2015-09-14

Justitiedepartementet
103 33 Stockholm

Remissvar över betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten (Ju2015/2650/SSK)

Stiftelsen för internetinfrastruktur (IIS) har beretts möjlighet att lämna synpunkter på förslagen inklusive den förordning som föreslås i betänkandet. IIS säkerhetschef Anne-Marie Eklund Löwinder har även varit förordnad som expert i utredningen från den 10 november 2014.

Tidigare arbete på området

Det är inte första gången som regeringen lämnar ett uppdrag att utreda den övergripande strategiska frågan om samordning av samhällets informations- och cybersäkerhet. **IIS vill framföra** som en generell synpunkt att många av dessa områden har avhandlats och åtgärder har föreslagits i ett flertal tidigare utredningar. Däremot har förslagen sällan resulterat i någon konkret handlingsplan som omsatts i praktiken.

Ett mycket bra exempel är PTS rapport PTS-ER-2011:16, publicerad den 15 juni 2011 med titeln ”Robust elektronisk kommunikation - vägledning för användare vid anskaffning”, där mycket konkreta rekommendationer lämnas i syfte att erhålla en robust infrastruktur för elektronisk kommunikation inom offentlig förvaltning (som givetvis kan användas även utanför sektorn).

Den typen av rekommendationer **borde enligt IIS** ställas som obligatoriska krav mot stat, kommuner och landsting att genomföra och en uppföljning av att så skett ha genomförts. Då hade vi förmodligen haft ett mycket bättre läge när det gäller robust infrastruktur för den statliga förvaltningen än vad som nu är fallet.

Minst tre mer omfattande statliga uppdrag har under de senaste 15 åren berört informations- och it-säkerhet ur ett helhetsperspektiv. Innan dess hade dessa frågor också utretts, både länge och väl av kommittéer som SÅRK, SÅRB och SAMS. Arbetsgruppen för skydd mot informationskrigföring (AgIW) presenterade den 19 augusti 1998 i sin rapport med en strategi och ansvarsfördelning för skydd mot informationsoperationer (då benämnt informationskrigföring) med tio förslag:

- En samordningsgrupp på hög nivå inom Regeringskansliet
- En ny nationell IO-samordning inom dåvarande Överstyrelsen för civil beredskap (nu MSB)
- En nationell incidenthanteringsorganisation (CERT) under Post- och telestyrelsen (PTS)
- Inrättande av en statistikenhet i dialog med Näringslivets säkerhetsdelegation (NSD)
- Rapporteringsplikt för IT-relaterade incidenter inom statsförvaltningen
- Försvarsmaktens mandat beträffande signalskyddstjänsten gentemot totalförsvaret – vilket förvaltas av TSA – vidgas till att även omfatta civila informationssystem av betydelse för totalförsvaret

- En aktiv IT-kontrollfunktion för statsförvaltningen med Försvarsmakten som bas
- Författningsändringar i datalagen med mera initieras snarast
- Mediebevakning på IT-området
- Förändrade samverkansformer, delgivning, utbildning med mera på underrättelseområdet vad avser IO-information

Dessa förslag behandlades av regeringen i propositionen ”Förändrad omvärld – omdanat försvar” och PTS fick senare och som följd av AgIW:s förslag i uppdrag att utreda förutsättningarna för att inrätta en särskild funktion för IT-incidenthantering. I en rapport daterad 28 november 2000 presenterade PTS sina överväganden och förslag.

Det andra övergripande uppdraget hade Statskontoret, som den 24 juni 1998 presenterade sin rapport ”Sammanhållen strategi för samhällets IT-säkerhet”. Detta uppdrag utfördes vid samma tid som AgIW utförde sitt uppdrag. AgIW och Statskontoret drog en skiljelinje mellan sig så att Statskontoret inriktade sig mot hotbilden från enskilda personer till organisationer och företag i fredstid, medan AgIW hade hotbilden i kris och krig samt hotbilden mellan stater och pakter i fredstid. Resultaten av de båda uppdragen företedde stora likheter, med förslag som i stora drag stämde överens med varandra. Även Statskontoret lade förslagen om att dåvarande ÖCB skulle ges en samordnande roll och att lagstiftningen behövde ses över. Statskontoret föreslog också en statistikfunktion och en statlig incidenthantering. Statskontoret indikerade därvid att man borde överväga att göra rapporteringen obligatorisk för statliga myndigheter. Vidare föreslog Statskontoret att PTS skulle ges i uppdrag att ta initiativ till att åtgärder snarast skulle vidtas för att erhålla en säkrare infrastruktur för Internet i Sverige.

PTS fick i regleringsbrevet år 2000 av regeringen i uppdrag att utreda möjligheterna vidare. PTS redovisade 31 maj 2000 sina förslag till åtgärder i rapporten ”Drift av Internet i Sverige oberoende av funktioner utomlands”. I regleringsbrevet år 2001 fick PTS tre uppdrag som en följd av Statskontorets rapport. Statskontorets förslag behandlades av regeringen i propositionen ”Ett informationssamhälle för alla”. I denna proposition gjorde regeringen bedömningen att en tvärsektoriell samordning för IT-säkerhet och skydd mot informationskrigföring borde utformas.

Det ingick i sin tur i det tredje uppdraget, den så kallade Sårbarhets- och säkerhetsutredningens direktiv, att föreslå hur utformningen skulle göras. Regeringen gjorde vidare bedömningen att för den närmaste framtiden borde tre områden prioriteras: skydd mot informationsoperationer, ett säkrare Internet samt elektroniska signaturer och annan säkerhetsteknik.

Utredningens förslag lades fram i maj 2001 i betänkandet ”Strategi för ökad IT-säkerhet och skydd mot informationsoperationer”, SOU 2001:41.

Utredningen redovisade ett antal åtgärder för att öka IT-säkerheten och för att förbättra skyddet mot så kallade informationsoperationer som var på modet att diskutera vid den tiden. Utredningen konstaterade också att Sverige - till skillnad från många andra länder - saknade ett sammanhållet system för att hantera allvarliga IT-hot. Verksamheten inom detta område var uppsplittrad på många organ i samhället och ansvarsfördelningen mellan dessa var i många fall oklar. Detta gällde också statens satsningar inom IT-säkerhetsområdet. Med stöd av erfarenheter i andra länder såg utredningen ett behov av följande funktioner inom IT-säkerhetsområdet:

- En funktion för samordning på nationell nivå av åtgärder mot allvarliga IT-relaterade hot och IT-incidenter.
- En funktion för kvalificerad omvärldsbevakning och omvärldsanalys inom IT-säkerhetsområdet.
  En funktion för hantering av IT-incidenter (bevakning, statistik och varning av berörda systemägare).
- En teknikkompetensfunktion inom IT-säkerhetsområdet (expert- och stödfunktion med hög teknisk kompetens).
- Ett system för säkerhetsinriktad evaluering och certifiering av IT-produkter och IT-system.

