser som finns för säkert informationsutbyte mellan myndigheter.*
- *Ett effektivt nyttjande av nationens samlade resurser för säkert informationsutbyte*

Åtgärdsförslag 39: Framtagande av informationspaket gällande signalskydd
Det bör tas fram ett informationspaket om signalskydd som omfattar en beskrivning av statens organisation och ansvar inom området samt om de förmågor för säkert tvärsektoriellt informationsutbyte som kan erbjudas myndigheter.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Försvarsmakten i samverkan med berörda myndigheter

Åtgärdsförslag 40: Bildande av samverkansorgan inom kryptoområdet
Det bör bildas ett samverkansorgan inom kryptoområdet för att skapa ett effektivt nyttjande av den nationella kompetens som finns vid myndigheter och inom näringslivet.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Försvarsmakten i samverkan med berörda myndigheter

Åtgärdsförslag 41: Rekommendationer för signalskydd
Det bör ges ut rekommendationer för signalskydd som riktar sig till myndigheter, kommuner, landsting och samhällsviktiga företag.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB

8.3 Swedish Government Secure Intranet – SGSI

8.3.1 Bakgrund

I Infosäkutredningen föreslogs ett GovernmentNet; ett myndighetsnät för säkerhetsklassad information som skulle erbjuda kommunikationstjänster mellan myndigheter. 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), som förutom kommunikation via TESTA kan nyttjas för säkert informationsutbyte mellan svenska myndigheter. Kommunikationen mellan myndigheterna är krypterad med ett nationellt godkänt signalskyddssystem. SGSI har ackrediterats för att kunna hantera information som klassats RESTREINT UE. SGSI kan ses som ett embryo till ett nät till vilket myndigheter kan ansluta sig då verksamheten har behov av att förmedla information som värderats som känslig och skyddsvärd via en robust kommunikation utan beroende av Internet. Idag skyddas kommunikation av klassad information av specifika krypton för tal, data och fax. Ett myndighetsnät skulle kunna nyttjas för kriskommunikation inom områdena skydd mot olyckor, krisberedskap och civilt försvar samt för kontakter med EU:s medlemsstater och organ. Krisberedskapsmyndigheten är systemägare för SGSI.

Det finns inom statsförvaltningen ytterligare nät som eventuellt kan ingå i eller kopplas till SGSI. Det vore önskvärt att skapa en sektionerad del av nätet som även kan nyttjas för underrättelseinformation i samband med en kris eller annan allvarlig händelse där sådan information behöver förmedlas över ett säkert nätverk. Det uppstår dock problem genom att den svenska sekretesslagstiftningen inte bygger på samma klassningssystem som inom EU när man delar in ”EU classified information” och indelas i följande nivåer:

- TRÈS SECRET UE/EU TOP SECRET
- SECRET UE
- CONFIDENTIAL UE
- RESTREINT UE

Enligt svensk lagstiftning kan en handling sekretessklassas öppen, hemlig eller kvalificerad hemlig vilket innebär att det inte finns nivåer som motsvarar EU:s nivåer CONFIDENTIAL UE och RESTREINT UE. Detta försvårar internationella samarbeten. Att klassa information Hemligt är många gånger inte praktiskt eftersom detta genererar högre kostnad och mer omfattande administrativa regler och rutiner. För känslig information räcker det ofta med de skyddsåtgärder som erfordras för nivån RESTREINT UE. Försvarsmakten och dess tillsynsmyndigheter hanterar denna problematik genom att indela säkerhetsskyddet i fyra informationsklasser, i syfte att underlätta internationellt samarbete och samtidigt få ett balanserat säkerhetsskydd. Detta föreskrivs i Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd 1 kap. 4§.

Inom statsförvaltningen bör det utvecklas en lättanvänd tjänst för säkert informationsutbyte via Internet eller annat publikt nätverk. Det ska även vara möjligt att skydda filer så att dessa kan bifogas via nättjänsten. För att uppnå säkerhet i nättjänsten bör nationellt godkända kryptografiska funktioner nyttjas. En fortsatt utveckling av SGSI kan utgöra grunden för denna tjänst.

