IT-kommissionen
K 1998:04
Anne-Marie Eklund Löwinder
Tel 08-405 33 67

2001-08-15
Fö 2001/175/ZIV
ITK 2001/57

Till Regeringen
(Försvarsdepartementet)

Remissyttrande - Sårbarhets- och säkerhetsutredningens betänkande Säkerhet i en ny tid (SOU 2001:41)

Allmänna synpunkter

IT-kommissionens svar omfattar allmänna synpunkter endast i de delar som avser strategi för ökad IT-säkerhet och skydd mot informationsoperationer, samt utredningens förslag om en planeringsmyndighet.

Riksdag och regering har som utredaren påpekar i sin rapport det övergripande strategiska ansvaret för samhällets informationsförsörjning, IT och informationssäkerhet främst när det gäller samhällsviktiga funktioner. Genom att formulera en tydlig strategi kan riksdag och regering ange inriktningen på och de övergripande målen för arbetet och rekommendera en önskad säkerhetsnivå.

IT-kommissionen är av uppfattningen att säkerhetsfrågorna borde vara högre prioriterade i ett modernt samhälle som Sverige. Utvecklingen av informationssamhället har skapat en förändrad hotbild, Sverige är beroende av sin IT-infrastruktur för att driva och utveckla olika typer av verksamheter i en global miljö.

Frågor om IT- och informationssäkerhet har varit föremål för utredning sedan början av 80-talet, de flesta förslag har passerat utan åtgärd. Idag är risken stor att konsekvenser av störningar i IT-system blir utomordentligt allvarliga. Allt oftare återkommande, och alltmer omfattande angrepp på IT-system bär vittnesbörd om detta. Även om Internet är extremt motståndskraftigt mot slumpmässiga fel och bortfall av såväl länkar som noder så är nätet ytterst känsligt för en samordnad utslagning av ett fåtal specifika noder. Dessa noder behöver inte vara särskilt många för att någon ska kunna slå ut praktiskt taget hela Internet.

På den nationella nivån är väl fungerande informationssäkerhet viktigt för samtliga samhällssektorer och för medborgares demokratiska rättigheter. Utvecklingen av informationssäkerheten innebär också att medborgarnas rättigheter och intressen kan tryggas effektivare enligt de principer om offentlighet och öppenhet som iakttas inom den offentliga förvaltningen.

Utgångspunkten för regeringens strategi om informationssäkerhet bör vara att varje företag, organisation och myndighet ansvarar för att den egna informationsbehandlingen sker med betryggande säkerhet. Denna ansvarsprincip har varit gällande i Sverige så länge som verksamheter använt informationsteknik, och den gjordes tydlig under 1980-talet bl.a. genom ett uttalande av den dåvarande dataministern Bo Holmberg (s).

En väl formulerad strategi för informationssäkerhet har ett stort symbolvärde för såväl offentlig sektor som för näringslivets och medborgarnas synsätt på dessa frågor. Strategin ska vara teknikoberoende, men den måste ändå

baseras på kännedom om tekniken och dess dynamiska utveckling. Med hänsyn till utvecklingstakten bör den också uppdateras regelbundet. IT-kommissionen saknar en sådan målsättning i utredningen.

IT-kommissionen anser att utredningen tenderar att måla upp en alltför centralistisk modell för arbetet med IT- och informationssäkerhet. Det är viktigt att det arbete som utförs, utförs lokalt men att det kan samordnas, och att erfarenheter kan spridas. Säkerhetsarbetet kan inte bedrivas centralt i dagens distribuerade informationssystem. Varje incident och situation är given av hur den enskilda miljön ser ut, vilka programvaror och tekniker som används, vilken typ av information som hanteras etc**. IT-kommissionen anser** att man här bör dra nytta av de erfarenheter av samverkan som gjordes i samband med omställningen till år 2000. I stället för att dela upp arbetsuppgifterna vertikalt (s k ”stuprörsprincip”) så bör man organisera arbetet efter den "närprincip" som utredningen framhåller som viktig, dvs. att gå från det lokala, till det centrala, där de föreslagna funktionerna utgör en samordnande och vägledande kraft, inte en verkställande och dominerande.

När det gäller statens möjligheter att utforma en strategi för informationssäkerhet i samhällets informationsförsörjning är det **enligt IT-kommissionen** viktigt att ta hänsyn till statens olika roller, vilket Statskontoret också betonade i sin utredning 1998. Å ena sidan formulerar statsmakterna normer och regler för samhället som helhet, å andra sidan utgör staten en stor och viktig användare i samhällets informationsförsörjning. Detta ger delvis olika utgångspunkter för de olika åtgärder som kan vidtas. För statlig verksamhet kan regeringen utforma strategin inom ramen för sin behörighet och med beaktande av den lagstiftning som gäller för berörda myndigheter. För privat verksamhet, kommuner och landsting fordras det att regeringen har stöd i lag för att förordna om informationssäkerhet. Enligt IT-kommissionen påtalar utredningen här på angelägna förändringar i lagstiftningen.

Viktigt att notera är att säkerheten i samhällets informationsförsörjning inte är en angelägenhet enbart för den offentliga förvaltningen, utan för hela samhället. Det kommunala självstyret är emellertid starkt och inriktningen på regeringens åtgärder måste sannolikt bygga på samverkan och frivillighet. Det privata näringslivet utgör också en viktig beståndsdel av samhällsstrukturen i dessa frågor. Bred samverkan är nödvändig i såväl det pågående som det fortsatta arbetet. Därför fanns det också i Statskontorets förslag en strävan om att finna en struktur där regeringen kan samverka med alla delar av samhället - kommuner, landsting och näringsliv - på frivillig väg för att bygga upp en nödvändig struktur för informationssäkerhet.

IT-kommissionen vill betona att sådan samverkan kräver att den föreslagna planeringsmyndigheten, som också föreslås utgöra kansli åt det föreslagna samordningsorganet, är öppen och flexibel i kontakter med omvärlden, och att den är bemannad med personal som har både god teknisk kompetens och säkerhetskompetens.

Förslag om en planeringsmyndighet

IT-kommissionen är positiv till förslaget att samordna resurserna på IT-säkerhetsområdet**. IT-kommissionen anser** dock att utredningen inte löper linan ut. De förslag som läggs fram innebär **enligt IT-kommissionens uppfattning** relativt små förändringar i förhållande till nuvarande struktur, samtidigt som nya funktioner föreslås inrättas i nära anslutning till befintliga myndigheter, varvid man löper en risk att öka splittringen av ansvarsfördelningen och den formella trögheten på området. Skälet är det som anförs ovan, under allmänna synpunkter, om att en horisontell orientering är att föredra framför en vertikal, när det gäller fördelning av arbetsuppgifter.

IT-kommissionen vill betona att alla verksamheter, inklusive statsmakten, har ett intresse av att samhällets informationsförsörjning är säker och håller en tillräckligt hög kvalitet. Incidenthantering som exempel, är långt ifrån en formell process. De olika organ som finns på olika nivåer inom Internet samarbetar och bygger upp nätverk av förtroende och kompetens, och hjälper varandra med lokal kännedom och personliga kontakter när någonting inträffar. Den snabbhet med vilken olika händelser måste mötas förutsätter informella strukturer och kontaktvägar. Incidentrapportering kan ge information om inträffade, oönskade händelser. Den kan ge underlag för bedömning av nya åtgärder, nya typer av händelser, trender etc. I dag finns ingen riktig överblick över vare sig vilka incidenter som inträffar eller vilka konsekvenser dessa får. Därmed blir det svårt att på ett övergripande plan genomföra några analyser och veta vilka säkerhetsåtgärder som är relevanta i en enskild verksamhet, än mindre för en hel sektor som t.ex. den statliga förvaltningen. De olika nationella funktioner som föreslås måste fungera väl sinsemellan.

På den tekniska sidan har många framsteg gjorts på säkerhetsområdet. Däremot har ansvariga organ och ansvariga i organisationer vare sig de resurser eller den kompetens som behövs för att säkra och skydda den information som finns i systemen. Ett av problemen är den ständigt föränderliga tekniken och därmed förändrade hotbilden. En annan av orsakerna är att problemen inte är helt lokala. Om någon attackerar och bryter sig in i ett svenskt system, så kan det vara såväl individer i Sverige som någon eller några som sitter på andra sidan jordklotet. Det kan också vara konsekvensen av användning av viss programvara och därmed också mer tekniskt än geografiskt betingat.

Karaktären på Internetanvändare har ändrats radikalt senaste åren. Varje enskild användare har, trots att de blir allt mer erfarna som användare, allt lägre teknisk kompetens och säkerhetskompetens. Stora insatser måste göras för att sprida och öka kunskaperna om IT- och informationssäkerhet.

Det är som flera tidigare utredningar påpekat viktigt att få till stånd en organisation där IT-säkerhetsarbetet kan koordineras**. IT-kommissionen anser** att det inte är helt enkelt att ta ställning till förslaget om inrättandet av de olika funktioner som föreslås utgående från utredningens rapport. **IT-kommissionen tillstyrker förslaget** om att tillsätta en organisationskommitté för att tydligare beskriva planeringsmyndighetens roll, uppgifter och relation till andra aktörer. Det måste klart preciseras var ansvaret för olika säkerhetsfrågor ligger inom statsförvaltningen. Det finns en utbredd känsla av osäkerhet om vem som tar ansvar för att vidta åtgärder om någon allvarligare incident verkligen inträffar.

Det räcker dock inte med att bara fördela ansvar utan det krävs tydligt formulerade mål och utvecklade metoder för granskning av om målen uppfylls. Målen för arbetet med informationssäkerhet måste också anpassas till lagstiftningen och till de internationella standarder som successivt utarbetas.

Åtgärder för att skydda information underlättas genom en samordnad utveckling av kunskap om informationssäkerhet, krav på informationssäkerhet i upphandlingar av IT-utrustning och -tjänster, användning av kryptering, funktioner för säker identifiering och digitala signaturer samt användning av öppna standarder, krav på certifiering och förekomsten av frivilliga branschvisa eller sektorsvisa överenskommelser.

En del av detta kan läggas på marknaden efter det att användarna (stat, kommun, näringsliv) i upphandlingar riktat relevanta och kvalificerade krav på funktioner, tjänster och produkter som krävs för att höja säkerhetsnivån i de egna systemen. Det kan nämnas i sammanhanget att IT-kommissionen har framställt två sådana kravspecifikationer, Generell specifikation av Internettjänst samt Grundskydd för persondatorer.

För IT-kommissionen

Christer Marking
kanslichef