Utredningen ansåg att det var statens uppgift att ta ett ansvar inom dessa områden. Samtidigt betonade utredningen den så kallade ansvarsprincipen; att varje verksamhetsansvarig och systemägare har ett ansvar för att säkra de egna systemen mot IT-intrång och andra typer av IT-hot.

Statens roll borde enligt utredningen vara att stödja detta arbete och att svara för funktioner som samhället i övrigt har svårt att organisera. Embryon till vissa av de funktioner som utredningen föreslog fanns då redan på vissa håll inom statsförvaltningen. Enligt utredningens uppfattning behövde ambitionsnivån dock höjas och ansvaret tydliggöras. Utredningen föreslog därför följande ansvarsfördelning:

Samordningsfunktionen borde handhas av ett beredande och rådgivande organ inom Regeringskansliet. Organet föreslogs bemannas av företrädare för departement, myndigheter och näringslivet. Omvärldsbevakningsfunktionen föreslogs läggas på en planeringsmyndighet och integreras i denna myndighets samhällsinriktade omvärldsbevakning.

- IT-incidenthanteringsfunktionen föreslogs ges en organisatoriskt fristående ställning med anknytning till PTS. Efter en tvåårsperiod skulle en utvärdering ske och slutlig ställning tas till huvudmannaskapet.
- IT-teknikkompetensfunktionen föreslogs ges en organisatoriskt fristående ställning med anknytning till Försvarets radioanstalt, FRA.
- Systemet för säkerhetsinriktad evaluering och certifiering av IT-produkter och IT-system skulle byggas upp av Försvarets materielverk, FMV.

I övrigt såg den utredningen ett behov av författningsändringar för att stödja de förslag som utredningen redovisade inom IT-säkerhetsområdet och skyddet mot informationsoperationer. Författningsändringarna ansågs behövas för att tillgodose följande behov:

- En mycket hög sekretess krävdes inom IT-teknikkompetensfunktionen och IT-incidenthanteringsfunktionen vilket kunde kräva lagändringar.
- En aktiv IT-kontroll med sanktionerade intrångsförsök i viktiga system måste kunna bedrivas av IT-teknikkompetensfunktionen och då behövde de lagtekniska förutsättningarna för detta belysas.

Slutligen ansåg utredningen 2001 att regler om obligatorisk incidentrapportering borde införas inom statsförvaltningen. Även denna skyldighet för myndigheterna behövde författningsregleras.

I bilaga 1 presenterar IIS en relativt, om än inte fullständigt, uttömmande lista över utredningar, ofta med mycket konkreta förslag. **Enligt IIS förmenande** är det nu hög tid att gå från förslag till handling.

Om den nu aktuella NISU-utredningen

Inledningsvis vill IIS påpeka att utredningen har haft mycket få möten med expertgruppen och förordnade experter har haft korta ställtider mellan presentation av material och senaste tidpunkt för att lämna synpunkter och påverka innehållet. IIS har ingenting att invända mot den mycket väl genomarbetade bakgrundsbeskrivningen och den översikt som återfinns i avsnitten 2-8. Den ger en bra bild av hur ansvarsfördelningen ser ut, vilken reglering som är aktuell och vilka myndigheter som är inblandade. Dessutom får man en bra internationell överblick.

IIS fokuserar på avsnitt 9, som utgör utredningens överväganden och förslag. Utredningen har bland annat resulterat i förslag om en strategi med sex mål:

De utöver strategin föreslagna åtgärderna inom de områden som utredningen bedömt som strategiska för att uppnå en god informationssäkerhet ska säkerställa att de statliga myndigheterna har ett gemensamt förhållningssätt till informationssäkerhetsfrågor och behovet av skyddad kommunikation samt säkra it-lösningar.

Detaljerade synpunkter på utredningens överväganden och förslag

IIS vill betona att regeringen som ett första steg behöver definiera mål för informationssäkerheten och ange vilket skydd som behövs, för vilka det behövs, hur det ska mätas och hur det ska definieras et cetera. Ett riskbaserat arbetssätt är både nödvändigt och önskvärt. Utredningen föreslår en strategi med sex målsättningar.

- Styrning och tillsyn av informationssäkerheten i staten stärks
- Staten ska bli en tydlig kravställare som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster
- Tillgång till säker kommunikation i staten
- Alla statliga myndigheter ska rapportera it-incidenter
- Stärka förebyggande och bekämpande av it-relaterad brottslighet
- Sverige ska vara och uppfattas som en stark internationell partner

Målsättningarna stöds sedan av de överväganden och förslag som utredningen lägger fram i avsnitt 9.

Den strategi som presenteras är **enligt IIS** en konservering av dagens situation med samma aktörer som alltid, men med lite omfördelning av ansvar och mandat. Det är en lösning som **enligt IIS uppfattning** inte har förutsättningar att lyfta hela det civila Sveriges samhällsapparat säkerhetsmässigt.

IIS saknar också medborgarperspektivet - allt är fokuserat på de statliga myndigheterna själva och kommunikation mellan dessa. **IIS saknar vidare** ett resonemang kring hur säkerhetsfunktioner utvecklas, införs, valideras och används i det civila samhället i dag, det vill säga säkerhet som bygger på öppna standarder, öppen kod och en mångfald leverantörer. Det

borde **som IIS ser det** vara självklart att sträva efter att all kommunikation ska skyddas med moderna metoder.

9.1 En nationell strategi för statens informations- och cybersäkerhet

IIS är positivt till förslaget om att regeringen antar en strategi som tar sikte på att stärka informations- och cybersäkerheten i staten.

Ansvaret för styrning och ledning av statsförvaltningens informations- och cybersäkerhet är fördelat mellan riksdagen, regeringen samt de av regeringen utsedda tillsyns- och stödmyndigheterna. Ett operativt ansvar är också fördelat till den enskilda myndighetsledningen i samtliga myndigheter. Precis som utredningen konstaterar har flera tidigare utredningars resultat endast i begränsad omfattning kommit att genomföras. Det är **enligt IIS** hög tid att gå till handling.

9.1.5 Strategigenomförande och handlingsplan

9.2.2 Inrättande av ett myndighetsråd

IIS ställer sig bakom utredningens förslag i avsnitt 9.1.5 om inrättandet av en genomförandekommitté. **IIS är positivt** till att MSB ges i uppdrag att i samverkan med ett nybildat myndighetsråd ta fram en ny handlingsplan. I detta bör också ingå ett uppdrag om uppföljning av genomförandegraden av förslaget om att alla myndigheter ska definiera och införa ett ledningssystem för informationssäkerhet.

Arbetet med informationssäkerhet behöver professionaliseras och tillsynen över de statliga myndigheterna stärkas. **IIS vill också** att det ställs krav på statliga myndigheters ledning att dessa ska vidta lämpliga säkerhetsåtgärder för att skydda den information som hanteras i de statliga systemen. För att få en relevant och återkommande uppföljning **föreslår IIS** att de statliga myndigheterna i sin årliga resultatredovisning åläggs att redovisa vilka åtgärder som vidtagits och vad som återstår att göra.