8.3.2 Åtgärdsförslag

Målsättningar SGSI

- *Det bör i statsförvaltningen finnas en användarvänlig tjänst för säkert informationsutbyte*

Åtgärdsförslag 42: Plan för utveckling av SGSI
Det bör tas fram en plan för hur SGSI kan vidareutvecklas och spridas till alla myndigheter inom statsförvaltningen som behöver utbyta information på ett säkert sätt. Det bör också tas fram ett informationspaket med information om vad SGSI kan tillhandahålla samt om kraven för att ansluta till nätet.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2009
Ansvar: MSB (systemägare) i samverkan med berörda myndigheter

8.4 E-förvaltning

8.4.1 Bakgrund

I januari 2008 presenterades en nationell handlingsplan för e-förvaltning. I handlingsplanen utpekas ett väl fungerande och säkert system för elektronisk identifiering som en av förutsättningarna för utvecklingen av en säker elektronisk förvaltning. Säker elektronisk identifiering är en grundförutsättning för fungerande e-tjänster i samhället. Det är samhället som sörjer för att alla medborgare tilldelas en unik identitet. När allt fler vardagsärenden ”digitaliseras” faller det sig därför också naturligt att samhället åtar sig ett omfattande ansvar avseende ett ramverk för elektronisk identifiering. Det gäller här att få fram enkla metoder som når allmän spridning. Därför borde detta område prioriteras i statens satsningar på informationssäkerhetsområdet.

På uppdrag av regeringen tar Verva fram en färdplan för framtidens e-legitimation (år 2007 – 2017). En central funktion i färdplanen är att samordning sker genom en funktion till vilken andra aktörer är knutna såsom myndigheter, kommuner, näringsliv och utfärdare av ett nationellt ID-kort. Samordningsfunktionen har olika uppgifter som kan vara tekniska, administrativa eller legala. Viktiga krav vid säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar är att:

- Meddelanden når rätt mottagare
- Meddelanden inte förvanskas
- Meddelanden är skyddade mot otillbörlig insyn
- Beslut ska kunna dokumenteras och härledas till myndighet och handläggare
- Beslut ska kunna meddelas medborgare på säkert sätt
- Inkommande och upprättade handlingar ska vara tillgängliga över tid
- Den personliga integriteten skyddas
- Elektronisk signering ska vara möjlig

8.4.2 Åtgärdsförslag

Målsättningar e-legitimation

- *Ett system för e-legitimation finns som möjliggör statens satsning på e-förvaltning och bidrar till säkerheten vid elektroniskt informationsutbyte*

Åtgärdsförslag 43: Färdplan för e-legitimation
Vervas färdplan för e-legitimation bör skyndsamt genomföras för att stödja regeringens handlingsplan för e-förvaltning.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under år 2009
Ansvar: Verva i samverkan med berörda myndigheter

Åtgärdsförslag 44: Säkerhetsgranskning av elektronisk identifiering och signering
Den konceptuella metod som Verva föreslår för elektronisk identifiering och signering bör granskas ur ett säkerhetsperspektiv för att säkerställa kvalitet och långsiktighet av e-tjänster.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under år 2008
Ansvar: Verva och KBM

9 Säkerhet i produkter och system

9.1 Evaluering och certifiering av IT-säkerhetsprodukter

Infosäkutredningen konstaterade i sina delbetänkanden att standarder inom främst styrning och ledning samt för evaluering och certifiering av säkerhetsegenskaper i produkter och system har stor betydelse för utvecklingen inom informations- och IT-säkerhet.

