Datum
2015-09-08

Diarienr
2015-2930

Ert datum
2015-05-06

Er referens
Ju 2015/2650/SSK

Avdelningen för risk- och sårbarhetsreducerande arbete
Verksamheten för samhällets informations- och cybersäkerhet
Helena Andersson
helena.andersson@msb.se

Regeringskansliet
Justitiedepartementet

103 33 Stockholm

Betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige

Sammanfattning

Myndigheten för samhällsskydd och beredskap (MSB) tillstyrker merparten av de förslag som lämnas i betänkandet. I sin helhet bidrar förslagen till viktiga förbättringar inom ett område som idag uppvisar brister trots att området är grundläggande för hela samhällets funktion.

MSB kan i allt väsentligt ställa sig bakom den föreslagna nationella strategin. Av de sex strategiska målen ser MSB det som särskilt betydelsefullt att förslaget om obligatorisk it-incidentrapportering genomförs skyndsamt.

MSB tillstyrker en utvecklad förordningsreglering om statliga myndigheters informationssäkerhet men den närmare utformningen behöver övervägas ytterligare. När det gäller tillsyn kan det övervägas om inte MSB i ett första skede borde fokusera på att utveckla de centrala åtgärdsförslagen i betänkandet. Därefter kan tillsynsfrågan prövas på nytt.

De nya uppgifter som MSB föreslås få i betänkandet kan komma att kräva större resurser än som beskrivs i utredningen.

Även om MSB ställer sig positiv till utredningens förslag finns det anledning att lämna synpunkter på några av de åtgärder som föreslås för att uppnå de strategiska målen.

Övergripande synpunkter på strategin

MSB instämmer i att det systematiska informationssäkerhetsarbetet hos myndigheterna generellt behöver stärkas. Alla de föreslagna strategiska målen är viktiga för en sådan utveckling.

En grundläggande förutsättning för arbetet är att det kan utgå från och anpassas till en korrekt riskbild. Genom förslaget om att samtliga statliga myndigheter ska rapportera it-incidenter skapas förutsättningar för att kartlägga riskbilden inom statlig verksamhet. För att få en heltäckande riskbild behöver rapporteringen kompletteras med bland annat riskanalyser. Riskbilden behöver omfatta alla typer av risker, inte endast de som kan kopplas till inträffade incidenter.

Särskilda synpunkter med koppling till de olika åtgärdsförslagen

MSB tillstyrker i stort utredningens förslag på åtgärder som stöd för att uppnå de olika strategiska målen. Myndigheten har dock synpunkter på utformningen av vissa av åtgärderna.

Nationell styrmodell

MSB delar utredningens syn på att det behövs en starkare styrning och uppföljning av hur informationssäkerhetsarbetet bedrivs hos statliga myndigheter, inte minst av det skälet att e-tjänster ställer nya krav på myndigheternas arbete. När det gäller den nationella styrmodellen, som på sikt kan utsträckas till att omfatta hela offentliga sektorn, bör därför inte syftet med en sådan modell vara att skapa en gemensam syn på en lägsta nivå, så som föreslås i utredningen, utan istället bör det vara att skapa former för att på ett standardiserat sätt ställa krav och realisera säkerhetslösningar på olika nivåer.

Frågan om inrättande av ett myndighetsråd för informationssäkerhet

MSB delar utredningens uppfattning om betydelsen av den samordning som nu sker genom en grupp av myndigheter med särskilda uppgifter inom området informationssäkerhet (SAMFI). Arbetet som idag sker inom detta forum kommer att bli ännu viktigare i framtiden vilket påverkar både formerna för och innehållet i arbetet. Det kan därmed vara en fördel om regeringen på ett tydligare sätt än idag markerar forumets betydelse och MSB:s roll.

MSB ställer sig dock tveksam till utredningens förslag om hur ett nytt myndighetsråd skulle kunna etableras. Beskrivningen av myndighetsrådet och dess uppgifter i den föreslagna nya förordningen är alltför detaljerad och samtidigt oklar.