9.2 Ansvar, styrning, samordning och tillsyn

9.2.1 En nationell styrmodell

En allt större andel av den offentligt finansierade verksamheten utförs av privata aktörer. Det är viktigt att även de omfattas av stärkta krav på tjänster som innehåller informationshantering eller it-tjänster. **Enligt IIS** behöver regeringen både uppmuntra och höja kraven på leverantörer av tjänster, och tillverkare av program- och maskinvara att förbättra säkerheten i sina produkter.

Med början i propositionen ”Statlig förvaltning i medborgarnas tjänst” (prop. 1997/98:136) har regeringen tydligt deklarerat att den tekniska infrastrukturen för statsförvaltningens kommunikation med medborgare och företag bör bygga på internet. Inom ramen för internet bör myndigheterna utveckla tjänster som förenklar kontakterna med och samspelet mellan medborgare, företag och offentlig förvaltning.

Myndigheter bör använda kommunikation baserad på internetstandarder mot medborgare och företag, därför att tekniken uppfyller de krav som kan ställas på en öppen kommunikationsarkitektur. Genom att använda system som bygger på internet åstadkoms en

enhetlig miljö för samverkan, utveckling, drift och säkerhet. Regeringen framförde i IT-propositionen våren 2000 bland annat att regler och system på IT-området bör vara sådana att de skapar förtroende genom att vara säkra, förutsägbara och teknikneutrala, internationella samt skydda individens integritet. Samhället bygger datornät och använder dem allt mer till funktioner och tjänster där vi inte kan acceptera att något slutar fungera. **IIS vill understryka detta faktum.**

Om en nationell satsning på systematiskt informationssäkerhetsarbete i statlig verksamhet i form av ett gemensamt ramverk bidrar till att myndigheternas informationssäkerhetsarbete utförs på ett enhetligt sätt så är **IIS positiv till** att förslaget genomförs. En sådan satsning måste omfatta relativt mycket praktiskt arbete för att skapa en gemensam syn på en lägsta nivå av informationssäkerhet. **IIS har inget att invända** mot att styrmodellen utvecklas inom det myndighetsråd som utredningen föreslår. **IIS vill dock betona** vikten av att en sådan styrmodell förankras i andra sektorer i samhället för att få större genomslag.

9.2.3 En ny förordning för statliga myndigheters informationssäkerhet

9.2.4 Tillsyn

IIS är positivt till föreslaget om att MSB får i uppgift att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet. **IIS tror** emellertid att det kräver en kompetensförstärkning hos myndigheten.

Den som ska kunna ge råd i förebyggande informationssäkerhetsarbete och vid incidenter måste själv ha hög kompetens och god kännedom inom flera områden som berör informationssäkerhet som till exempel om hur systemen är uppbyggda (operativsystem, DNS, IP och nätteknik), om skydd mot intrång och skydd mot avlyssning.

Ett av de största problemen på internet idag är den bristande säkerheten i de enskilda internetanvändarnas miljöer, det vill säga de som ska kommunicera med offentlig förvaltning. Datorer eller annan ändutrustning som inte är tillräckligt skyddade kan kapas och utnyttjas som plattformar för överbelastnings- och andra typer av störningsattacker mot bland annat kritiska delar av internets infrastruktur. Detta innebär inte bara en risk för den enskilde användarens integritet eller egendom, utan även för internets funktion i stort.

En överbelastningsattack mot kritiska delar av internets infrastruktur kan få konsekvenser för internetanvändare världen över. Det är därför viktigt att alla internetanvändare kan förmås att ta ett större ansvar för sitt eget beteende på internet och säkerheten i sin egen miljö. Men de säkerhetsproblem som finns idag är komplexa och för att användarna ska kunna agera säkert på internet och kunna säkra sin egen miljö krävs ofta en omfattande förståelse och kunskap.

Att öka kompetensen och därmed säkerhetsmedvetandet är något som bör ske på olika nivåer och för olika målgrupper. En målgrupp är privatanvändarna för vilka det är särskilt viktigt att bli medvetna om de risker de utsätter sig för när de är uppkopplade till internet samt hur dessa risker kan minimeras.

En annan målgrupp är de organisationer som erbjuder tjänster via internet och som administrerar ett eget nätverk kopplat till internet. Många problem kan uppstå som kan få till följd att organisationen blir isolerad från internet, vilket kan få stora konsekvenser för samhället. Det kan röra sig om bland annat kabelbrott, störningar i elförsörjningen och problem hos olika operatörer på såväl fysisk som logisk nivå. En organisation som administrerar sitt eget nätverk i form av ett eget AS (autonomt system) behöver till exempel goda kunskaper om BGP (Border Gateway Protocol) för att inte av misstag skapa stora problem för många andra internetanvändare. Vi har

på senare år sett exempel på att ett litet handhavandefel hos en internetoperatör kan få stora konsekvenser över hela världen.

Dessa båda målgrupper är inte bara internetanvändare, de är även beställare av utrustning och internetanslutningar. Genom att höja kompetensen hos dessa beställare kan de bli mer kvalificerade kravställare med möjlighet att identifiera och minimera sårbarheter. Ytterligare en viktig målgrupp här är staten som en stor användare av internet. Dels erbjuder staten tjänster, dels använder staten internet som en kanal för att automatiskt lämna och hämta information till och från centrala register och system. E-post och webbtjänster används dessutom som ett huvudsakligt kommunikationsmedel mellan medborgare och myndigheter i Sverige och internationellt.

Som stor inköpare av olika produkter och tjänster för internetanvändning har staten goda möjligheter att i samband med upphandlingar påverka marknaden gällande säkerhet i hårdvara, mjukvara och tjänster. För att kunna utnyttja denna starka position maximalt är det enligt **IIS uppfattning nödvändigt** att staten förstärker sin kompetens om internetsäkerhet bland statens egna upphandlare och kravställare. Säkerhetstjänster erbjuds först när efterfrågan blir så stor att den motiverar leverantörens merkostnader för utveckling och genomförande. Därför blir också statens, och även kommunernas och landstingens, roll så avgörande i sammanhanget.

Beroendet av internet växer kontinuerligt, och som en konsekvens av det blir samhället allt mer mottagligt för IT-angrepp. Utvecklingen mot ökad konvergens och användningen av nya tekniker medför dels att användarnas terminaler utgör en allt högre risk, dels att kompetensgapet riskerar att öka i takt med komplexiteten.

Nätets ökade komplexitet gör att endast ett fåtal personer har helhetsbilden klar för sig och samtidigt är det ingen som har helhetsansvaret. Utvecklingen på internet är till stor del decentraliserad och teknikdriven. Säkerheten på internet drivs därför inte av en samlad plan. Lösningar sker främst genom att ”lappa och laga”. Detta tillsammans med avsaknaden av ansvar och helhetsbild medför att avsiktliga och oavsiktliga fel lätt kan uppstå.