Standarden ISO/IEC IS 15408 *Evaluation criteria for IT security* utgör vad som brukar kallas Common Criteria (CC). Common Criteria är en standard för kravställning, deklaration och evaluering av säkerhet i IT-produkter och IT-system samt i deras användningsmiljöer. Common Criteria omfattar dokumentation i följande delar:

- CC del 1 är en introduktion till metoden, terminologin och aktuella roller. Här beskrivs strukturen och de principer som gäller vid evaluering.
- CC del 2 ger detaljerad beskrivning av funktionella säkerhetskrav. Här finns en katalog över funktionella säkerhetskomponenter indelade i familjer och klasser.
- CC del 3 listar assuranskrav paketerade i sju olika assuransnivåer. Här finns även evalueringskriterier för kravprofiler och säkerhetsmål.

Myndigheternas efterfrågan av certifierade produkter är ännu begränsad. En viktig fråga är därför också hur man ska öka efterfrågan från offentlig sektor på produkter som kan bidra till önskad säkerhet. Ett allmänt intryck vad gäller standardisering av informations- och IT-säkerhet är att tillämpningen av standarder i många fall är alltför begränsad. Ett tydligt skäl är brister i kunskap om vilka standarder som finns och om deras innehåll. Standardiseringsarbetet sker i alltför liten utsträckning genom aktiv kunskapsinhämtning och aktiv medverkan. Ofta råder oklarhet i vilken utsträckning standarder bör tillämpas och följas och också huruvida det finns någon statlig hållning till standarder och standardisering.

Ingen enskild person behärskar alla teknikområden utan beroendet av specialister är stort. I en för offentlig sektor övergripande IT-arkitektur kan samordning av teknik, samsyn på ledning och styrning, gemensam upphandling och användning av produkter som kan användas i samverkan med varandra i hög grad bidra till ökad effektivitet både vad gäller funktion, ekonomi och informationssäkerhet. *Se även Åtgärdsförslag 8 i kapitel 5: Rekommendationer för kravställning vid upphandlingar.*

Central upphandling av IT-produkter genomförs redan i stor utsträckning genom i första hand Vervas uppdrag. Genom gemensamma kravformuleringar bidrar detta i hög grad till användning av gemensamma lösningar och produkter som också ger god interoperabilitet.

Offentlig förvaltning bör vara en tydligare kravställare när det gäller sin IT-verksamhet. Ökade krav på följsamhet mot öppna standarder, bättre metodstöd för kravställande ger ökad kvalitet vad gäller funktion och säkerhet, skapar möjligheter till modularitet genom utbytbara komponenter med öppet beskrivna och standardiserade gränssnitt. Evaluerade och certifierade produkter skapar normer för förutsättningar och krav på omvärlden. När det gäller krav på certifiering av produkter har vissa andra länder gått

relativt långt när det gäller att ställa krav. Exempelvis ger Japan bidrag och rabatter till myndigheter som använder CC-certifierade produkter och USA kräver tillämpning av CC-certifierade produkter hos myndigheter som har höga krav på konfidentialitet. I Sverige saknas ännu denna typ av krav.

Det kan dock vara rimligt att i ökad utsträckning ställa centrala krav på följsamhet mot gemensamma policies. Hur ska man på ett bättre sätt styra produktval så att IT-produkter för e-tjänster håller den säkerhet som krävs för robust och tillitsfull verksamhet? Kan utvecklingen genomföras snabbare mot ökad interoperabilitet och modularitet, säkrare former för informationsutbyte samt minskade risker för intrång i personlig integritet genom tydligare normer och direktiv från centrala instanser.

Ökad tillämpning av Common Criteria (CC) som metodstöd vid kravställande kan bidra till säkrare produkter och system, under förutsättning 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 kravprofiler (PP -protection profile) offentliggjorda. En begränsad insats som kan ge stor nytta är att öka kunskapen om var dessa kravprofiler finns och hur dessa bör tillämpas. Ett ”nationellt bibliotek” med information kopplat till beskrivningar av den offentliga sektorns IT-arkitektur och IT-säkerhetsarkitektur kan vara ett sätt att åstadkomma en relevant lösning.