Istället för att reglera ett nytt myndighetsråd i förordning som utredaren föreslår anser MSB att myndigheten bör ges i uppdrag att inrätta och ansvara för ett myndighetsråd med utgångspunkt i det samordningsarbete som hittills bedrivits. Ett sådant uppdrag skulle kunna ha en liknande utformning som det regeringsuppdrag MSB fick 2013 rörande den nationella arbetsgruppen för sprängämnessäkerhet. Arbetet med utformningen av myndighetsrådet bör ske i samverkan med nuvarande SAMFI-myndigheter. Arbetet bör inkludera analys

av arbetssätt, uppgifter och möjligheterna att utöka antalet deltagande myndigheter med exempelvis Svenska kraftnät.

En ny förordning om statliga myndigheters informationssäkerhet

MSB anser att det är bra att bryta ut de nuvarande reglerna om informationssäkerhet ur förordningen (2006:942) om krisberedskap och höjd beredskap och ersätta dem med en utbyggd reglering av informationssäkerhetsområdet i en ny förordning. Det förslag till en sådan förordning som lämnas i betänkandet har emellertid brister, både författningstekniskt och innehållsmässigt. Frågan om det behövs någon reglering av ett nytt myndighetsråd har redan berörts. I övrigt bör förordningsförslaget bland annat ses över med avseende på hur omfattande reglering som behövs samt hur den ska förhålla sig till regleringen av informationssäkerhet såsom en del av säkerhetsskyddet samt till bestämmelserna om MSB:s uppdrag i MSB:s instruktion.

Frågor om reglering om sensorsystem behandlas nedan under rubriken Sensorsystem.

Tillsyn

MSB instämmer i att det systematiska informationssäkerhetsarbetet hos myndigheterna generellt behöver stärkas. En starkare uppföljning av hur arbetet bedrivs kan därför behövas. En ny förordning med mer utvecklade krav i fråga om statliga myndigheters informationssäkerhet bidrar redan i sig till en ökad medvetenhet och ett bättre informationssäkerhetsarbete hos myndigheterna. MSB bereder för närvarande också nya föreskrifter och allmänna råd för statliga myndigheters informationssäkerhet. Avsikten är att de nya myndighetsreglerna på ett tydligare och mer utförligt sätt ska beskriva hur arbetet ska bedrivas, så att det blir lättare för myndigheterna. Att regeringen i regleringsbrev för de mest berörda myndigheterna uppdragit åt dessa att redovisa sitt informationssäkerhetsarbete bör också påtagligt bidra till att skärpa myndigheternas uppmärksamhet på vikten av arbetet. Vidare kan utvecklingen av arbetet med den nationella risk- och förmågebedömningen få betydelse för det här området.

Det finns också ett flertal metoder för uppföljning av myndigheternas arbete som kan tillämpas även när det gäller informationssäkerhetsarbetet. Det kan övervägas om inte MSB i ett första skede borde fokusera på att utveckla de centrala åtgärdsförslagen i betänkandet. Därefter kan tillsynsfrågan prövas på nytt.

Revision

De uppföljningar som har gjorts inom området informationssäkerhet har bland annat visat att myndigheternas granskning av sitt eget informationssäkerhetsarbete behöver effektiviseras. Granskningen kan bedrivas med olika metoder och på olika nivåer. Den kan också behöva kombineras med rapportering för att uppnå avsedd effekt. Olika alternativa vägar för att stärka både granskning och rapportering av informationssäkerhetsarbetet kan övervägas. De specifika

förslag som utredaren föreslår innebär dock en tydlig principiell skillnad mot nuvarande styrning som är generell och där inget specifikt område pekas ut särskilt. En specifik reglering för informationssäkerhet enligt utredarens förslag aktualiserar en analys av huruvida även andra viktiga områden, såsom miljöskydd, jämställdhet och skydd mot korruption, ska specificeras på motsvarande sätt.

Åtgärdsförslag med koppling till upphandling

Myndigheten tillstyrker utredningens förslag om kravställning vid upphandling. När det gäller uppgiften att ta fram skyddsprofiler som anger minimikrav på säkerhet i vanligt förekommande it-produkter som används av statliga myndigheter vill dock MSB hänvisa till det behov av ytterligare utredning som lyfts fram nedan under rubriken säkra kryptografiska funktioner.

Utredningens förslag att åtgärder som säkerställer att informationssäkerhet ska beaktas i samband med upphandlingar kan få stor betydelse för både myndigheters och privata aktörers informationssäkerhet. MSB vill särskilt betona behovet av att ytterligare utveckla beställarkompetensen samt betydelsen av standarder när det gäller säkra it-produkter och certifiering. Genom den nationella styrmodell som föreslås etableras väl definierade skyddsnivåer vilket i sin tur underlättar arbetet för leverantörerna när det gäller utveckling och tillhandahållande av säkra produkter och tjänster. MSB ser också mycket positivt på de möjligheter som privat-offentlig samverkan kan ge. En sådan samverkan behöver givetvis anpassas till aktörernas olika intressen och förmåga. MSB ser särskilt att det skulle vara av intresse att utveckla sektorsinriktad samverkan.

Swedish Government Secure Intranet (SGSI)

MSB tillstyrker utredningens förslag om att utveckla kommunikationssystemet SGSI. Det kan övervägas att inkludera fler myndigheter än de som nämns i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap, företrädesvis de som omfattas av det särskilda regeringsbeslutet som reglerar vilka myndigheter som ska ha tjänsteman i beredskap.

MSB anser även att det i samband med utbyggnaden av SGSI är nödvändigt att utveckla ett fysiskt nät som i huvudsak är baserat på statligt ägd infrastruktur. Även i utredningen pekas det på fördelar med en sådan lösning. Om staten äger och kontrollerar infrastrukturen kan den såväl operativt som kvalitativt bestämma, prioritera och inrikta utvecklingen av den funktionalitet som krävs. MSB delar utredningens bedömning att staten äger omfattande mängder av infrastruktur som skulle kunna användas för att bygga ett framtida utvecklat SGSI. En gemensam förvaltning av denna infrastruktur skulle vara en kostnadseffektiv lösning.

Radiospektrum är en förutsättning för att MSB ska kunna tillhandahålla mobila kommunikationstjänster. MSB hänvisar i denna del till det pågående

arbetet för att säkerställa förutsättningarna för säker och tillgänglig kommunikation för samhällsviktiga aktörer som Post- och telestyrelsen ansvarar för inom ramen för sitt uppdrag att tilldela radiospektrum. MSB understryker vikten av att SGSI framgent även stödjer det alltmer utökade mobila arbetssätt som användarna har. Mobilitet är en förutsättning för användarnas fortsatta utveckling av arbetsmetoder och effektivisering av verksamheterna.

Sensorsystem

I utredningen beskrivs kortfattat vad sensorsystem är och vilken roll de kan spela för att höja säkerheten. Bristen på en rättvisande lägesbild i Sverige när det gäller attacker på it-system är problematisk. Det är inte bara information om mängden it-attacker som saknas, det finns även indikationer på att attackerna blir allt mer raffinerade och svårupptäckta. Denna utveckling sker parallellt med att samhällets beroende av fungerande it-system stadigt växer och nya sårbarheter i systemen nästan dagligen identifieras. Flera myndigheter med uppdrag inom informationssäkerhetsområdet har tillgång till verktyg och information, bland annat tack vare internationella samarbeten, som kan både förebygga och hantera allvarliga it-incidenter. Med hjälp av ett sensorsystem som används för att stödja samhällets informations- och cybersäkerhet kan samhällets resurser användas effektivt. Anslutna organisationer kan få ett kvalificerat stöd i att identifiera attackmönster och skadliga ip-adresser som inte är tillgängliga i motsvarande kommersiella tjänster. Om angrepp mot exempelvis en viss typ av it-system ökar i antal skapar sensorsystemet även möjlighet att i tid varna ännu inte drabbade organisationer så att de kan vidta adekvata skyddsåtgärder. MSB bedömer därför att sensorsystem på ett påtagligt sätt kan bidra till att öka informationssäkerheten både på organisations- och samhällsnivå.

En myndighets användning av sensorsystem i syfte att stärka samhällets informations- och cybersäkerhet förutsätter dock anpassningar av den författningsmässiga regleringen av den personuppgiftsbehandling som kommer att ske, eftersom de ip-adresser som hanteras i sensornätverket under vissa förhållanden kan betraktas som personuppgifter. MSB har fört en dialog med Datainspektionen om dessa frågor. Datainspektionen framhåller att både integritets- och rättssäkerhetsskäl talar för att en hantering av personuppgifter av detta slag bör ges en särskild författningsreglering.

MSB bedömer således att det behöver tydliggöras i författning att personuppgifter får behandlas specifikt för detta syfte. En myndighet med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter bör få behandla personuppgifter om det är nödvändigt för att antingen bistå anslutna organisationer att upptäcka, verifiera och hantera it-incidenter, eller för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Det skulle dessutom, enligt MSB:s uppfattning, behöva göras ett undantag från den i 23 § personuppgiftslagen (1998:204) föreskrivna skyldigheten att lämna information till den person, vars uppgifter behandlas. Enligt 8 a § personuppgiftslagen får regeringen i vissa fall föreskriva om sådana undantag.

Tidssynkronisering

MSB delar utredningens bedömning av tidssynkroniseringens betydelse och tillstyrker förslaget om att statliga myndigheter ska använda samma synkroniserade tidsskala i sina it-system.

Säkra kryptografiska funktioner

Kryptering har länge setts som det viktigaste tekniska skyddet mot obehörig åtkomst i kommunikationssystem och lagring av information. De signalskyddssystem som utvecklats inom staten har dock ofta visat sig vara utvecklade för ett annat syfte än att de ska kunna användas i de mer distribuerade miljöer som är vanliga idag inom till exempel hälso- och sjukvårdssektorn. Därför bör även andra kommersiella lösningar som till exempel anonymisering och signeringstjänster som är lämpliga för miljöer där övervägande delen av informationen är personuppgiftsbaserade, på sikt kunna utvecklas och tillhandahållas baserade på den offentliga förvaltningens behov/kravbild. De offentliga kommunikationslösningar som finns bör kunna redovisas utifrån vilken skyddsnivå de uppnår. Detta bör innefatta inte bara konfidentialitetsaspekten utan även riktighet, tillgänglighet och spårbarhet för att myndigheterna ska kunna avgöra vilken lösning som är lämplig för deras kommunikationsbehov.

Avseende säkra kryptografiska funktioner (avsnitt 9.4.2) delar MSB utredningens uppfattning att den av MSB gemensamt med Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten, föreslagna nationella strategin med åtgärdsplan (bilaga 4) bör ligga till grund för utvecklingen av processerna på området. Säker kommunikation är avgörande för informationssäkerheten och frågan är därför av stor vikt för många myndigheter och det är angeläget att processerna snabbt kan komma på plats. Försvarets materielverk har genom CSEC (Sveriges certifieringsorgan för it-säkerhet) en central roll i den föreslagna modellen och har också stor erfarenhet av utveckling av processer inom området. Därför bör Försvarets materielverk få i uppdrag att, i samråd med de övriga nämnda myndigheterna, precisera underlaget så att det kan ligga till grund för konkreta uppgifter till respektive myndighet.

Ytterligare en fråga som behöver beaktas enligt MSB:s uppfattning, är hur krypterings- och signeringslösningar ska hanteras över tid. I många fall är det information som ska lagras i oförändrat skick under lång tid och där nycklar måste kunna bevaras för att informationen ska vara tillgänglig under hela bevarandetiden. I denna fråga har Riksarkivet en viktig roll.

Obligatorisk it-incidentrapportering

MSB tillstyrker utredningens åtgärdsförslag om obligatorisk it-incidentrapportering. MSB ser det som angeläget att dessa åtgärder genomförs så snart som möjligt.

Myndigheten följer noga utvecklingen av EU-direktivet om nät- och informationssäkerhet (NIS-direktivet). MSB har också lämnat en uppdragsredovisning till regeringen om hur ett nationellt system för it-incidentrapportering kan utformas. Redovisningen, tillsammans med övrigt arbete som myndigheten genomfört inom området, utgör enligt MSB:s bedömning en god grund för det fortsatta arbetet.

För att ytterligare utveckla ett nationellt system för it-incidentrapportering kan det också, enligt MSB:s mening, finnas anledning att överväga möjligheten att föreskriva om absolut sekretess för it-incidentrapporter.

Åtgärdsförslag med koppling till förebyggande och bekämpande av it-relaterad brottslighet

It-brottslighet utgör en växande utmaning i dagens samhälle. Nya tekniska lösningar kan innebära nya säkerhetsproblem. Därtill har vi användarnas höga krav på tillgänglighet, integritetsskydd och verksamheternas krav på ekonomisk effektivitet. Detta leder till att alltmer känslig information lagras i sårbara internetanslutna system. Dessa it-system blir därmed attraktiva mål för it-angrepp vilka är globala, ständigt pågående och även riktade mot svenska intressen. Utredningarna av den här typen av brottslighet är beroende av att det finns möjlighet för brottsbekämpande myndigheter att bedriva sin förebyggande och brottsbekämpande verksamhet i den digitala miljön på motsvarande sätt som i den fysiska. Samtidigt växer behovet av samarbete mellan nationella och internationella aktörer som på olika sätt kan bidra i arbetet. MSB delar helt utredningens syn på att det finns behov av att närmare utreda de legala förutsättningarna för att underlätta både samverkan och användning av tvångsmedel.

Internationella aspekter

Det internationella samarbetet är i många delar en förutsättning för och underlättar det nationella informationssäkerhetsarbetet. MSB delar utredningens bedömning att en ökad samordning underlättar möjligheterna att dra nytta av och påverka utvecklingen på internationell och nationell nivå.

Övning

I utredningen betonas att övningar fyller en mycket väsentlig funktion i det samlade arbetet kring informations- och cybersäkerhet i samhället samt att övningsverksamheten bör fortsätta och förstärkas. MSB instämmer i detta och erinrar om att myndigheten förvaltar en nationell plan över tvärsektoriella övningar inom området samhällsskydd och beredskap och är sammanhållande för ett nationellt forum för inriktning och samordning av sådana övningar.

Resurser

Den strategi för informations- och cybersäkerhet som utredningen föreslår innehåller förslag som påverkar ett stort antal aktörer. Nedan kommer endast MSB:s egna resursbehov att kommenteras då myndigheten enligt utredningen ska tillföras omfattande ansvar och uppdrag.

MSB bedömer att myndighetens resursbehov för att uppfylla de tilldelade uppgifterna på avsett sätt är större än vad utredningen har indikerat. Generellt bedömer utredningen behoven i termer av årsarbetskrafter som behöver tillföras MSB. Detta är dock en allt för snäv syn då flertalet av uppgifterna som MSB föreslås genomföra innebär behov av investeringar, annan utrustning och driftskostnader för dessa. Uppgifterna innebär också att myndighetens indirekta kostnader ökar, såsom avgifter till Statens servicecenter och egna kostnader för administration och lokaler.

Tillsyn

En eventuell tillsynsuppgift för MSB kommer att kräva en väsentlig resursförstärkning hos myndigheten, om tillsynen ska kunna utövas systematiskt och kontinuerligt över i princip hela det statliga myndighetsområdet. En underdimensionerad tillsyn kommer endast att kunna genomföra punktinsatser.

Obligatorisk it-incidentrapportering

En obligatorisk it-incidentrapportering förutsätter inte bara personal utan även administration och drift av olika system, i vissa fall även utveckling av sådana system. MSB tar redan idag emot rapporter om it-incidenter men en sådan utökning av verksamheten som en obligatorisk rapportering innebär medför ett större resursbehov än som beskrivs i utredningen. Detta gäller inte minst för att kunna säkerställa återrapportering och redovisning av trender. Om genomförandet av NIS-direktivet skulle innebära att obligatoriet utsträcks till andra aktörer än statliga myndigheter, och MSB ges ansvar för att hantera även en sådan rapportering, skulle det innebära ytterligare behov av personal och system. Eventuella krav på bemanning dygnet runt ökar också resursbehovet.

Säkra kryptografiska funktioner samt drift och administration av system

Vid en övergripande bedömning ser MSB att det finns ett behov av utökade resurser. Den närmare omfattningen är dock tänkt att framgå av det preciserade underlag som MSB, Försvarsmakten, Försvarets radioanstalt och Försvarets materielverk föreslår att Försvarets materielverk får i uppdrag att, i samråd med de övriga nämnda myndigheterna, ta fram. Som nämnts ovan är syftet med underlaget att det ska ligga till grund för ett förslag på konkreta uppgifter till respektive myndighet.

Övning

En eventuell utökad övningsverksamhet får ekonomiska konsekvenser, både för de aktörer som deltar i övningarna och de som arrangerar övningarna.

I detta ärende har generaldirektör Helena Lindberg beslutat. Helena Andersson har varit föredragande. I den slutliga handläggningen har också avdelningschefen Cecilia Nyström, chefsjuristen Key Hedström, verksamhetschefen Richard Oehme, ekonomi- och planeringsdirektören Björn Myrberg, t.f. enhetschefen Åke Holmgren och seniora handläggaren Ingela Darhammar Hellström deltagit.

Helena Lindberg

Helena Andersson

Kopia: Försvarsdepartementet