En utveckling som innebär en ökad komplexitet är övergången till internetprotokollet IPv6. Under överskådlig tid kommer den tidigare versionen, IPv4, att samexistera med IPv6 genom tillfälliga men ändå komplexa lösningar.

Den ökade komplexiteten är en konsekvens av ökad funktionalitet och säkerhet. Det gäller som princip för all vidareutveckling, inte bara på internet. Ett exempel förutom IPv6 är säkrare DNS (Secure DNS), där funktionen ökar säkerheten, men även komplexiteten på grund av nyckelhantering med mera.

9.2.5 Informationssäkerhet som en del av myndighetens revision

IIS är positivt till behovet av att utveckla revision av informationssäkerhet bland annat genom rapporteringskrav vid årsredovisning och budgetunderlag. Till det **vill IIS även lägga** en skyldighet att informera de drabbade vid incidenter med exempelvis informationsläckage som följd, även till enskilda medborgare.

Inrättande av en IT-haverikommission

IIS säkerhetschef har ingått i utredningen som expert, och som sådan har hon framfört argument för inrättande av en IT-haverikommission, något som utredningen dock valt att inte ta upp i betänkandet.

IIS vill därför upprepa argumentationen. Motiven för inrättandet av en IT-haverikommission är följande. Gång efter gång drabbas samhället av allvarliga störningar och avbrott i e-förvaltning och andra frekvent använda tjänster på grund av haverier hos tredjepartsleverantörer av IT-drift, infrastruktur och applikationer.

I rapporten ”IT- och informationssäkerhet i Sverige. Erfarenheter och reflektioner från några större it-incidenter under 2012-2014” (publ.nr: MSB721 – januari 2015) beskrivs fem fall av it- och informationssäkerhetsincidenter som inträffat i Sverige de senaste tre åren och där samhällets informationshantering påverkades kraftigt.

Efter en kabelbrand i en av Fortums tunnlar i september 2013 blev tiotusentals hushåll i Vasastan i Stockholm utan telefon och internet i flera veckor. Trygghetslarm slutade att fungera. Även ambulansutrop störde. Länsstyrelsen har tidigare pekat ut tunnelbränder som en allvarlig samhällsrisk för Stockholm.

Stokabs kablar i Fortums tunnel kopplades om efter branden till andra kablar i stadsnätet inom loppet av ett par dagar. Den andra stora infrastrukturägaren i landet, det Telia Sonera-ägda bolaget Skanova, valde att inte följa ansvarsprincipen och till exempel samverka med eller ta hjälp av Stokab. Man kunde till exempel ha lånat fiberkabel under avbrottet. I stället valde Skanova att laga kabeln i den utbrända tunneln, vilket tog avsevärt längre tid och bidrog till att det dröjde så länge som upp till fyra veckor innan alla kunder fått sina tjänster tillbaka.

Tieto- och Evry-haverierna ligger i färskt minne hos många av oss. Haverierna hos Evry drabbade dessutom samma kunder två gånger inom loppet av sex månader. Det lär ju påverka kundernas kunder och deras förtroende för kompetensen och förmågan hos exempelvis SJ, SL, Posten och Systembolaget att upphandla tillgängliga och robusta IT-tjänster och inte bara stirra sig blinda på prislappen.

Våren 2012 briserade nyheten om läckta personnummer till personer med skyddad identitet från Skatteverket efter ett dataintrång hos myndighetens leverantör Logica. Det visade sig att långt fler myndigheter drabbats, både i och utanför Sverige, däribland Danmark. På samma server låg också Kronofogdens databaser med uppgifter om skuldsatta privatpersoner och företag – något som uppdagades långt senare och som inblandade parter försökte tysta ner.

Första intrånget skedde genom att man lyckades använda riksdagens konto i SPAR-registret genom att lura systemet för lösenordsåterställning, och sedan rullade angriparen, med hjälp av information om systemets konstruktion som man kommit över vid ett tidigare intrång hos Logica, upp allt mer av systemet och det lagrade innehållet. Bland de drabbade myndigheterna fanns även Polisen.

I början av juni 2013 inträffade en rad haverier i IT-systemet Take Care som hanterar miljoner svenskars sjukjournaler. Systemet gör journalerna tillgängliga för vårdpersonal på en rad sjukhus och vårdcentraler i Stockholms län och på Gotland. Vården stod stundtals helt utan tillgång till journaler och andra viktiga datasystem. Händelserna fick Inspektionen för vård och omsorg att begära en redogörelse och fallet anmäldes enligt Lex Maria.

IIS anser att det är skrämmande hur låg säkerheten i samhällsviktiga funktioner är. Och hur lite man så här långt har gjort åt det. Samhällsskydd och beredskap handlar om att hela samhället ska kunna klara av såväl mindre incidenter som stora olyckor och kriser. Krisberedskapen syftar till att skydda befolkningens liv och hälsa, samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga rättigheter.

Den grundläggande strukturen för samhällets krisberedskap baseras på den så kallade ansvarsprincipen, vilket innebär att den som bedriver verksamhet under normala förhållanden har motsvarande ansvar även under krissituationer.

Det innebär att verksamheter själva ska ha en organisation som också är riggad för att klara av sina åtaganden vid en eventuell kris. Det finns ofta ett behov av att den som är ansvarig för en verksamhet samverkar, såväl inom sin sektor som utanför, för att kunna lösa uppgiften. Därför innebär ansvarsprincipen också ett ansvar för varje aktör att arbeta tillsammans med andra för att hantera och lösa kriser.

I efterhand kan IIS konstatera att det inte finns någon ansvarig myndighet som ser till att ansvaret hanteras på ett lämpligt sätt. MSB, PTS, och länsstyrelserna har olika uppdrag och olika mandat. Av det skälet **tror IIS** att det skulle underlätta med en IT-haverikommission, i alla fall när något så allvarligt händer, som haverierna hos Tieto och Evry.

Staten har redan flera inspektioner och kommissioner som kontrollerar efterlevnad av statliga normer och regler samt utreder förhållandena vid en olycka eller en katastrof. Statens haverikommission (SHK) är en statlig myndighet som tillkom 1978 för att utreda såväl civila som militära flygolyckor. År 1990 ändrades lagstiftningen så att alla svåra olyckor till lands, till sjöss eller i luften omfattas av i stort sett samma utredningskrav. SHK gör undersökningar enligt lagen (1990:712) om undersökning av olyckor. I lagen anges också att tillbud till en olycka skall undersökas om det kunnat leda till en allvarlig olycka. Kommissionen skall följa den nationella och internationella utvecklingen på områden som omfattas av kommissionens verksamhet och samarbeta med berörda säkerhetsmyndigheter i deras olycksförebyggande verksamhet.

Regeringen har formulerat mål om tillit och tillgänglighet till IT i Sverige. En av svårigheterna med en sådan målsättning är att statistik över och analys av olika typer av incidenter inom data- och telekommunikation är bristfällig. Vanligtvis åtgärdas problemen lokalt, oftast utan rotorsaksanalys av det händelseförlopp som lett fram till att incidenten inträffat eller av de åtgärder som vidtagits för att återställa systemen.