9.1.1 Åtgärdsförslag

Målsättningar evaluering och certifiering av IT-säkerhetsprodukter

- *En ökad tillämpning av Common Criteria (CC) som metodstöd vid kravställande.*
- *Offentlig förvaltning ska vara en tydlig kravställare när det gäller sin IT-verksamhet.*

Åtgärdsförslag 45: Tillämpning av certifierade produkter
En gradvis ökande tillämpning bör ske av *Common Criteria (CC)*. Kravställning avseende tillämpning av certifierade produkter bör utgå från den grundläggande säkerhetsnivån som föreslås i åtgärdsförslag 14.

Kostnad: Förslaget medför låg kostnad
Tid: Bör påbörjas under 2008
Ansvar: KBM och FMV i samverkan med berörda myndigheter

Åtgärdsförslag 46: Bibliotek med CC-evaluerade kravprofiler
Det bör utvecklas ett ”nationellt bibliotek” med offentliggjorda CC-evaluerade kravprofiler (PP, ”protection profile”) kopplat till beskrivningar av den offentliga sektorns IT-arkitektur.

Kostnad: Förslaget medför låg till medelstor kostnad
Tid: Bör påbörjas under 2008
Ansvar: KBM och FMV i samverkan med berörda myndigheter

9.2 Säkerhet i digitala kontrollsystem

9.2.1 Bakgrund

Digitala kontrollsystem (SCADA)[1] används i samhällsviktiga verksamheter – exempelvis el- och vattendistribution samt spårbunden trafik och petrokemisk industri – för att styra och övervaka de centrala fysiska processerna. Dagens kontrollsystem görs i allt högre utsträckning tillgängliga via publika nätverk (Internet), bygger allt mer på samma teknik som vanliga IT-system och integreras med administrativa IT-system. Sammanfattningsvis medför denna utveckling en ökad risk för samhället.

Störningar i digitala kontrollsystem kan påverka tillgången på livsviktiga allmänna funktioner såsom elkraft, dricksvatten, persontransporter och gas- eller oljeproduktion. Säkerhet i digitala kontrollsystem är ett tvärsektoriellt område där myndighetsansvaret ligger på flera tillsynsmyndigheter. De grundläggande säkerhetsproblemen kan till stor del hänföras till beroenden mellan IT-system och fysiska försörjningssystem, det vill säga frågeställningen omfattar både CIIP (Critical Information Infrastructure Protection) och CIP (Critical Infrastructure Protection). I dagsläget finns mycket få svenska aktörer med djupare kompetens inom området. Speciellt små och medelstora operatörer av samhällsviktig infrastruktur saknar såväl resurser som kompetens för att utföra ett kvalificerat säkerhetsarbete. Eftersom området berör aspekter som är vitala ur ett nationellt säkerhetshänseende så är det mycket viktigt att det finns en statlig kompetens inom området.

Sverige behöver en sammanhållen statlig satsning på säkerhet i digitala kontrollsystem. Avsikten med ett sådant initiativ är att skapa en ökad nationell förmåga att förebygga och hantera störningar i de informations- och kommunikationssystem som används för styrning, övervakning och kontroll av samhällsviktiga verksamheter. En sådan satsning kan skapa en ökad medvetenhet om risker och möjligheter till skydd, samt förbättra statsmaktens kompetensförsörjning vad gäller kunskaper inom praktisk kontrollsystem-säkerhet. I förlängningen leder detta till en ökad nationell säkerhet, speciellt en ökad beredskap för att hantera kvalificerade antagonistiska IT-angrepp mot samhällsviktiga verksamheter. Det ger även större möjligheter för svenska aktörer att delta i det internationella arbetet med att skapa säkerhet i digitala kontrollsystem.

En effektiv svensk satsning på säkerhet i digitala kontrollsystem bör till stor del bygga på befintliga organisationer, utveckla befintlig expertis, samordna befintliga resurser

[1] Begreppet SCADA (Supervisory, Control, and Data Acquisition) har i vissa tekniska sammanhang varit reserverat för en speciell typ av kontrollsystem. Ibland används dock förkortningen SCADA som en samlingsterm för alla former av industriella informations- och kommunikationssystem.

samt dra nytta av internationella aktörers erfarenheter och kunskap. En statlig satsning på säkerhet i digitala kontrollsystem bör innefatta att:

- Öka samarbetet kring säkerhet i digitala kontrollsystem inom statsmakten
- Vidareutveckla det pågående samarbete kring säkerhet i digitala kontrollsystem mellan Sverige och andra länder
- Öka medvetandet kring säkerhet i digitala kontrollsystem bland användare och leverantörer av dessa system
- Vidareutveckla den formella dialogen mellan statliga aktörer och ägare och användare av digitala kontrollsystem
- Genomföra riktade insatser för att öka den praktiska säkerheten i de digitala kontrollsystem som ingår i samhällsviktiga verksamheter

En viktig del av samverkan mellan den centrala statsmakten och användare av digitala kontrollsystem har sedan år 2005 skett inom ramen för KBM:s informationsdelningsforum FIDI-SC.[2] Detta arbete utvärderades med positivt resultat under våren 2007 och forumets verksamhet har därefter permanentats och utökats. Verksamheten inom FIDI-SC engagerar ett antal myndigheter och för närvarande pågår ett arbete med att ta fram ett förslag till programplan för en mer samordnad statlig samverkan kring säkerhet i digitala kontrollsystem.

För att skapa möjligheter för underrättelse- och säkerhetsmyndigheter samt sektorsmyndigheter att delta som attraktiva samarbetspartner och respekterade aktörer i arbetet tillsammans med användare av digitala kontrollsystem så krävs en praktiskt inriktad verksamhet. En samordnad statlig satsning på säkerhet i kontrollsystem bör därför omfatta följande: medvetandehöjande åtgärder såsom utbildning och framtagande av riktlinjer och rekommendationer, samverkan och informationsdelning samt praktisk labbverksamhet och tekniska säkerhetsgranskningar.

9.2.2 Åtgärdsförslag

Målsättningar säkerhet i digitala kontrollsystem (SCADA)

- *Att skapa en ökad nationell förmåga att förebygga och hantera störningar i de informations- och kommunikationssystem som används för styrning, övervakning och kontroll av samhällsviktiga verksamheter.*

Åtgärdsförslag 47: Statlig samordnad satsning på säkerhet i digitala kontrollsystem inom samhällsviktiga verksamheter
Regeringen bör ge MSB i uppdrag att genomföra en statlig satsning på säkerhet i digitala kontrollsystem. Avsikten med ett sådant initiativ är att skapa en ökad nationell förmåga att förebygga och hantera störningar i de informations- och kommunikationssystem som används för styrning, övervakning och kontroll av samhällsviktiga verksamheter.

Kostnad: Förslaget medför hög kostnad
Tid: 2009-2011
Ansvar: MSB i samverkan med berörda myndigheter och näringsliv

[2] Läs mer om FIDI-konceptet i avsnitt 7.3.

Referenser

Lagar

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

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

Personuppgiftslagen (1998:204)

Sekretesslagen (1980:100)

Säkerhetsskyddslagen (1996:627)

Förordningar

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

Förordningen (2006:942) om krisberedskap och höjd beredskap

Myndighetsförordningen (2007:515)

Säkerhetsskyddsförordningen (1996:633)

Förordningen (1994:714) med instruktion för Försvarets radioanstalt

Förordningen (1996:103) med instruktion för Försvarets materielverk

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

Förordningen (1998:1192) med instruktion för Datainspektionen

Förordningen (2000:555) med instruktion för Försvarsmakten

Förordningen (2002:518) med instruktion för Krisberedskapsmyndigheten

Förordningen (2002:1050) med instruktion för Säkerhetspolisen

Förordningen (2005:860) med instruktion för Verket för förvaltningsutveckling

Förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte

Föreskrifter och allmänna råd

Datainspektionen: Allmänna råd – Säkerhet för personuppgifter, 1999.

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

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

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

Verket för förvaltningsutveckling: Föreskrift (VERVAFS 2007:2) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte.

Verket för förvaltningsutveckling: Allmänna råd (VERVAFS 2007:2AR) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte.

Dokument från regeringen

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

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

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

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

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

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

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

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

SOU 2004:23 *Från verksförordning till myndighetsförordning.*

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

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

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

Dokument från myndigheter

KBM: *Lägesbedömning av samhällets informationssäkerhet 2008.*

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

KBM: *Lägesbedömning av samhällets informationssäkerhet 2007.*

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

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

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

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

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

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

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

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

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

Vinnova (2005) *IT security in the USA, Japan and China – A Study of Initiatives and Trends within Policy, R&D, Industry and Technology*, Vinnova A2005:015.

Standarder

SIS: *HB 550 Terminologi för informationssäkerhet*, Utgåva 3.

SIS/ISO/IEC: *ISO/IEC 27001:2005, Information Technology – Security Techniques - Information Security Management Systems – Requirements.*

SIS/ISO/IEC: *ISO/IEC 27002:2005, Information Technology – Security Techniques - Code of Practice for Information Security Management.*

ISO/IEC: *IS 15408 Evaluation criteria for IT security (Common Criteria – CC).*

Internationella rapporter

Japan: *Secure Japan Strategy – First Step towards a Trustworthy Strategy*.

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

OECD: *OECD:s riktlinjer för säkerheten i informationssystem och nät – På väg mot en säkerhetskultur*.

Storbritannien: *A National Information Assurance Strategy*, Cabinet Office, Central Sponsor for Information Assurance.

Tjeckien: CR *National Strategy for Information Security CR NSIS*.

Tyskland: *National Plan for Information Infrastructure Protection – Protection of Critical Infrastructures*, Federal Office for Information Security (BSI).

USA: *Federal Information Security Management Act (FISMA)*.

USA: *National Infrastructure Protection Plan*, Department of Homeland Security, 2006.

USA: *Standards for Security Categorization of Federal Information and Information Systems* (FIPS PUB 199).

Bilaga 1: Sammanställning av åtgärdsförslag

Åtgärd	
Kapitel 3: Genomförande	
1	Förvaltning av handlingsplanen under 2008
2	Fortsatt förvaltning av handlingsplanen
3	Uppdatering av strategin
Kapitel 4: Författningsförändringar	
4	Översyn av lagstiftningen på informationssäkerhetsområdet
5	Föreskriftsrätt inom informationssäkerhetsområdet
Kapitel 5: Informationssäkerhet i verksamheter	
6	Myndighetsledningars formella ansvarstagande för hantering av informationssäkerhetsrisker
7	Förtydligande av informationssäkerhet i vägledningar för risk- och sårbarhetsanalyser
8	Rekommendationer för kravställning vid upphandlingar
9	Informationsmaterial till myndighetsledningar
10	Rekommendationer för tillämpning av standarderna ISO/IEC 27001 och 27002
11	Stödmaterial för införande av ledningssystem för informationssäkerhet
12	Utveckling och införande av ett värderingssystem för informationssäkerhet
13	Gemensam modell för klassificering av informationstillgångar
14	En grundläggande säkerhetsnivå för informationssäkerhet i samhället
15	Rekommendationer för en grundläggande säkerhetsnivå
Kapitel 6: Kompetensförsörjning	
16	Nationellt kunskapscenter för informationssäkerhet
17	Utökning av kampanjen Surfa lugnt
18	Stimulera folkbildning inom informationssäkerhet
19	Rekommendationer till grundskola och gymnasium
20	Rekommendationer till högskolor och universitet
21	Identifiering av kompetensbehov hos yrkesverksamma
22	Utbildningar i informationssäkerhet
23	Nationell forskningsstrategi
24	Koordinering av forskningsmedel
25	Inrättande av forskarskola
Kapitel 7: Informationsdelning, samverkan och respons	
26	Operativ nationell samordning
27	Upprättande av en IT-beredskapsorganisation
28	Obligatorisk incidentrapportering
29	Utveckling av förmågan att förebygga och bekämpa IT-relaterad brottslighet
30	Polisiärt deltagande i samverkan inför krissituationer
31	Informationsdelning kring IT-relaterade brott
32	Nätverkssamverkan
33	Samverkan mellan offentlig och privat sektor
34	Upprättande av FIDI-Finans
35	Bevaka EU:s informationssäkerhetsarbete
36	Etablera ett forum för samverkan inom ramen för EPCIP
37	Internationell samverkan
Kapitel 8: Kommunikationssäkerhet	
38	Genomföra åtgärder och utveckla handlingsplanen från Strategin för ökad säkerhet i Internets infrastruktur
39	Framtagande av informationspaket gällande signalskydd
40	Bildande av samverkansorgan inom kryptområdet
41	Rekommendationer för signalskydd
42	Plan för utveckling av SGSI
43	Färdplan för e-legitimation
44	Säkerhetsgranskning av elektronisk identifiering och signering
Kapitel 9: Säkerhet i produkter och system	
45	Tillämpning av certifierade produkter
46	Bibliotek med CC-evaluerade kravprofiler
47	Statlig samordnad satsning på säkerhet i digitala kontroll system inom samhällsviktiga verksamheter

