

Underlag 2.

Direktiv till två pågående utredningar som har bäring på informationssäkerhet

Under denna gransknings gång har två pågående utredningar haft i uppdrag att hantera mer övergripande frågor som rör styrning och kravställning av informationssäkerhet. Här lämnas en beskrivning av utredningarnas uppdrag.

En modern säkerhetsskyddslag¹

En särskild utredare har i uppdrag att göra en översyn av säkerhetsskyddslagstiftningen. Syftet är främst att bättre anpassa lagstiftningen till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet och till de krav det internationella samarbetet ställer. Som ett delområde i utredningen ska utredaren föreslå hur reglerna om informationssäkerhet, som är en del av säkerhetsskyddet, bör vara utformade.

Regeringen anför i utredningsdirektiven att bestämmelserna om informationssäkerhet i dag uteslutande är inriktade på att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet. Lagen ger därför små möjligheter att vidta åtgärder för att skydda IT-systemen som sådana. Samtidigt har utvecklingen på IT-området inneburit att vissa informationssystem för bland annat styrning, reglering och övervakning, till exempel inom energiförsörjningen, fått en allt större betydelse för rikets säkerhet. Det gäller oavsett om det i systemen hanteras uppgifter som omfattas av sekretess som rör rikets säkerhet. Avgränsningen av säkerhetsskyddslagens bestämmelser om informationssäkerhet till åtgärder som behövs för att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet framstår alltså inte längre som ändamålsenlig.

Regeringen anför vidare att det vid sidan av Säkerhetspolisens arbete med informationssäkerhet enligt säkerhetsskyddslagen finns flera myndigheter som är verksamma inom informationssäkerhetsområdet med stöd av andra författningar. Det är därför enligt regeringen angeläget att den samlade kompetens som finns vid de myndigheter som utför uppgifter på informationssäkerhetsområdet kan utnyttjas på ett effektivt och ändamålsenligt sätt. Utifrån bland annat dessa behov får utredaren i uppdrag att

- föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade
- med beaktande av övrig rättslig reglering på informationssäkerhetsområdet, utarbeta nödvändiga författningsförslag.

Vad gäller tillsynen av säkerhetsskyddet anför regeringen att det i dag inte finns några sanktionsmöjligheter för tillsynsmyndigheterna att tillgå. Det

¹ Dir. 2011:94.

finns inte heller någon skyldighet att anmäla inträffade säkerhetsincidenter till tillsynsmyndigheten i andra fall än där en hemlig uppgift har röjts, om röjandet kan antas medföra men för rikets säkerhet som inte är ringa. Regeringen anför vidare att den ökade internationaliseringen och informationsteknikens utveckling ställer nya krav på säkerhetsskyddet och därmed även på tillsynen. En förutsättning för att reglerna om säkerhetsskydd ska få det genomslag som är avsett är att tillsynen kan ske på ett effektivt och ändamålsenligt sätt. Det är också enligt regeringen viktigt att den samlade kompetens som finns hos de myndigheter som har tillsyns- och kontrollansvar på säkerhetsskyddsområdet kan utnyttjas på ett effektivt sätt.

Utredaren ska därför även

- analysera hur Säkerhetspolisens och Försvarsmaktens tillsyn över säkerhetsskyddet bör vara utformat, bl.a. i förhållande till de sektorsansvariga myndigheternas kontroll
- ta ställning till om ett system med sanktionsåtgärder bör införas och i sådant fall hur det bör utformas
- utarbeta nödvändiga författningsförslag.

Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system²

En särskild utredare har i uppdrag att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system. Utredningen förkortas NISU 2014.

Utredaren ska

- föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och IT-system
- föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig IT-infrastruktur
- klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt av sådana som används i förslaget till nationell strategi
- med utgångspunkt i uppdraget redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Nuvarande ansvarsförhållanden och åtaganden ska beaktas men inte begränsa utredningen, som ska utgå från ansvarsprincipen och gällande ekonomiska ramar. De begrepp eller benämningar som används i dessa direktiv ska inte föregripa eller begränsa utredarens arbete.

Regeringen anför i utredningsdirektiven att myndigheternas arbete med informationssäkerhet ska bedrivas utifrån en nationell strategi som tar sin utgångspunkt i att värna befolkningens liv och hälsa, samhällets funktionalitet samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter. Att stärka

² Dir. 2013:110.

samhällets säkerhet kräver att skyddsvärden, hot och skyddsmedel ses i ett sammanhang. Denna helhetssyn bör genomsyra verksamheten över hela kedjan, från orsaksförebyggande och sårbarhetsreducerade till hanterande och återuppbyggande verksamhet.

Strategin ska utgå från, och även kunna bidra till, fortsatt utveckling av politiska prioriteringar på området. Strategin ska innehålla övergripande mål samt utgångspunkter för hur aktörer i samhället ska samverka i arbetet med att förebygga, upptäcka, ingripa mot och agera i samband med allvarliga IT-incidenter som drabbar samhällsviktig verksamhet.

Regeringen anför vidare att informationssäkerhet är en betydelsefull del i arbetet med att nå målen för Sveriges säkerhet och samhällets krisberedskap. Därför bör arbetet med att stärka informationssäkerheten vara en del av det allmänna säkerhets- och krisberedskapsarbetet. För att hålla samman såväl det nationella som det internationella arbetet inom informationssäkerhetsområdet och för att nå Sveriges politiska mål är det viktigt med en nationell strategi som bland annat tar sin utgångspunkt i en bred säkerhetspolitisk kontext. Strategin ska ta sin utgångspunkt i målen för Sveriges säkerhet och målen för samhällets krisberedskap.

De övergripande målen ska utformas så att de ger mål, riktlinjer för och prioriteringar som kan ligga till grund för myndigheternas eget informationssäkerhetsarbete. Den nationella strategin för hantering och överföring av information i elektroniska kommunikationsnät och IT-system ska ses som ett övergripande sammanhållet ramverk för hur arbetet med informationssäkerhet ska bedrivas i Sverige. Det förutsätts att mer nedbrutna detaljerade riktlinjer och handlingsplaner skapas för delområden och sektorer i samhället inklusive det militära försvaret och försvars-underrättelseverksamheten.

Den nationella strategin för hantering och överföring av information i elektroniska kommunikationsnät och IT-system ska hantera risker på alla nivåer i samhället. Informationssäkerhetsområdet är tvärsektorielt och omfattar många aktörer i samhället på lokal, regional och central nivå. Även näringslivet har en stor roll i detta arbete. Till detta kommer också den internationella dimensionen där olika aspekter måste beaktas. Den nationella strategin bör inkludera alla relevanta aspekter och aktörer. Syftet med strategin ska enligt regeringen vara att uppnå ett effektivare och mer samordnat arbete med informationssäkerhet i samhället. Strategin ska vara ett stöd för myndigheternas arbete och kopplas till styrmedel och åtgärder för att åstadkomma ett operativt och verksamt arbete med informationssäkerhet i hela samhället.