SHK:s olycksundersökningar syftar till att ge svar på tre frågor:

- Vad hände?
- Varför hände det?
- Hur undviks att en liknande händelse inträffar?

SHK hanterar däremot inte frågor om skuld eller ansvar, vare sig civilrättsligt, straffrättsligt eller förvaltningsrättsligt.

Det behövs betydligt högre IT-säkerhet på alla nivåer, från den fysiska infrastrukturen och hela vägen till den enskilde användaren och dennes beteende. Och det behövs definitivt fler insatser för att bygga robustare IT-infrastruktur. Idag verkar inte säkerhet självklart ligga med som en del av kraven. Det ska gå snabbt och vara billigt. Då glömmer man bort åtgärder som att ha separat matning av el, reservkraft och separat kanalisation av ledning. På riktigt. Att fokusera upphandling enbart på pris är att skjuta problemen på framtiden.

Kraven på driftsäkerhet i IT-infrastrukturen är i korthet att den är tillgänglig för användning, att den leder informationen till rätt mottagare, att den ger störningsfri kommunikation och ger underlag för korrekt debitering av de tjänster som utnyttjas.

Länsstyrelsen har tidigare pekat ut tunnelbränder som en allvarlig samhällsrisk för Stockholm – men vad gör man åt det? IT-haverier har ännu kanske inte inneburit direkt skada för person eller sak, men de innebär ändå stora kostnader för samhället. Enligt en forskare på KTH orsakar varje försenad persontimme samhällsekonomiska kostnader på omkring 300 kronor per timme[1], och ett i förlängningen bristande förtroende för kollektiva transporter kan få än större konsekvenser. Med den utvecklingen vi nu ser på området elektronisk kommunikation så torde det bara vara en tidsfråga innan något riktigt allvarligt händer som leder till förlust av mer än bara egendom och pengar.

I en verklighet där samhället blir alltmer beroende av att internet och IT-baserade system fungerar som de ska för att viktiga samhällsfunktioner ska kunna upprätthållas är det rimligt att inrätta en IT-haverikommission, eller låta SHK hantera även IT-haverier för att få en samlad bild av vad som inträffar, och framför allt en möjlighet att upprätta en handlingsplan för att undvika att det händer igen.

För alla andra händelser behöver vi också få igång en process för lärande och återkoppling till samhällets olika aktörer, och då är också ett system med obligatorisk incidentrapportering för statliga myndigheter (och på sikt övrig offentlig sektor) och frivillig dito för den privata sektorn en framkomlig väg.

9.3.1 Kravställning vid upphandling

Som utredningen mycket riktigt påpekar leder lagen om offentlig upphandling till formell begränsning i mångfald bland leverantörer. I informationssäkerhetssammanhang är det direkt kontraproduktivt. **IIS tillstyrker** utredningens slutsatser om behovet av en utvecklad beställarkompetens. **IIS anser** att det är för tidigt att uttala sig om det är positivt att ställa krav på skyddsprofiler som följer standarden Common Criteria. Alltför rigida krav på certifiering av produkter blir kostnadsdrivande och riskerar att begränsa utbudet av lämpliga tjänster och produkter.

9.3.2 Fördjupad dialog mellan privat och offentlig sektor

IIS ställer sig positivt till utredningens förslag om en fördjupad dialog mellan privata och offentlig aktörer.

9.4 Säkrare kommunikation i staten

9.4.1 Spårbar tid och statligt nätverk

IIS står bakom de delar av utredningens förslag som rör tillgång till spårbar tid.

Övervakning är en central funktion i alla IT-system och något som alla IT-ansvariga har behov av. **IIS anser sig** emellertid inte kunna ta ställning till inrättandet av ett centralt sensorsystem utan att ha tillgång till en mer detaljerad beskrivning av vilken information som samlas in, hur den ska hanteras och av vem.

IIS ställer sig tveksam till förslaget om en obligatorisk anslutning till Swedish Government Secure Intranet (SGSI).

---

[1] http://computersweden.idg.se/2.2683/1.544472/hog-tid-for-en-it-haverikommission/sida/3/det-far-inte-tillatas-fortsatta

SGSI är säkert bra för de få myndigheter som behöver det, men det är dyrt att införa och ger bara skydd av trafiken mellan de deltagande myndigheterna. Något som **IIS saknar** i utredningen är ett generellt krav på att myndigheter i sin kommunikation - internt, mellan myndigheter och med medborgare, företag och andra organisationer, alltid ska kommunicera säkert. Det borde inte vara föremål för prövning om vilka myndigheter som ska kunna göra det, utan det borde alla göra. **IIS ser hellre** att alla myndigheter använder krypterad kommunikation med stöd av protokoll som HTTPS och TLS för all sin kommunikation och då använder etablerade öppna kryptolösningar än att några få använder specialiserade lösningar medan de andra fortsätter att kommunicera i klartext och icke-autentiserat.

Att förmå alla myndigheter att använda kryptering vid kommunikation med stöd av HTTPS och TLS skulle **som IIS ser det** lyfta den allmänna säkerhetsnivån rejält. Det skulle också sätta press på utvecklingen inom andra sektorer i samhället som kommuner, företag et cetera och därmed stödja en allmän höjning av skyddsnivån.

Inte minst borde detta ske för industriella kontrollsystem (så kallade SCADA-system) och andra typer av anslutna enheter (Internet of Things) liksom övriga tänkbara tekniska system.

Myndigheterna måste ha tillgång till transporttjänster på IP-nivå med goda prestanda vars tillgänglighet är anpassad efter myndigheternas krav. I början av 2000-talet tillgodosågs detta med Statskontorets upphandlingar av internettjänster. En generell specifikation för internettjänst formulerades gemensamt av Statskontoret och IT-kommissionen. Dessvärre har den inte förvaltats och underhållits. PTS har uttalat en ambition att uppdatera den generella specifikationen men har inte genomfört någon sådan översyn.

Statliga myndigheter ska, baserat på internetstandarder och -teknik, kunna kommunicera säkert myndigheter emellan samt med övriga delar av offentlig förvaltning, medborgare, företag och andra. Målsättningen borde vara att säker kommunikation ska skapas i den öppna IT-infrastrukturen, inte att skapa en parallell infrastruktur. Att staten skulle vara bättre på att driva infrastruktur än de operatörer som finns på den öppna marknaden är inte troligt. Däremot är det fullt möjligt att skapa ett virtuellt nät med användning av en eller flera operatörers nät. I det virtuella nätet bör det finnas en gemensam *distribuerad* brandväggslösning med en gemensam grundsäkerhetspolicy. Att den är distribuerad (och inte centraliserad) innebär att man undviker problem **om** det skulle visa sig att en myndighet bryter mot den gemensamma policyn. Skulle en myndighet upprätta en bakdörrsförbindelse till internet från det egna systemet skulle det påverka en *central* brandvägg så att alla system utsätts för samma risk för intrång. En distribuerad brandväggslösning innebär att bara den aktuella myndigheten kan drabbas av problem.