Bilaga 2: Förslag till författningsförändringar

Förslag till ändring av förordningen (2006:942) om krisberedskap och höjd beredskap

KBM föreslår en ny paragraf i förordningen om krisberedskap och höjd beredskap som ersätter nuvarande 21 § och är avsedd att gälla för alla myndigheter under regeringen även om det inte råder höjd beredskap.

Vidare föreslås en följdändring i 34 § om rätten att utfärda verkställighetsföreskrifter. Eftersom första stycket avser höjd beredskap och föreskriftsrätt ska gälla även i andra fall föreslås ett nytt andra stycke.

Nuvarande lydelse

> 21 § En bevakningsansvarig myndighet ansvarar för att dator- och kommunikationssystem uppfyller sådana säkerhetskrav att myndighetens uppgifter kan utföras på ett tillfredsställande sätt även under höjd beredskap.
>
> 34 § Myndigheten får meddela de ytterligare föreskrifter som behövs för verkställigheten av 16-21 samt 33 §§ (i den mån höjd beredskap avses), utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket.

Förslag till ny lydelse

> *X § Varje myndighet ansvarar för att dator- och kommunikationssystem uppfyller sådana säkerhetskrav att myndighetens uppgifter kan utföras på ett tillfredsställande sätt.*
>
> *34 § MSB får meddela de ytterligare föreskrifter som behövs för verkställigheten av 16-21 samt 33 §§ (i den mån höjd beredskap avses), utom i fråga om …….*
>
> *MSB får vidare meddela de ytterligare föreskrifter som behövs för verkställigheten av X §.*

Bilaga 3: Samverkansredovisning

Handlingsplanen har tagits fram i samverkan med en mängd aktörer. Samverkan har skett i form av möten, workshops och remisser. Två remisser har genomförts under arbetet med handlingsplanen; 1-17 oktober 2007 och 1-15 februari 2008. Remisserna har varit informella där utkast till handlingsplanen har distribuerats via e-post till lämpliga personer (intresserade och kunniga inom informationssäkerhetsområdet).

Ett flertal möten och workshops har genomförts med KBM:s samverkansråd SAMFI och Informationssäkerhetsrådet. De myndigheter som ingår i SAMFI beskrivs i Bilaga 4. Informationssäkerhetsrådet och dess undergrupp AgN (Arbetsgruppen för Näringslivssamverkan) består av representanter från följande organisationer:

AstraZeneca, Combitech, Ericsson, Försvarets materielverk, Försvarets Radioanstalt, Försvarshögskolan, Försvarsmakten, Finansinspektionen, Hennes & Mauritz, Läkemedelsverket, Microsoft Post- och Telestyrelsen, Rote Consulting, Regerings-kansliet, Saab, Scania, Skanska, Stockholms universitet/KTH, Svenska kraftnät, Svenskt näringsliv, Säkerhetspolisen, TeliaSonera, Totalförsvarets forskningsinstitut, Vattenfall och Verva

Övriga aktörer som har ingått i samverkan (möten, workshops och/eller remisser):

Blekinge tekniska högskola, Brottsförebyggande Rådet (Brå), Bundesamt für Sicherheit in der Informationstechnik (Tyskland), Chalmers tekniska högskola, Countermine, Dataföreningen Sverige, Datainspektionen, Department of Homeland Security (USA), EME Tjänstedesign AB, Försäkringskassan, Generic systems Sweden AB, Högskolan i Skövde, IT- och Telekomföretagen, Imentum AB, Karlstads universitet, Lüning Consulting, Länsstyrelserna, Meile AB, M Gullberg Systemkonsult AB, Nasjonal sikkerhetsmyndighet (Norge), Omicron software systems AB, Riksrevisionen , SIG Security , SIRNET, SIS Tekniska kommitté för ledningssystem för informationssäkerhet (TK 318), Sjöfartsverket, Skatteverket, Socialstyrelsen, Stockholms Läns Landsting, Stockholms universitet, Institutionen för rättsinformatik (IRI), Stockholms universitet/KTH, Institutionen för data- och systemvetenskap , Sveriges Kommuner och Landsting (SKL), Symantec, Södertälje kommun, Technology Nexus AB, Visente AB, Örebro universitet

Bilaga 4: SAMFI-myndigheterna

Samarbetet mellan nedanstående myndigheter bedrivs i Samverkansgruppen för informationssäkerhet (SAMFI). SAMFI ska genom informationsutbyte och samverkan stödja de aktuella myndigheternas uppdrag inom informationssäkerhet och defensiva informationsoperationer. Sedan 2001 har uppgifterna på informationssäkerhetsområdet varit uppdelade på ett antal myndigheter:

KBM — Krisberedskapsmyndigheten har ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. KBM har idag ingen föreskriftsrätt inom informationssäkerhetsområdet.

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

PTS (Sitic) — Post- och telestyrelsen med ansvar för infrastruktur inom telekom-området inrymmer också Sitic som är ett svenskt centrum för IT-incidentinformation. Sitic fungerar idag som en internationell s.k. CERT-organisation.

FMV (CSEC) — Försvarets materielverk har genom CSEC uppgiften att utforma ett system för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med standarden ISO/IEC 15408, Common Criteria (CC).

RKP — Rikskriminalpolisen ansvarar för att utreda brottsrelaterade IT-incidenter. RKP representeras i SAMFI av S-BIT som är en samordningsfunktion för brottsrelaterade IT-incidenter, gemensamägd av Rikskriminalpolisen och SÄPO.

SÄPO — Säkerhetspolisen ansvarar för tillsyn och rådgivning inom informationssäkerhetsområdet för samhällsviktiga civila verksamheter. Tillsynen och rådgivningen avser skydd av rikets säkerhet och skydd mot terrorism. Säpo representeras i SAMFI av S-BIT.

FM — Försvarsmakten ansvarar för informationssäkerhet med inriktning på rikets säkerhet och relation till främmande makt. FM har föreskrifts- och tillsynsansvar för aktörer inom sitt ansvarsområde och för statliga myndigheter i övrigt vad gäller signalskydd.

Verva — Verket för förvaltningsutveckling har uppdraget att leda och samordna statsförvaltningens utvecklingsarbete med säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar. Verva får utfärda föreskrifter och ge vägledning med denna inriktning.