På varje enskild myndighet måste det lokala IP-nätet implementeras korrekt. För att underlätta myndigheternas arbete ska det finnas en centralt definierad *lokal* IP-grundtjänst, med angiven funktion, tillgänglighet och prestanda. För att en myndighets lokala nät ska få ingå i myndighetsstrukturen totalt (det vill säga ingå i det virtuella nätet) måste det uppfylla dels kraven för IP-grundtjänst, dels krav på grundsäkerhet enligt en gemensam säkerhetspolicy. Där ingår frågor som behörighetskontroll, brandväggsimplementation, krav på tunnling av trafik mellan myndigheter et cetera.

9.4.2 säkra kryptografiska funktioner

IIS delar utredningens uppfattning att den svenska kryptoindustrin är av nationellt intresse och måste stödjas. **IIS saknar** dock ett resonemang kring bättre möjligheter till innovation på området, i dagsläget upplevs det som väldigt byråkratiskt och tungrott.

Utredningen föreslår att regeringen uppdrar åt ett par myndigheter med kopplingar till försvaret att ta fram säkra kryptografiska funktioner. Dessutom ska man besluta vilka myndigheter som ska få rätt att kommunicera säkert med de funktioner som erbjuds. **IIS saknar** ett resonemang kring de öppna, internationella processer där nya kryptoalgoritmer och -tekniker utvecklas, bland annat inom Internet Engineering Task Force (IETF).

IIS noterar att man från ansvariga myndigheters (FRA, MSB och FMV) verkar anse att det är av stor vikt att man använder egenutvecklade krypton inklusive implementationer av dessa, och att detta förutsätter att det finns företag som ska leverera dessa. Detta innebär om IIS tolkar avsnitt 9.4.2 rätt att ett antal bolag ska underhållas med uppdrag i första hand för att bibehålla kompetens, inte för att täcka ett faktiskt utrustningsbehov. Tidigare försök i den riktningen har visat att det inte är en framkomlig väg.

Bra kryptografiska funktioner i civila sammanhang utvecklas över flera år granskade av många ögon från flera olika länder, inte av några få individer i en mer eller mindre statligt kontrollerad verksamhet. **IIS ställer sig frågan** om inte alla myndigheter alltid borde sträva efter att kommunicera säkert?

Vidare blir det **enligt IIS uppfattning** svårt att validera implementationerna och de blir troligen inte kostnadseffektiva. Att stötta ett fåtal svenska företag med uppdrag för att de ska kunna bibehålla kompetensen riskerar dessutom att snedvrida konkurrensen.

Att försvaret och de myndigheter som ligger inom den sektorn anser att de behöver använda egna kryptografiska funktioner är inte kontroversiellt, men att hela den civila statsapparaten skulle ha samma behov **anser IIS vara tveksamt.**

Bilaga 4 i utredningen ger **enligt IIS** en bra bakgrundsbeskrivning till användningen av kryptografiska funktioner i det civila samhället. Bilagan ger även en bra bakgrund till de problem som kan uppstå. Den är dock helt fokuserad på kryptografiska funktioner och skydd utifrån ett militär- och totalförsvarsperspektiv.

Som utredningen också skriver i en fotnot Termen ”Säkra kryptografiska funktioner” definieras i krisberedskapsförordningen SFS (2006:942) 4§ som ”kryptografiska funktioner godkända av Försvarsmakten". Det vill säga endast svenska krypton kommer i fråga. Man förbigår alltså den utveckling av öppna kryptografiska funktioner som sker inom exempelvis EU med ECRYPT-projekten och andra internationella samarbeten.

Vidare avspeglas i utredningen en stark tro på att CC-evalueringar (Common Criteria) ger bra assurans om att kryptoimplementationer fungerar. **IIS vill här betona** att något vi borde ha lärt oss av Snowdens och liknande avslöjanden är att CC-evalueringar och CMVP-stämplar[2] från NIST inte behöver betyda så mycket.

I betänkandet föreslår utredningen att Sveriges Certifieringsorgan för IT-säkerhet (CSEC) som etablerades efter ett regeringsbeslut år 2002 ska godkänna de kryptolösningar som myndigheterna ska använda. Det man inte nämner i sammanhanget är att både CSEC och Militära underrättelse- och säkerhetstjänsten (MUST) som båda gör evalueringar är överbelastade redan i dagsläget. Det tar bokstavligen år att evaluera en ny produkt, och då har

[2] http://csrc.nist.gov/groups/STM/cmvp/

den produkten antagligen kommit ut i en ny version. Om man beslutar i denna **riktning förutsätter IIS att** det sker en rejäl förstärkning av både CSEC och MUST.

Slutligen **saknar IIS** mer i utredningens betänkande om vad de kryptografiska funktionerna ska användas till, och att bland annat staten måste bli bättre på att använda befintliga säkerhetsprotokoll för internetkommunikation som exempelvis TLS (https) och end-to-end-kryptering av innehåll.

9.5 Incidentrapportering

IIS är positivt till förslaget om obligatorisk it-incidentrapportering för samtliga statliga myndigheter. Det är ett förslag som framförts flera gånger i tidigare utredningar, men aldrig genomförts.

9.6 Brottsbekämpning

9.6.1 It-brottskonventionen

I denna del hänvisar utredningen till en annan offentlig utredning vars betänkande ”Europarådets konvention om it-relaterad brottslighet”, SOU 2013:39, innehåller förslag till vilka åtgärder Sverige behöver vidta inom bland annat författningsområdet för att kunna ratificera Europarådets konvention om IT-relaterad brottslighet från 2001. Vissa författningsändringar har med anledning av konventionen redan ägt rum, exempelvis införandet av brottet grovt dataintrång. Någon ratificering har dock inte skett och Sverige är nu en av få medlemsstater som inte har ratificerat konventionen. Därmed saknar Sverige flera av de instrument och verktyg som förväntas av oss som samarbetspart och medlemsstat inom EU.

IIS har inte tagit del av den SOU som utredningen hänvisar till och känner inte att vi har tillräcklig kunskap för att kunna ta ställning till om IIS ska ställa bakom utredningens förslag i den delen. **IIS förhåller sig därför neutralt till** förslaget om ratificering av Europarådets konvention om it-relaterad brottslighet.

9.6.2 Informationsutbyte

IIS ställer sig avvaktande till förslaget om tydligare reglering i offentlighets- och sekretesslagen för uppgifter som utbyts vid samverkan mellan brottsbekämpande myndigheter.

I betänkandet står att Polismyndigheten har uppmärksammat utredningen på att det föreligger svårigheter när en brottsbekämpande myndighet ser ett behov av att delge samverkande myndigheter information och att det finns situationer då Polismyndigheten behöver delge en annan myndighet underrättelseinformation men samtidigt bedömer att sekretess alltjämt bör råda. Man menar att en reglering i offentlighets- och sekretesslagen (2009:400) avseende överföring av sekretessen skulle förenkla delgivningen av information.

NISU-utredningen har alltså fått denna information direkt från polisen om att det finns problem i att vissa uppgifter skulle behöva lämnas ut till annan myndighet. Här borde kanske utredningen **enligt IIS** på egen hand tagit reda på det reella behovet av informationsutbyte mellan myndigheterna, och inte bara ta polismyndighetens ord på att ett sådant behov existerar.

9.6.3 Översyn av bestämmelser om tvångsmedel i den digitala miljön

IIS är positivt till förslaget om en översyn av bestämmelserna om tvångsmedel i 27 och 28 kap. rättegångsbalken och övriga lagrum för att säkerställa att brottsbekämpande myndigheter kan bedriva sin förebyggande och utredande verksamhet i den digitala miljön. **IIS uppmanar** dock regeringen att ta intryck av de synpunkter som framförts i remissen över utredningen Datalagring och integritet, SOU 2015:31. Det är viktigt att införandet av sådana åtgärder föregås av en ytterst noggrann avvägning mellan å ena sidan rätten till privatliv och skyddet av personuppgifter och å andra sidan behovet att bekämpa allvarlig brottslighet och upprätthålla allmän säkerhet.

9.7 Internationella och regionala relationer

IIS har inget att invända mot utredningens förslag i dessa delar.

9.8 Övriga förslag

9.8.1 Framtida övningsutveckling inom information- och cybersäkerhetsområdet

IIS är positivt till förslaget om fortsatt och förstärkt övningsverksamhet inom informations- och cybersäkerhetsområdet. I sammanhanget bör ett större fokus läggas på internetrelaterade störningar.

9.8.2 Fördjupad dialog om kompetensförsörjning

IIS delar utredningens bild av att det saknas kompetens på området. Huruvida en fördjupad dialog är en tillräcklig åtgärd för att komma till rätta med bristen är tveksamt**. Generellt anser IIS** att universitet och högskolor misslyckas med att lära ut tillräckliga säkerhetskunskaper och man examinerar studenter som i stort sett innebär en potentiell risk för varje organisation som rekryterar dem. Många av dagens studenter har kanske en abstrakt uppfattning om informationssäkerhet, men hur många kan faktiskt ens identifiera en bilagd fil som innehåller skadlig kod, ett mer sofistikerat nätfiskeförsök eller tolka resultaten från ett penetrationstest?

Man kan ju ställa sig frågan vad vitsen är med att skicka ut fantastiska utvecklare och webbdesigners om de inte har en aning om hur de ska designa någonting som också är säkert? Security by design är ett eftersatt område som **enligt IIS mening** behöver ingå i all informationstekniskt relaterad utbildning.

Vidare behövs det särskild kompetens för utredning av brott med anknytning till informationsteknik och det **bör ju enligt IIS** höra hemma på Polishögskolan. I många andra länder har det behovet lett till att man inrättar specialiserade funktioner inom polisorganisationerna, där man samlar personer med nödvändiga kunskaper för utredning av IT-relaterad brottslighet. Här har vi i Sverige också sett en tillväxt på både efterfrågan och utbud när det gäller utbildning i forensisk analys.

10 Konsekvenser av förslagen

IIS är av den bestämda uppfattningen att informations- och IT-säkerhet kostar och att vidta de åtgärder som utredningen föreslår är definitivt förenat med kostnader för staten. Huruvida finansieringen ska ske inom ramen för befintlig budget eller med tillskott av nya medel och

resurser **har IIS inga åsikter** om. Sker det inom ramen för befintlig budget måste förmodligen något annat stryka på foten. Går det att hitta tillräckligt många uppgifter som myndigheterna har idag men som inte längre behöver utföras och där pengarna kan läggas på arbete med informationssäkerhet så är det positivt. **IIS vill betona att** kostnaderna i sig inte får anses utgöra ett hinder för genomförandet.

Det är också av stor vikt att forskning bedrivs på områdena informations- och cybersäkerhet som bland annat gör det möjligt att identifiera och analysera nya hot så att dessa tas om hand på ett effektivt sätt. Det är ett budskap som regeringen bör ta med sig i arbetet med den forskningsproposition som ska läggas fram 2016.

Danny Aerts, vd

Bilaga 1. Tidigare utredningar och rapporter med IT- och informationssäkerhet i fokus

1. Dataskydd, rapport 1975:9 och 1976:38 från Statskontoret
2. Sårbarhetskommittén - SÅRK, tillsatt 1976 - utredde frågan om datasystemens sårbarhet och föreslå åtgärder i syfte att minska denna.
    a. Lägesrapport 1978 - ADB och samhällets sårbarhet
    b. SÅRK, SOU 1979:93, ADB och samhällets sårbarhet - överväganden och förslag
3. Datasäkerhet ur ett svenskt perspektiv, DAS 90, förstudierapport, Statskontoret/Utvecklingsrådet, 1990-06-14
4. Myndigheternas säkerhetsanalyser av sina ADB-system, Statskontoret, regeringsuppdrag 617/91-5, rapport 1991-12-05
5. ADB-säkerhet i Sverige: VAd som gjorts och vad som pågår. Resultat av inventering februari 1992, Statskontoret/ÖCB 1992.
6. Samrådsgruppen för samhällets säkerhet inom dataområdet - SAMS, C 1986:G, 1993-06-30).
    a. SAMS-rapport DS 90:43 ”De verksamhetsansvarigas säkerhetsansvar"
    b. SAMS-rapport DS 90:44 ”Samhällsaspekter på säkerheten inom betalningsväsendet”
    c. SAMS-rapport Informationssystemens säkerhet i samhället på 90-talet. Revisionens roll och förutsättningar för att stärka informationssystemens säkerhet, SAMS 1993-06-23
    d. SAMS-rapport Informationssystemens säkerhet i samhället på 90-talet. En effektiv organisation i samhället för informationssystemens säkerhet, SAMS slutrapport, 1993-06-30
7. Svenska delen av Internet, Struktur, säkerhet och regler, Statskontoret 1997:18
8. ADB-säkerhet vid åtta statliga myndigheter - en uppföljningsstudie, Statskontoret 1998:5
9. Förslag till svenska insatser rörande informationssäkerhet, Slutrapport från CITI-projektet, IT4-projekt nr 4112, 1992-06-24.
10. Ett säkrare samhälle, Huvudbetänkande, Hot- och riskutredningen, SOU 1995:19
11. Åtgärder för att bredda och utveckla användningen av informationsteknik, Prop 1995/96:125, Statsrådsberedningen
12. Åtgärder för att bredda och utveckla användningen av informationsteknik, Försvarsutskottets yttrande 1995/96:FöU4y i 1995/96:TU19
13. Beredskapen mot svåra påfrestningar på samhället i fred, prop 1996/97:11, Försvarsdepartementet
14. Statlig förvaltning i medborgarnas tjänst, prop. 1997/98:136, Finansdepartementet
15. Utvecklingen i informationssamhället, Regeringens skrivelse 1997/98:19, Kommunikationsdepartementet
16. Regeringens och myndigheternas befogenheter vid svåra påfrestningar på samhället, Ds 1996:4, Försvarsdepartementet
17. Elektronisk dokumenthantering, betänkande av IT-utredningen, SOU 1996:40
18. Informationskvalitet i offentlig verksamhet, Toppledarforum, Riksskatteverket, Dnr 8904-97/920, 1997-11-12

19. Informations-/datasystem inom civila försvaret - säkerhetskrav - utvärdering och driftgodkännande, ÖCB 5-1613/95, december 1996
20. Datasystemsäkerhet, analys av ett antal samhällsviktiga datasystem inom Uppsala län, ÖCB, 1997:12
21. Säkerhetshöjande åtgärder för samhällsviktiga datasystem inom civila delen av totalförsvaret - redovisning av uppdrag, ÖCB
22. Ds 1998:32, Arbetsgruppen Ledningskedjan (Fö1997:F) utredning om bl.a. de frågor om skyldigheter och befogenheter vid svåra påfrestningar på samhället i fred för den s.k. ledningskedjan - regering, civilbefälhavare (vid höjd beredskap), länsstyrelser, landsting och kommuner - som behandlas i försvarsutskottets betänkande 1996/97:FöU5.
23. Riksrevisionsverket (Rätt data? revisionsrapport, Riksrevisionsverket, Dnr 1989:393)
24. Fel data kostar!, Riksrevisionsverket F 1992:2
25. Kvalitetssäkrad informationsförsörjning i offentlig förvaltning, QVALIT, Toppledarforum, ÖCB, 1996
26. Rapport nr 1 om åtgärder och skydd mot informationskrigföring, regeringens arbetsgrupp för informationskrigföring AgIW, PM 13/97.
27. Kryptopolitik - möjliga svenska handlingslinjer, Regeringskansliets referensgrupp för krypteringsfrågor, rapport Oktober 1997
28. Datorrelaterade missbruk och brott - en kartläggning gjord av Effektivitetsrevisionen, Riksrevisionsverket RRV 1997:33
29. Sammanhållen strategi för samhällets IT-säkerhet, Statskontoret 1998:18
30. Telelagen och Internet, Post- och Telestyrelsen, PM 1998-04-08, Dnr 98-6923
31. 2000, Arbetsgruppen för skydd mot informationsoperationer (Ag IO)
32. SOU 2000:30, Domännamnsutredningen
33. PM 1:2001, IT-kommissionen, Observatoriet för Informationssäkerhet, Grundskydd i datorer och programvaror http://www.itkommissionen.se/doc/24.html
34. Skrivelse till regeringen: http://www.itkommissionen.se/doc/222.html
35. SOU 2001:41, Säkerhet i en ny tid, Sårbarhets- och säkerhetsutredningen
36. SOU 2002:60, Lag om elektronisk kommunikation
37. Post- och telestyrelsens rapport "Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering" (PTS dnr 99-15420/62)
38. PTS 2001-12-15, Internets robusthet https://www.pts.se/upload/Documents/SE/Internets%20robusthet.pdf
39. Proposition 2001/02:158, Samhällets säkerhet och beredskap angående informationssäkerheten i samhället.
40. 39/2001, IT-kommissionen, Observatoriet för informationssäkerhet, Hantering av IT-incidenter, vem gör vad och hur? http://www.itkommissionen.se/doc/94.html
41. SOU 2002:109, Delbetänkande av utredningen om elektronisk kommunikation, Myndighetsfrågor m.m.
42. SOU 2002:87, Rikets säkerhet och den personliga integriteten, betänkande från Säkerhetstjänstkommissionen.
43. PTS-ER-2003:1, Är Internet i Sverige robust?
44. PTS-ER-2003:34, ISSN 1650-9862, Vilket informationsbehov har Internetanvändare vid störningar i Internettrafiken?
45. SOU 2003:11, System för samordnad krisinformation
46. SOU 2003:27, Signalskydd - delbetänkande från InfoSäkutredningen
47. SOU 2003:32, Vissa riksdagsbeslut m.m. efter 11 september 2001

48. SOU 2003:59, Toppdomän för Sverige
49. SOU 2004:25, Informera om samhällets säkerhet, Utredningen om översyn av totalförsvarsinformation
50. SOU 2004:32, Informationssäkerhet i Sverige och internationellt - en översikt. Delbetänkande från Infosäkutredningen
51. SOU 2005:42, Säker information - förslag till informationssäkerhetspolitik. Delbetänkande från Infosäkutredningen.
52. SOU 2005:71, Informationssäkerhetspolitik - organisatoriska konsekvenser. Slutbetänkande från Infosäkutredningen
53. PTS-ER-2006:12, Strategi för ett säkrare Internet i Sverige
54. SOU 2007:31 Alltid redo! En ny myndighet mot olyckor och kriser
55. SOU 2007:47: Den osynliga infrastrukturen - om förbättrad samordning av offentlig IT-standardisering
56. 2007: PTS förslag till allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid
57. 2007: PTS rapport, Utveckling av Sitic, Sveriges IT-incidentcentrum
58. SOU 2007:76 Lagring av trafikuppgifter för brottsbekämpning
59. Interpellation i riksdagen 2008/09:71 Handlingsplan för samhällets informationssäkerhet
60. PTS-ER-2009:25 2009-07-08, Robust elektronisk kommunikation, Strategi för åren 2009-2011
61. 2009: Förstärkt integritetsskydd vid signalspaning
62. SOU 2009:86, Strategi för myndigheternas arbete med e-förvaltning
63. MSB 2009, MSBFS 2009:10 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet
64. MSB, 2010, Strategi för samhällets informationssäkerhet 2010-2015
65. 2011, It i människans tjänst - en digital agenda för Sverige. Diarienummer 2011/342/ITP
66. PTS-ER-2011:16, 15 juni 2011, Robust elektronisk kommunikation, vägledning för användare vid anskaffning
67. PTS-ER-2012:8 2012-06-15, Robust elektronisk kommunikation, Strategi för åren 2012-2014
68. MSB, Nationell handlingsplan för samhällets informationssäkerhet 2012.
69. MSB, Strategi för informationssäkerhet i e-förvaltning, 2014
70. MSB, Statusrapport om arbetet med Nationell handlingsplan för samhällets informationssäkerhet, 2014.
71. MSB, En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter
72. Riksrevisionen, RIR 2014:23, Informationssäkerheten i den civila statsförvaltningen
73. En ny säkerhetskyddslag, SOU 2015:25
74. Informations- och cybersäkerhet i Sverige, SOU 2015:23
75. Ett fungerande samhälle i en föränderlig värld - Nationell strategi för skydd av samhällsviktig verksamhet, MSB 2011
76. Vägledning för samhällsviktig verksamhet - Att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid