REGERINGSKANSLIET

Promemoria

2017-02-24

Justitiedepartementet

Tillhandahållande av tekniska sensorsystem – ett sätt att förbättra samhällets informationssäkerhet

Sammanfattning

Regeringen föreslås ge Myndigheten för samhällskydd och beredskap rättsligt mandat att stödja vissa offentliga och enskilda verksamhetsutövare inom samhällsviktig verksamhet med informationssäkerheten genom att, på deras begäran, tillhandahålla sensorsystem. Myndigheten för samhällsskydd och beredskap (MSB), som enligt förslaget bestämmer vilka verksamhetsutövare som på begäran kan få systemet placerat hos sig, ska vid utplaceringen samverka med Säkerhetspolisen. De mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag som Försvarets radioanstalt erbjuder ett tekniskt detekterings- och varningssystem ska inte tillhandahållas sensorsystemet. En bestämmelse som ger mandat för MSB att tillhandahålla sensorsystem bör införas i förordningen (2008:1002) med instruktion för MSB. I övrigt saknas behov av författningsändringar för den personuppgiftsbehandling som systemet föranleder.

Bakgrund

Betänkandet Informations- och cybersäkerhet i Sverige

Regeringen uppdrog i november 2013 (dir. 2013:110) åt en särskild utredare att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Uppdraget redovisades i mars 2015 genom betänkandet *Informations- och cybersäkerhet i Sverige* (SOU 2015:23). Utredningen föreslår en strategi för informations- och cybersäkerhet i staten. Strategin har sex mål, som främst vänder sig till regeringen, Regeringskansliet och till de statliga myndigheterna. Strategin syftar bl.a. till att bidra till att reducera sårbarheten och uppnå en effektiv risknivå i statens olika informationssystem.

Inom de strategiska områdena anges olika förslag till åtgärder, bl.a. ett författningsreglerat rapporteringskrav för myndigheter avseende it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten levererar till en annan organisation. Rapporteringskravet har redan införts för flertalet myndigheter i den nya förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, som trädde i kraft den 1 april 2016. Rapporteringsskyldigheten omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633). I de fallen sker rapporteringen till Försvarsmakten eller Säkerhetspolisen enligt vad som anges i 39 § samma förordning.

Utredningen föreslår också en ny förordning för statliga myndigheters informationssäkerhet med bl.a. en bestämmelse som gäller sensorsystem. Den föreslagna bestämmelsen föreskriver att myndigheter som har ett särskilt ansvar för krisberedskap enligt den nya förordningen om krisberedskap (10 §) och de myndigheter som MSB beslutar i enskilda fall, är skyldiga att uppfylla särskilda krav på informationssäkerhet rörande bl.a. användning av sensorsystem för it-incidentidentifiering.

Utredningen konstaterar att de legala frågorna med koppling till sensorsystem och dess utformning samt användning i vissa delar kräver närmare analys.

Betänkandet har remitterats och bereds nu i Regeringskansliet. Arbetet med en nationell strategi för stärkt informations- och cybersäkerhet i samhället pågår. MSB har i sitt remissvar framfört att förslaget om att myndigheten ska få tillhandahålla sensorsystem är angeläget och bör prioriteras. I denna promemoria behandlas därför frågan om MSB ska få tillhandahålla tekniska sensorsystem, vilken personuppgiftsbehandling detta kan aktualisera och vilka författningsförändringar som krävs för att personuppgiftsbehandlingen ska vara förenlig med gällande rätt.

Flera remissinstanser efterlyser en analys av främst vissa bestämmelser i personuppgiftslagen

I sitt remissvar har MSB anfört att sensorsystem som används för att stödja samhällets informations- och cybersäkerhet kan leda till en mer effektiv användning av samhällets resurser. MSB pekar bl.a. på att regeringen behöver tydliggöra att personuppgifter får behandlas specifikt för detta syfte.

Även flera andra remissinstanser har hänvisat till att det saknas en rättslig analys av sensorsystems förenlighet med främst personuppgiftslagen och har angett att användningen av sensorsystem förutsätter anpassningar av den författningsmässiga regleringen av den personuppgiftsbehandling som kommer att ske.

Datainspektionen (DI) efterlyser en integritetsanalys och mer ingående information om de närmare förutsättningarna för sensorsystem. Kunskapen behövs för att inspektionen ska kunna göra en proportionalitetsbedömning, där behovet och de positiva effekterna av sensorsystem vägs mot den förlust i integritetshänseende som systemet ger upphov till. DI ifrågasätter om sensorsystem är förenligt med ändamålsbestämmelsen i PuL (9 § d) och anser att informationsplikten i PuL blir svår att uppfylla. Inspektionen efterlyser även en närmare analys av behovet av ändringar i offentlighets- och sekretesslagen (2009:400), OSL.

Ekobrottsmyndigheten och Skatteverket avstyrker förslaget om obligatorisk användning av sensorsystem, eftersom användningen av sensorsystem och de rättsliga och integritetsmässiga konsekvenserna inte är närmare belysta eller analyserade. Båda myndigheterna är kritiska till att utredningen inte gjort någon egen analys av viktiga integritets- och sekretessfrågor som aktualiseras i det författningsförslag som utredningen lägger fram.

Nya säkerhetshot och sårbarheter

Den snabba it-utvecklingen innebär förutom nya möjligheter nya säkerhetshot. Säkerhetshoten beror i stor utsträckning på att it-systemen blir mer komplexa och med fler inbördes beroenden. Därtill finns användares höga krav på tillgänglighet och verksamhetsutövares krav på ekonomisk effektivitet. Alltmer skyddsvärd information lagras därför i sårbara internetanslutna system, som blir attraktiva mål för it-angrepp. Eftersom verksamhetsutövare i dag är beroende av digital informationshantering, riskerar de att drabbas allvarligt vid it-angrepp. Vissa skyddsvärda verksamheter är också i ökande utsträckning beroende av industriella informations- och styrsystem som vid obehörig eller felaktig påverkan kan drabba samhällsviktiga funktioner.

Det finns alltså ett stort behov av att snabbt kunna vidta åtgärder för att begränsa störningar på samhällsviktig verksamhet och kritisk infrastruktur. För att begränsa effekter av it-angrepp är det viktigt att berörda verksamhetsutövare snabbt får information om hot, sårbarheter och stöd för hantering av incidenten.

Ett heltäckande skydd för informationssäkerhet förutsätter åtgärder på både nationell nivå och verksamhetsnivå. I regel har verksamhetsutövare egna säkerhetssystem installerade, såsom t.ex. virusskydd och brandväggar. Systemen syftar till att detektera och kunna hantera intrång. Inte sällan beställer verksamhetsutövaren därutöver säkerhetstjänster av utomstående aktörer. Hur pass effektiva sådana tjänster är beror i stor

utsträckning på vilken tillgång till data om skadlig kod, ip-adresser[1] och motsvarande som verksamhetsutövaren har.

Att skydda sin information och sina systems funktionalitet utgör i många fall även ett samhällsintresse. Allt fler tjänster och system är sammankopplade och kopplingen är inte alltid känd. Detta innebär att it-angrepp mot en verksamhetsutövare kan få kaskadeffekter på andra verksamhetsutövare. It-angrepp kan även ske samtidigt mot flera samhällsviktiga system.

Vidare kan störningar eller antagonistiska hot där system tas över av tredje part hota samhällsviktiga funktioner. Data- och nätverks-operationer har utvecklats till att utgöra ett separat antagonistiskt hot som ett av flera militära maktmedel. (Se mer om detta i regeringens försvarspolitiska inriktningsproposition 2014/15:109, *Sveriges försvar 2016-2020* s. 111–113.) Att identifiera, förebygga och ha förmåga att hantera it-incidenter med antagonistiskt ursprung är en väsentlig del i skyddet av samhällsviktig verksamhet, främst samhällsviktig och kritisk infrastruktur. Arbetet kräver ett brett samarbete mellan olika samhällsaktörer. I det arbetet är information om allvarligare it-incidenter viktig för att skapa en nationell lägesbild, vilken i sin tur ger förutsättningar för effektiv hantering av incidenterna.

Även i Riksrevisionens rapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23) pekas på att den ökande utvecklingen av it innebär stora risker samt att brister i hanteringen och informations-säkerheten riskerar att få omfattande konsekvenser, både för samhället i stort och för enskilda. Riksrevisionens slutsats är att arbetet med informationssäkerheten i den civila statsförvaltningen inte är ändamåls-enligt, sett till de hot och risker som finns. I rapporten anges även att det saknas en samlad lägesbild som inkluderar bl.a. hot och i vilken omfattning och mot vilka hoten realiseras. Riksrevisionen anser därför att det är nödvändigt att regeringen och regeringens stöd- och tillsynsmyndigheter vidtar åtgärder, så att det går att få en samlad bild av läget och utifrån detta anpassar kraven på säkerheten till de behov som finns.

Sensorsystem

Sensorsystem är ett verktyg för att upptäcka it-relaterade hot. Systemet kan utformas på olika sätt och syfta till att stärka informationssäkerheten hos både enskilda verksamhetsutövare och i samhället i stort. Det är t.ex. möjligt att installera sensorer lokalt i verksamhetsutövares egna nätverk och datorer för att upptäcka, larma och agera på misstänkta angrepps-

[1] En ip-adress (Internet Protocol address) är ett nummer som används som adress för enskilda datapaket i ip-standarden, vilket är den grundläggande standard som används för trafik på Internet.

försök. Sensorsystem finns i dag i många länder och i alla typer av verksamheter.

Ett sensorsystem består förenklat beskrivet av en förteckning över vilka skadliga koder och skadliga ip-adresser systemet ska leta efter samt tekniska sensorer som larmar vid upptäckt hot. Vidare består systemet av säkra kommunikationslösningar, databaser för att bevara inhämtad information och en analysfunktion. Analytiker kan därefter analysera angreppet och meddela både drabbad och ännu inte drabbade aktörer om vad som hänt och ge stöd för hantering och skydd.

Sensorsystem kan förenklat delas in i tre typer av system. Indelningen beror bl.a. på vilken information som systemet har tillgång till och vem som tillhandahåller systemet. De olika typerna av system kompletterar varandra.

Den första typen av system är tekniska detekteringsverktyg som tillhandahålls av enskilda aktörer och bygger på information som dessa erbjuder kommersiellt. Dessa system ger stöd för den aktuella verksamhetens eget arbete med informationssäkerhet och ger ett grundskydd för informationssäkerhet.

Sensorsystem som tillhandahålls av den myndighet som har uppgift att vara ett lands CERT[2]-funktion ger ett utökat skydd jämfört med system som tillhandahålls kommersiellt. Nationella CERT:ar ska ha väl etablerat samarbete med andra nationella aktörer, offentliga som privata, och besitta stor kunskap om skadliga koder och aktörer som sprider sådan kod. Därutöver har en nationell CERT väl etablerat samarbete med nationella CERT:ar i andra länder för utväxling av information som kan komma till nytta i uppsättning av sensorsystem. Informationen som används för att detektera signaturer och skadliga ip-adresser inhämtas främst genom det nationella och internationella CERT-arbetet. Informationen är inte allmänt tillgänglig utan omfattas i regel av sekretess till skydd för uppgifter om säkerhets- och bevakningsåtgärder.

Slutligen finns sensorsystem som tillhandahålls av expertmyndigheter på underrättelseområdet som har tillgång tillunderrättelseinformation. Dessa system ger ett förstärkt skydd för de mest skyddsvärda funktionerna i samhället. Systemen analyserar datatrafik för att upptäcka ett mer avancerat spektrum av it-angrepp, eftersom informationen

[2] CERT står för Computer Emergency Response Team. Vid MSB finns CERT-SE, Sveriges nationella funktion med uppgift att stödja samhället i arbetet med it-incidenter. CERT-SE är en så kallad CSIRT, (Computer Security Incident Response Team) och deltar aktivt i flera internationella nätverk med motsvarande funktioner.

bygger på nationell förmåga till strategisk signalspaning. Den information som finns i sensorerna omfattas i stor utsträckning av sekretess till skydd för rikets säkerhet. Ett sådant system tillhandahålls i dag av Försvarets radioanstalt för de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag, som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Systemet kallas för tekniskt detekterings- och varningssystem, TDV. TDV är en viktig delmängd i ett samlat cyberförsvar.

Informationsflödet i sensorsystem som kan tillhandahållas av MSB

Hanteringen av information i det sensorsystem som MSB föreslås få tillhandahålla sker i flera steg och processer, både hos den anslutna verksamhetsutövaren (verksamhetsutövaren) och hos MSB som tillhandahåller sensorsystemet (tillhandahållaren). Nedan beskrivs informationsflödet.

Förteckningen

I sensorsystemets förteckning finns uppgifter som leder till att it-angrepp kan upptäckas. Uppgifterna i förteckningen består av t.ex. ip-adresser som skickar ut skadlig kod eller på annat sätt används vid it-angrepp (skadliga ip-adresser). De kan också bestå av skadliga koder som är kända att användas vid angrepp. Det är uppgifterna i förteckningen som avgör vilka it-angrepp som sensorsystemet kommer att upptäcka.

Tillhandahållaren uppdaterar kontinuerligt förteckningen med uppgifter som använts vid nyupptäckta it-angrepp. De uppgifter som krävs för att upptäcka hot varierar. Oftast handlar det om en beskrivning av den skadliga koden i form av ettor och nollor. I vissa fall kan dock den skadliga koden vara dold i eller kopplad till e-post och därmed till en e-postadress eller någon annan typ av personuppgift. I dessa fall kan förteckningen behöva inkludera även sådana uppgifter för att säkerställa att den skadliga koden verkligen upptäcks.

Trafik på internet skickas mellan olika ip-adresser. Ett exempel på när en skadlig ip-adress används är vid dataintrång som syftar till att, utan att det märks, få en dator i en verksamhet att börja skicka ut känslig information till en viss ip-adress. Både den ip-adress varifrån den skadliga koden skickas för att styra den drabbade datorn och den ip-adress som används som mottagare av informationen utgör skadliga ip-adresser.

Detekteringssensorerna

Verksamhetsutövaren ansluter sig till sensorsystem genom att låta tillhandahållaren placera ut detekteringssensorer hos sig. Detekteringssensorerna placeras utanför verksamhetsutövarens brandvägg och går igenom all in- och utgående trafik från verksamhetsutövaren, vilket sker

på samma sätt som med t.ex. anti-virusprogram. Olika slags trafik bevakas för att kunna upptäcka olika slags attacker, såsom t.ex. phishing-attacker[3] som främst sker via e-post eller intrångsförsök i verksamhets-system som kan ske via webbtrafik.

Detekteringssensorernas uppgift är att upptäcka skadlig kod eller trafik från skadliga ip-adresser m.m. som finns angivna i förteckningen. Om detekteringssensorerna upptäcker sådana uppgifter larmas tillhanda-hållaren om upptäckten och den centrala analysfunktionen och verksamhetsutövaren informeras om den. Om misstanke om falsklarm finns eller om informationen om it-incidenten är ofullständig spelas även berörd trafik in. Trafikinspelningen, på ett par minuter, omfattar om det är e-posttrafik, även e-postinnehållet. Efterföljande hantering av sådana trafikinspelningar är begränsad till det som direkt föranleds av säkerhetsarbetet och utförs i stor utsträckning av säkerhetsanalytiker med stöd av tekniska verktyg.

Inspelning vid misstanke om falsklarm görs för att analysera om larmet är falskt eller äkta. Vissa typer av larm orsakas av ospecifika uppgifter i förteckningen och genererar därför falsklarm.

Inspelning vid ofullständig information om en it-incident görs när uppgifter i förteckningen inte är fullständiga, t.ex. när endast delar av en skadlig kod finns i förteckningen, vilken därför kan ingå i flera olika typer av upptäckta skadliga koder. För att kunna veta vad verksamhetsutövaren drabbats av och kunna ge lämpligt stöd, behövs i sådana fall kompletterande information om angreppet.

Det är endast trafiken på utsidan av brandväggen som omfattas av inspelningar, vilket innebär att trafik mellan ip-adresser inom organisationen inte spelas in. Trafikinspelningen består av information om avsändande och mottagande ip-adress, tidpunkt för trafiken, trafikens storlek samt viss teknisk data om uppkopplingen. Om larmet utlösts av e-posttrafik omfattar inspelningen även e-postinnehållet.

Inspelningen sparas inte i detekteringssensorn, utan skickas automatiskt till larmdatabasen hos tillhandahållaren där den kopplas till berört larm.

Larmen

När detekteringssensorn upptäcker t.ex. en skadlig kod skickar den ett larm till tillhandahållaren. Larmet innehåller uppgift om vad detekteringssensorn upptäckt för hot, t.ex. en viss skadlig kod, tidpunkt för upptäckten samt vilken avsändar- och mottagar-ip-adress trafiken

[3] Phishing är i dag en vanligt förekommande metod som används i syfte att lura användare på känslig information (e.g. lösenord och bankuppgifter) eller leverera skadlig kod. Phishing förekommer i flera former, där e-post som uppmanar mottagaren att klicka på en länk, öppna ett dokument eller fylla i personliga uppgifter hör till de vanligaste.

har. Larmet innehåller inte några andra personuppgifter än sådana som redan förts in i förteckningen. Larmet skickas från detekteringssensorn till tillhandahållarens larmdatabas.

Larmdatabasen

I larmdatabasen, som finns hos tillhandahållaren, sparas alla larm som genererats i detekteringssensorerna hos anslutna verksamhetsutövare och, i de fall det finns, inspelning av trafik kopplat till ett specifikt larm. Det är tillhandahållaren av sensorsystem som bestämmer vilken information som ska läggas in i larmdatabasen, hur den informationen ska användas och hur skyddet för informationen ska utformas.

Syftet med att spara larm är, förutom att kunna bedöma dess riktighet, att kunna upptäcka mönster och pågående angrepp som riktas mot fler än en verksamhetsutövare. Sådan kunskap gör det möjligt för tillhandahållaren att lämna varningar och rekommendationer till berörda verksamhetsutövare, som underlättar hanteringen av it-angrepp. Verksamhetsutövare bestämmer själva om it-incidenter ska hanteras genom egen kompetens, bistånd av tillhandahållaren eller extern konsult.

Trafikflödessensorerna och trafikflödesdatabasen

I ett sensorsystem ingår, utöver detekteringssensorerna, även så kallade trafikflödessensorer. Även dessa sensorer samlar kontinuerligt in viss information om trafik hos verksamhetsutövaren och skickar den till en annan databas, den så kallade trafikflödesdatabasen, hos tillhandahållaren. Syftet med denna insamling är att i efterhand kunna söka efter genomförda attacker som inte upptäckts av detekteringssensorerna. Trafikinformationen består bl.a. av uppgift om mellan vilka ip-adresser trafik skickats, storlek på trafiken och tidpunkten för trafiken. Inget innehåll i trafiken, t.ex. i e-postmeddelanden, spelas in i trafikflödessensorerna.

Hos tillhandahållaren finns en separat trafikflödesdatabas för varje ansluten verksamhetsutövare där informationen lagras på ett skyddat sätt.

För att identifiera tidigare genomförda attacker som inte upptäckts av detekteringssensorerna, kan tillhandahållaren regelbundet låta samköra den uppdaterade förteckningen mot uppgifterna som finns i trafikflödesdatabasen. Om tillhandahållaren får träff vid samkörningen, larmas verksamhetsutövaren och informationen analyseras.

Eftersom vissa särskilt allvarliga attacker kan pågå under lång tid (s.k. APT – Advanced Persistent Threat) förekommer det i många fall att en attack som initierats under ett år inte når sitt slutliga resultat förrän långt senare, ibland efter flera år. Det är mycket angeläget för en verksamhetsutövare att upptäcka sådana attacker eftersom de inte sällan initierats av en målmedveten angripare. Trafikflödesdatabasen möjliggör för till-

handahållaren att regelbundet kontrollera om ett nyupptäckt hot, både APT och andra, har drabbat verksamhetsutövaren redan innan uppgifter om t.ex. den skadliga koden fördes in i förteckningen.

MSB bör få tillhandahålla sensorsystem

Behovet av att MSB får tillhandahålla sensorsystem

Av 11 a § i förordningen med instruktion för MSB följer att MSB ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Av samma bestämmelse följer att MSB ska rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder på olika nivåer och områden i samhället. Vidare anges i instruktionen att MSB ska ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter (11 b §).

Vid MSB finns CERT-SE, Sveriges nationella funktion med uppgift att stödja samhället i arbetet med it-incidenter. CERT-SE är en så kallad CSIRT, (Computer Security Incident Response Team) och deltar aktivt i flera internationella nätverk med motsvarande funktioner. I nätverken delas olika typer av information såsom uppgifter om skadlig kod och skadliga ip-adresser. Informationen är sällan allmänt tillgänglig. MSB/CERT-SE har till uppgift bl.a. att agera skyndsamt vid inträffade it-incidenter genom att sprida information. Vid behov har MSB till uppgift att arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade.

En viktig förutsättning för att kunna arbeta effektivt med att både förebygga och att skyndsamt kunna hantera it-incidenter är tillgången till en god lägesbild. Införandet av obligatorisk it-incidentrapportering för statliga myndigheter har bidragit till att MSB kan skapa en bättre lägesbild över allvarligare it-incidenter som upptäcks av de olika myndigheterna. Som angetts ovan omfattar rapporteringsskyldigheten inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen. MSB ska årligen till regeringen lämna en sammanställning av de incidenter som har rapporerats in till myndigheten enligt 20 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Inför sammanställning av rapporten ska MSB inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till de myndigheterna enligt 10 a § säkerhetsskyddsförordningen.

Det finns behov av att ytterligare stärka verksamhetsutövarnas förmåga att tidigt upptäcka försök till intrång och attacker. Som nämnts

inledningsvis leder den snabba it-utvecklingen till nya säkerhetshot och dessa förväntas fortsätta öka framöver. Tillgången till data från sensorer är av väsentlig betydelse för MSB:s uppdrag inom krisberedskap och skydd av samhällsviktig verksamhet där även andra aktörer än statliga myndigheter behöver ett utökat skydd.

De sensorsystem som redan i dag tillhandahålls som kommersiella produkter av enskilda verksamhetsutövare ger ofta ett bra och brett grundskydd. De enskilda verksamhetsutövarna har dock inte tillgång till, och kan därmed inte i sina sensorsystems förteckningar inkludera den typ av särskilt känslig information som statliga verksamhetsutövare delar i sina internationella nätverk. Ett sensorsystem som tillhandahålls av MSB skulle däremot stärka anslutna verksamhetsutövares förmåga att även upptäcka mer sofistikerade hot samt även starkt kunna bidra till att tillgodose behovet av en samlad lägesbild över it-incidenter i samhället. En samlad lägesbild skulle på ett effektivare sätt kunna bidra i arbetet med att avvärja och begränsa följderna av it-incidenter. Vid larm skulle MSB skyndsamt informera berörda verksamhetsutövare om upptäckt skadlig kod och om de åtgärder som kan vidtas för att avvärja och begränsa konsekvenserna av it-incidenter.

Som nämnts ovan har Försvarets radioanstalt redan till uppgift att på begäran kunna placera ut TDV vid de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag, som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Utplaceringen av TDV sker i samverkan med Säkerhetspolisen. MSB:s sensorsystem skulle kunna täcka en annan och bredare krets av användare som inte erbjuds TDV. Härigenom skulle samhällets möjligheter att upptäcka och få underlag för att kunna hantera it-incidenter ytterligare stärkas.

Sammanfattningsvis bedöms att det finns ett behov av att MSB, vid sidan av de sensorsystem som i dag tillhandahålls av enskilda verksamhetsutövare och av Försvarets radioanstalt, också ges möjlighet att tillhandahålla sensorsystem i samhället.

Integritetsavvägning enligt 2 kap. 6 § regeringsformen

Behovet av att MSB tillåts tillhandahålla sensorsystem måste vägas mot det eventuella intrång i den personliga integriteteten som ett sådant system, som det beskrivs ovan, kan medföra i form av behandling av personuppgifter. Enligt 2 kap. 6 § andra stycket regeringsformen gäller att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Den första frågan är om åtgärder som vidtas inom ramen för sensorsystem ska anses innebära *övervakning eller kartläggning* av den enskildes personliga förhållanden. Vid bedömningen är inte det avgörande en

åtgärds huvudsakliga syfte utan vilken effekt åtgärden har (prop. 2009/10:80 s. 250).

De personuppgifter som kan komma att behandlas i det aktuella sensorsystemet är främst ip-adresser under förutsättning att de kan hänföras till en fysisk person. Ip-adresserna är mycket svåra att koppla till fysiska personer och för att kunna göra det krävs tilläggsinformation som t.ex. finns hos teleoperatörer. De externa ip-adresser som används som avsändare av trafik vid intrångsförsök eller utskick av skadlig kod kan finnas i nätverk i vilken del av världen som helst. Detta försvårar arbetet med att identifiera till vilken verksamhet eller person ip-adressen hör. En sådan uppgift är dessutom ofta irrelevant för säkerhetsarbetet, för att stoppa t.ex. ett flöde med skadlig kod. Det relevanta torde i dessa fall i stället vara att identifiera nätoperatören och få denne att stänga ned ip-adressen.

För att kunna knyta ihop en viss ip-adress med en individ hos mottagaren förutsätts tillgång till verksamhetsutövarens interna ip-adresstrafik. Eftersom trafikflödessensorerna, som visserligen kontinuerligt spelar in uppgifter om trafik inklusive ip-adresser, sitter på utsidan av verksamhetsutövarens nät kommer inte interna ip-adresser att samlas in, utan endast verksamhetsutövarens externt synliga organisationsanknutna ip-adress.

Utöver ip-adresser kan det även förekomma andra personuppgifter i förteckningen och i den informationsmängd som vid larm spelas in i detekteringssensorerna. När det gäller förteckningen är det fråga om enstaka fall och det rör sig då om t.ex. kreditkortsnummer och personnummer. Även om uppgifter i förteckningen kan knytas till en viss person är sökningen begränsad till trafik till och från de anslutna verksamhetsutövarna. Dessutom sparas uppgifterna i förteckningen endast om de har en tydlig koppling till ett säkerhetshot så att det är nödvändigt att detekteringssensorerna larmar vid upptäckt. När det sedan gäller de personuppgifter som kan komma att spelas in i detekteringssensorerna vid larm kan även de vara av skilda slag. Om det är e-posttrafik kan även e-postinnehåll komma att sparas. Detekteringssensorerna bevakar all typ av trafik som går till och från verksamhetsutövaren. Den korta inspelningen, som i särskilda fall görs för närmare analys, tas bort så snart analysen genomförts.

Sammanfattningsvis är det en mycket begränsad mängd personuppgifter som, efter ett larm, kan komma att behandlas inom ramen för sensorsystem. Till allra största del rör det sig om ip-adresser där det kommer att vara svårt att identifiera till vilken verksamhet eller person ip-adressen hör. Det kan ytterst sällan förväntas bli annat än mycket begränsad information hänförlig till en viss individ som behandlas. Mot den bakgrunden talar mycket för att åtgärden inte kan anses innebära en kartläggning eller övervakning av en enskilds personliga förhållanden,

men att det inte helt kan uteslutas att behandlingen av personuppgifter i systemet ändå får den effekten med tiden. Klart är dock att det i vart fall inte är fråga om något betydande intrång. Slutsatsen är därför att åtgärderna inom ramen för det aktuella sensorsystemet inte kommer i konflikt med 2 kap. 6 § regeringsformen.

Rättsligt stöd för MSB att tillhandahålla sensorsystem

Det finns, som nämnts, redan bestämmelser i instruktionen för MSB i vilka det anges att myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt ansvara för att Sverige har en nationell CERT-funktion (11 a och b §§). Trots detta bedöms det lämpligt att av tydlighetsskäl införa en särskild bestämmelse som ger MSB rättsligt stöd att tillhandahålla sensorsystem.

I betänkandet Informations- och cybersäkerhet i Sverige föreslås att de s.k. bevakningsansvariga myndigheterna, dvs. de myndigheter som har ett särskilt ansvar för krisberedskap och höjd beredskap, ska vara skyldiga att använda sig av sensorsystem. En sådan lösning anses i nuläget inte befogad. Anslutning till systemet bör i stället bygga på frivillighet och möjligheten att ansluta sig till systemet bör finnas för både offentliga och enskilda verksamhetsutövare.

Tillhandahållande av systemet bör dock begränsas till verksamhetsutövare som bedriver samhällsviktig verksamhet. En sådan avgränsning ger MSB möjlighet att öka förmågan att identifiera och hantera mer sofistikerade it-angrepp mot centrala verksamhetsutövare inom olika samhällssektorer samt skapa en förbättrad lägesbild av förekomsten av sådana it-incidenter i samhällets centrala funktioner. I MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser definieras en samhällsviktig verksamhet som en verksamhet som uppfyller minst ett av följande villkor (2 § i MSBFS 2016:7). 1) Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället. 2) Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt. Exempel på samhällssektorer med viktiga samhällsfunktioner är energiförsörjning, finansiella tjänster samt skydd och säkerhet.

Försvarets radioanstalts system TDV erbjuds, som nämnts ovan, de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag, som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. För att på bästa sätt utnyttja samhällets resurser och optimera informationssäkerheten är det lämpligt att båda systemen inte tillhandahålls en och samma verksamhetsutövare. MSB:s system bör därför endast tillhandahållas sådana verksamhetsutövare inom samhällsviktig verksamhet som inte erbjuds TDV. En sådan ordning medför ökad

tydlighet för verksamhetsutövarna. En utplacering av MSB:s sensorsystem bör, på samma sätt som gäller för Försvarets radioanstalts TDV, ske i samverkan med Säkerhetspolisen. Enligt Försvarets radioanstalts regleringsbrev bör myndigheten hålla MSB informerad om det fortsatta arbetet med TDV. MSB bör på motsvarande sätt hålla Försvarets radioanstalt informerad om arbetet med MSB:s sensorsystem. I de fall det inte står helt klart om en verksamhetsutövare ska tillhandahållas TDV eller MSB:s sensorsystem bör en dialog också föras mellan Försvarets radioanstalt och MSB.

En bestämmelse med ett rättsligt mandat för MSB att tillhandahålla sensorsystem, med nu nämnda avgränsningar, bör därför införas i förordningen med instruktion för MSB. Bestämmelsen bör införas under avsnittet om informationssäkerhet och föreslås lyda enligt följande.

11 c § Myndigheten får på begäran tillhandahålla offentliga och enskilda verksamhetsutövare inom samhällsviktig verksamhet ett sensorsystem för att upptäcka och hantera it-incidenter. Sensorsystemet ska placeras ut i samverkan med Säkerhetspolisen.

De mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag som erbjuds ett tekniskt detekterings- och varningssystem i enlighet med 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt ska inte tillhandahållas sensorsystemet.

Behandling av personuppgifter vid MSB:s tillhandahållande av sensorsystem

Personuppgiftslagen är tillämplig

Enligt 5 § PuL är personuppgiftslagen tillämplig vid behandling av personuppgifter som helt eller delvis är automatiserad.

EU:s dataskyddsförordning börjar gälla från och med den 25 maj 2018 och kommer att ersätta personuppgiftslagen och dataskyddsdirektivet från 1995. Eftersom författningsförslaget i denna promemoria planeras träda i kraft innan dataskyddsförordningen börjar gälla, beaktas i promemorian i första hand gällande personuppgiftsreglering. Med hänsyn till att dataskyddsförordningen börjar gälla relativt nära inpå ikraftträdandet finns det emellertid skäl att jämföra bestämmelserna i dataskyddsförordningen med motsvarande bestämmelser i gällande personuppgiftsreglering.

Regleringen omfattar alltså helt eller delvis automatiserad behandling av personuppgifter oavsett om uppgifterna finns i ett register och dessutom manuell behandling av personuppgifter i register. Behandling i datorer av personuppgifter som finns i datorformat – inklusive överföring av personuppgifter till sådant format – bör som regel anses som automatiserad behandling. Behandling av personuppgifter, även om inget

sparas, kan utgöra en sådan behandling som omfattas av PuL (t.ex. DI beslut 2008-05-30, dnr 390-2008).

Bestämmelsen i 5 § PuL återfinns i liknande lydelse i artikel 2.1 i dataskyddsförordningen.

Den information som kommer att hanteras i det aktuella sensorsystemet och betraktas som personuppgifter är främst ip-adresser under förutsättning att de kan härledas till en fysisk person. Den behandling av personuppgifter som kommer att utföras då ett sensorsystem används kan beskrivas enligt följande.

1. MSB behandlar personuppgifter när myndigheten för in främst skadliga ip-adresser i dess *förteckning,* som kommer att finnas i datorformat och utgöra en databas.

2. När *detekteringssensorerna* upptäcker skadlig kod och skadliga ip-adresser samlar sensorerna automatiskt in dessa. Uppgifterna sparas inte i detekteringssensorerna utan förs direkt och automatisk in till larmdatabasen.

3. MSB behandlar sedan personuppgifter i *larmdatabasen*. I nämnda databas behandlas alltså endast larmade skadliga ip-adresser, eventuellt larmade koder och eventuellt trafikinnehåll som spelats in för en falsklarmsanalys m.m.

4. I *trafikflödessensorerna* insamlas trafikinformation som kan innehålla personuppgifter i form av ip-adresser. Dessa sparas inte i trafikflödessensorerna utan uppgifterna förs direkt in till trafikflödesdatabasen.

5. I *trafikflödesdatabasen*, som finns hos MSB, sparas all information som rör trafik till och från verksamhetsutövaren, dock inte någon information om trafik som endast är intern hos verksamhetsutövaren. Trafikinformationen består av uppgift om bl.a. mellan vilka ip-adresser ett e-postmeddelande har skickats samt tidpunkt och plats för detta.

Sammanfattningsvis utgör all behandling av personuppgifter i MSB:s aktuella sensorsystem automatiserad behandling och personuppgiftslagen är därmed tillämplig vid personuppgiftsbehandling i systemet. När dataskyddsförordningen träder i kraft kommer den i stället att vara tillämplig på aktuell personuppgiftsbehandling.

Ändamålsbestämmelsen i personuppgiftslagen

För att behandling av personuppgifter med stöd av PuL ska vara tillåten måste de grundläggande krav som finns i 9 § PuL vara uppfyllda.

Personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål (9 § c PuL). Ändamålen med en behandling av personuppgifter måste alltså bestämmas redan när uppgifterna samlas in. Angivna krav återfinns även i artikel 5.1 b) i dataskyddsförordningen.

MSB måste således ha uttryckligt angivna ändamål med personuppgiftsbehandlingen. Vidare måste ändamålen med behandlingen vara särskilda, vilket innebär att en alltför allmänt hållen ändamåls-angivelse inte godtas. Ändamålet med MSB:s behandling av eventuella personuppgifter är dels att bistå anslutna verksamhetsutövare att upptäcka och hantera it-incidenter, dels att få en samlad lägesbild över it-incidenter i samhället och att kunna stödja och varna andra aktörer i samhället.

De ändamål för vilka personuppgifterna samlas in ska vidare vara berättigade. Informationssäkerheten i samhället och hos en enskild verksamhetsutövare i samhället får anses utgöra ett berättigat ändamål för insamling av eventuella personuppgifter. I samma riktning talar den nya dataskyddsförordningen, där det bl.a. anges att personuppgifts-behandling för att säkerställa informationssäkerhet utgör ett berättigat intresse, i den mån den är absolut nödvändig och proportionell (punkt 49 i ingressen).

Vidare får personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in, vilket är det som kallas för finalitetsprincipen (9 § d PuL och artikel 5.1 b) i dataskyddsförordningen). Eftersom insamlingen av uppgifter i sensor-system sker för såväl ändamål som syftar till verksamhetsutövarens egen informationssäkerhet som ändamål som gäller samhällets informations-säkerhet kommer personuppgifts-behandlingen inte i strid med finalitetsprincipen.

Sammanfattningsvis bedöms att den personuppgiftsbehandling som kommer att ske genom sensorsystem är förenlig med kraven i 9 § PuL och även kraven i dataskyddsförordningen.

Prövningen enligt 10 § personuppgiftslagen

Ytterligare en förutsättning för behandling av personuppgifter med stöd av PuL är att behandlingen föregås av en prövning enligt 10 § PuL. I bestämmelsen anges att personuppgifter bara får behandlas om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för vissa i bestämmelsen angivna ändamål. Samma krav återfinns i artikel 6.1 e i dataskyddsförordningen. I det nu aktuella sammanhanget är det inte möjligt att inhämta ett samtycke av den registrerade.

Ett ändamål som anges i bestämmelsen är om behandlingen är nödvändig för att en arbetsuppgift av *allmänt intresse* ska kunna utföras (10 § d). I

instruktionen för MSB anges att myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området (11 a §). I detta ingår, enligt instruktionen, att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Myndigheten har även enligt instruktionen flera uppgifter kopplade till arbetet med att förebygga och hantera it-incidenter, exempelvis att agera skyndsamt vid it-incidenter med informationsspridning, samordning av åtgärder respektive medverka i arbetet med att avhjälpa eller lindra effekter av det inträffade (11 b §). Sensorsystem syftar till att skydda information och funktionalitet samt att upptäcka it-angrepp. Behandlingen av personuppgifter inom ramen för sensorsystem ska ske för att stärka den till sensorsystem anslutna verksamhetsutövarens informationssäkerhet och samhällets informationssäkerhet. De verksamhetsutövare som ska få ansluta sig till sensorsystem kommer att vara verksamma inom samhällsviktig verksamhet.

Slutsatsen är att arbetsuppgiften, att stärka informationssäkerheten i samhället, bedöms vara av allmänt intresse. Personuppgiftsbehandlingen är därmed tillåten enligt 10 § d PuL och artikel 6.1 e) i dataskyddsförordningen.

Personuppgiftsansvaret

Det är de personuppgiftsansvariga som ska se till att personuppgiftslagen följs. Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Det kan finnas två eller flera personuppgiftsansvariga för en och samma behandling. Den som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas för personuppgiftsbiträde.[4]

MSB anlitas av verksamhetsutövare för att med myndighetens sensorsystem skapa ett skydd mot it-angrepp. Det är verksamhetsutövaren som äger den nätverkstrafik som passerar sensorerna och är därmed personuppgiftsansvarig för behandlingen av densamma. Med stöd av ett avtal med den anlitande verksamhetsutövaren agerar MSB personuppgiftsbiträde för dennas räkning. MSB:s behandling av personuppgifter i egenskap av personuppgiftsbiträde sker i enlighet med det regelverk och de ändamål som gäller för verksamhetsutövaren. Det närmare ansvarsförhållandet mellan MSB och berörd verksamhetsutövare bör tydligt regleras i det avtal som parterna träffar.

Den beskrivna utformningen av personuppgiftsansvaret innebär inte någon avvikelse från den reglering som finns avseende personuppgiftsanvaret i PuL och någon särskild reglering krävs därför inte.

---

[4] Se 3 § PuL. Definitionen i PuL återfinns i liknande lydelse i art. 4 i dataskyddsförordningen.

Bevarandetider för personuppgifter

I 9 § PuL anges att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Därefter ska personuppgifterna avidentifieras eller utplånas. Samma krav om bevarandetider ställs i dataskyddsförordningen (artikel 5.1e). Bestämmelserna i PuL hindrar inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet (8 § andra stycket PuL).

Om uppgifterna som förekommer i sensorsystemets databaser och förteckning kvalificerar sig som allmänna handlingar, ska de tas om hand för arkivering (2 kap. 3 § tryckfrihetsförordningen, TF, samt 3 § arkivlagen [1990:782]). Bestämmelsen om arkivering ger inte en myndighet en rätt att ha kvar personuppgifter som inte längre är nödvändiga i sitt aktiva verksamhetssystem (se t.ex. Datainspektionens beslut 2013-05-31, dnr 1492-2012). En löpande borttagning av personuppgifter som finns i sensorsystem och som inte längre är nödvändig bedöms som en motiverad integritetsskyddande åtgärd och förenlig med bestämmelserna i arkivlagen. Nedan följer en beskrivning av behovet att bevara personuppgifter i sensorsystemets olika delar.

I *detekterings- och trafikflödessensorerna* sparas inga uppgifter, varför frågan om bevaring inte är aktuell vad gäller dessa delar.

Syftet med att bevara uppgifter i sensorsystemets *förteckning* är att kunna använda uppgifterna vid identifieringen av riktade it-angrepp mot anslutna verksamhetsutövare. För att sensorsystemet ska vara så effektivt som möjligt och för att undvika falsklarm är det viktigt att förteckningen endast innehåller uppgifter som kan identifiera it-angrepp. Uppgifter som inte längre är tydligt kopplade till it-angrepp behöver därför tas bort löpande.

I *larmdatabasen* kan det, som nämnts, finnas olika typer av personuppgifter. Personuppgifter i larmdatabasen kommer från dels larm som detekteringssensorn skickar, dels trafikinspelningar av trafik som gjorts i särskilda fall. Larm innehåller endast personuppgifter som redan finns i förteckningen och ip-adresser mellan vilka trafiken som genererade larmet har skickats. Vad gäller trafikinspelningar, kan dessa, om det handlar om e-posttrafik, även bestå av e-postinnehåll. Larmen används till att stödja den drabbade verksamhetsutövaren och till att sprida varningar och information till andra berörda verksamhetsutövare. Larmen används även till att skapa en lägesbild över säkerhetshoten mot anslutna verksamhetsutövare. Med hänsyn till att informationen i larmen behöver användas både för operativ och förebyggande verksamhet är det angeläget för verksamheten att den sparas tillräckligt länge så att syftet med insamlingen av uppgifterna uppnås.

Vad gäller *trafikinspelningar* talar den omständigheten att dessa kan innehålla flera personuppgifter, för att informationen gallras så snart analysen slutförts. Även den omständigheten att inspelningen antingen behövs för att kunna bestämma riktigheten av ett larm eller så snart som möjligt skapa en fullständig bild av ett upptäckt it-angrepp talar för detta. Eftersom nödvändiga åtgärder för att hantera eventuella hot ska kunna vidtas utan dröjsmål, är det centralt för anslutna verksamhetsutövare och MSB att analysen slutförs så snart som möjligt.

Vidare bevaras i *trafikflödesdatabasen* ip-adresser, som skulle kunna kvalificera sig som personuppgift. Detta görs för att tillhandahållaren ska kunna kontrollera om ett nyupptäckt hot har drabbat verksamhetsutövaren redan innan uppgifter om t.ex. den skadliga koden fördes in i förteckningen. Eftersom detekteringssensorn endast letar efter markörer på sådana riktade it-angrepp som finns i förteckningen är det värdefullt att kunna göra en efterkontroll av tidigare trafik, för att säkerställa att verksamhetsutövaren inte drabbats av en specifik skadlig kod redan innan den fördes in i förteckningen. Vissa angrepp är kortvariga och andra byggs upp under lång tid och genom flera olika steg. Det är viktigt att kunna upptäcka vissa nyckelmoment i angreppen för att kunna konstatera att en attack pågår. Utan sådan trafikformation riskerar flera, även pågående attacker, att förbli oupptäckta.

I enlighet med vad som anges i 9 § i PuL är det den personuppgiftsansvariges ansvar att se till att personuppgifterna inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Även dataskyddsförordningen föreskriver denna ansvarsskyldighet för den personuppgiftsansvarige (artikel 5.2).

Informationsplikten i PuL

Enligt 23 § PuL gäller att den personuppgiftsansvarige, i samband med att uppgifter om en person *samlas in* från personen själv, självmant ska lämna information till den registrerade om uppgiftsbehandlingen. Informationsplikten återfinns även i artikel 13 i dataskyddsförordningen. Omfattningen av den information som ska lämnas till den registrerade utökas med den nya dataskyddsförordningen (se särskilt artikel 13.2).

Utgångspunkten är att personuppgifter som samlas in genom sensorerna anses insamlade från personen själv och alltså inte från någon annan källa. Bestämmelsen i 23 § PuL är således tillämplig när sensorerna samlar in personuppgifter. Som redan nämnts, insamlas personuppgifter i form av ip-adresser, under förutsättning att dessa kan kopplas till en fysisk person.

Enligt 27 § PuL gäller inte informationsplikten i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade. Även enligt dataskyddsförordningen

(artikel 23) ges medlemsstaterna möjlighet att begränsa informationsplikten. En sådan begränsning får genomföras om det sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle om syftet är vissa i artikeln angivna åtgärder. Enligt artikel 23.1 e) är en begränsning tillåten om den syftar till att säkerställa en medlemsstats viktiga mål av generellt allmänt intresse.

Enligt 18 kap. 8 § OSL gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden gäller bl.a. telekommunikation eller system för automatiserad behandling av information.

I förarbetena till bestämmelsen anges som exempel på säkerhets- eller bevakningsåtgärder funktioner för användning av lösenord, loggning och kryptering, installation av brandväggar och antivirusprogram samt administrativa rutiner för t.ex. utdelning av lösenord eller bevakning av loggar och larm (prop. 2003/04:93 s. 81 f.).

Syftet med sensorsystemet är att upptäcka skadliga koder och skadliga ip-adresser samt andra, för informationssäkerheten, skadliga uppgifter så att verksamhetsutövaren respektive MSB kan vidta olika åtgärder för att hantera upptäckta it-angrepp. Insamlingen av uppgifterna genom systemet utgör således en säkerhets- och bevakningsåtgärd. Att informera den registrerade om den behandling av personuppgifter som sker i systemet skulle röja den aktuella verksamhetsutövarens och MSB:s informationssäkerhetsåtgärder på ett sådant sätt att syftet med åtgärden motverkas. Mot den bakgrunden görs bedömningen att det är särskilt föreskrivet i lag att uppgifter inte får lämnas ut till den registrerade.

Behandling av känsliga personuppgifter i sensorsystem

Med känsliga personuppgifter avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv (13 § PuL).

Inspelningen av trafik kan inte helt uteslutas innehålla känsliga personuppgifter i de fall larmet berör e-posttrafik och därmed e-postinnehåll.

I personuppgiftslagen finns ett förbud mot att behandla känsliga personuppgifter (13 §). Det är trots förbudet tillåtet att behandla känsliga personuppgifter i de fall som anges i 15-19 §§ PuL. Det rör sig om t.ex. fall då den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort uppgifterna (15 §). Motsvarande förbud mot att behandla känsliga personuppgifter finns i

artikel 9.1 i dataskyddsförordningen.[5] I förordningen föreskrivs även ett antal undantag från förbudet, som i stort sett överensstämmer med undantagen i personuppgiftslagen (artikel 9.2 - 9.4).

Enligt 20 § PuL finns möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om ytterligare undantag från förbudet, om det behövs med hänsyn till ett viktigt allmänt intresse. Även enligt dataskyddsförordningen ges möjlighet att behandla känsliga personuppgifter med hänsyn till ett viktig allmänt intresse (artikel 9.2 g)).[6] Frågan är om det finns anledning att införa en sådan tillåtande bestämmelse som anges i PuL med anledning av att det inte helt kan uteslutas att känsliga personuppgifter kan förekomma i ett e-postmeddelande som sparats med anledning av ett larm.

MSB har inte, med stöd av de föreskrivna undantagen, uttryckligen rätt att behandla känsliga personuppgifter inom ramen för sitt informationssäkerhetsarbete. Samtidigt föreskrivs i 31 § PuL att en personuppgiftsansvarig är skyldig att vidta tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Även enligt dataskyddsförordningen är den personuppgiftsansvarige skyldig att vidta säkerhetsåtgärder i samband med personuppgiftsbehandling (artikel 32). Därutöver föreskrivs i förordningen en skyldighet för den personuppgiftsansvarige att dels anmäla en personuppgiftsincident[7] till tillsynsmyndigheten dels informera den registrerade om en personuppgiftsincident (artikel 33 och 34).

Syftet med sensorsystemet är att bygga upp en ökad förmåga att detektera och hantera it-angrepp som riskerar att drabba verksamhetsutövare inom samhällsviktig verksamhet. Sensorsystemet är utformat och kommer att användas på ett sådant sätt att de personuppgifter som hanteras i verksamheterna skyddas. Det är endast i ett e-postmeddelande, som spelats in, som det skulle kunna finnas känsliga personuppgifter. Eventuella känsliga personuppgifter är inte av intresse för MSB eller den till sensorsystemet anslutna verksamhetsutövaren. Det är endast skadliga ip-adresser och skadliga koder som är av intresse vid analysen och dessa innehåller inga känsliga personuppgifter.

---

[5] I dataskyddsförordningen listas även förbud mot behandling av genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en fysisk person samt uppgift om en fysisk persons sexuella läggning.

[6] I förordningen anges att behandlingen är nödvändig av hänsyn till ett viktig allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

[7] En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats (art. 4 punkt 12 i dataskyddsförordningen).

Frågan är alltså om e-posttrafik med en skadlig kod eller en ip-adress, som har använts i ett it-angrepp mot en verksamhetsutövares datasystem och där det inte kan uteslutas att meddelandet innehåller känsliga personuppgifter, ska leda till slutsatsen att det krävs en särskild förordningsbestämmelse som medger att MSB behandlar känsliga personuppgifter inom ramen för informationssäkerhetsarbetet. Ett sådant resonemang innebär i praktiken att personuppgiftsregleringen skulle utgöra ett hinder för samtliga säkerhetsåtgärder som t.ex. antivirusprogram, som kontinuerligt scannar en verksamhetsutövares trafik efter skadlig kod och andra angrepp. Sådana säkerhetsåtgärder anses i dag utgöra ett nödvändigt skydd för samtliga verksamhetsutövare med nätverk kopplade till internet och utgör därför sådana tekniska och organisatoriska åtgärder som det ställs krav på i 31 § PuL. Det är därför inte rimligt att förbudet mot att behandla känsliga personuppgifter ska leda till att en tillåtande bestämmelse om behandling av känsliga personuppgifter måste införas i säkerhetssyfte.

Dessutom skulle en särskilt tillåtande bestämmelse enligt ovan riskera att ge ett felaktigt intryck av vad de till sensorsystemet anslutna verksamhetsutövarna och MSB vidtar för åtgärder med anledning av ett it-angrepp mot en ansluten verksamhetsutövares verksamhet. Slutsatsen är därför att det inte finns skäl för att införa en särskild bestämmelse om behandling av känsliga personuppgifter som sker inom ramen för den till sensorsystemet anslutna verksamhetsutövaren och MSB:s informationssäkerhetsarbete.

Frågor om offentlighet och sekretess

Reglerna om allmänna handlingars offentlighet ger svenska medborgare en principiell rätt att få tillgång till allmänna handlingar (2 kap. 1 § TF). Även privaträttsliga juridiska personer anses ha rätt att ta del av allmänna handlingar enligt TF (RÅ 2003 ref. 83). Däremot har myndigheter i sig inte någon sådan grundlagsenlig rätt, men en motsvarande rättighet att få information (6 kap. 5 § OSL).

Reglerna om allmänna handlingars offentlighet tillämpas av bl.a. myndigheter och av vissa enskilda organ som anges i 2 kap. 4 § OSL (2 kap. 3 § OSL). Inom ramen för sensorsystem träffas således inte de anslutna enskilda verksamhetsutövarna av skyldigheten att lämna ut allmänna handlingar, såvida de inte är angivna i bilagan till lagen eller är sådana juridiska personer som avses i 2 kap. 3 § OSL. Anslutna enskilda verksamhetsutövare som inte avses i 2 kap. 3 § OSL omfattas inte heller av förbudet att röja uppgift enligt OSL, eller enligt lag eller förordning som OSL hänvisar till (2 kap. 1 § OSL).

Sensorsystem bedöms, som redan nämnts, utgöra en säkerhets- och bevakningsåtgärd som träffas av sekretessbestämmelsen i 18 kap 8 §

OSL. Enligt bestämmelsen gäller sekretess till skydd för det allmännas intresse under vissa förutsättningar för säkerhets- eller bevakningsåtgärd. Enligt punkten 3 i bestämmelsen gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser system för automatiserad behandling av information.

Som framhållits tidigare är det inte sannolikt att känsliga personuppgifter insamlas genom sensorsystemet. Det sällsynta fall som kan bli aktuellt är om ett e-postmeddelande, som spelats in med anledning av ett larm, innehåller uppgift som rör en enskilds personliga förhållanden som t.ex. hälsa. Vid sådant fall gäller sekretess för aktuella uppgifter om det måste antas att den enskilde eller någon närstående till denne kommer att lida betydande men om uppgiften röjs (21 kap. 1 § OSL).

Sekretessbestämmelserna för säkerhets- och bevakningsåtgärd (18 kap. 8 § OSL) och för enskilds personliga förhållanden (21 kap. 1 § OSL) är primära sekretessbestämmelser och består hos alla myndigheter och andra organ som ska tillämpa OSL.

Om sensorsystem tillhandahålls en enskild verksamhetsutövare kan MSB komma att behöva lämna denne sekretessbelagda uppgifter, trots att verksamhetsutövaren inte omfattas av förbudet att röja uppgifter. Främst torde detta aktualiseras när MSB i samband med att den meddelar ett larm till den enskilda verksamhetsutövaren, lämnar information från förteckningen, d.v.s. markören/koden som utlöst larmet. För att skydda sådana uppgifter, som kan omfattas av sekretess (18 kap. 8 § OSL), kan sekretessavtal mellan MSB och de anslutna enskilda verksamhetsutövarna träffas. Det finns också möjlighet att lagreglera om tystnadsplikt, vilket dock inte framstår som nödvändigt i detta fall. Dessutom kan MSB vid behov lämna uppgifter med ett förbehåll som inskränker mottagarens, verksamhetsutövarens i detta fall, rätt att lämna uppgiften vidare eller utnyttja uppgiften (10 kap. 14 § OSL).

Vidare kan den situationen uppstå att MSB får del av uppgifter av en ansluten enskild verksamhetsutövare, som verksamhetsutövaren inte vill ska offentliggöras. Detta torde främst aktualiseras när MSB tar del av falsklarmsunderlag, dvs. kommunikation mellan den enskilda anslutna verksamhetsutövaren och en potentiellt angripande verksamhetsutövare, vilket utgörs av några minuters inspelningar. Den sekretessreglering som finns (t.ex. 18 kap. 8 § OSL, 21 kap. 1 §, 9 kap. 3 § OSL och 1 § lag [1990:409] om skydd för företagshemligheter samt 30 kap. 23 § OSL i kombination med 9 § offentlighets- och sekretessförordningen [2009:641] med bilaga) torde kunna skydda sådan information från att offentliggöras.

Konsekvenser och ikraftträdande

Enligt förslaget är det MSB, i samverkan med Säkerhetspolisen, som efter en begäran av en verksamhetsutövare avgör om MSB:s sensorsystem ska installeras hos verksamhetsutövaren. En begränsning är också att MSB:s sensorsystem endast ska få installeras hos sådana verksamhetsutövare inom samhällsviktiga sektorer som inte erbjuds TDV. Kostnaderna för själva systemet bör finansieras av MSB och bedöms rymmas inom myndighetens befintliga anslag. De verksamhetsutövare som har önskemål om att få ansluta sig till systemet bör själva stå för kostnaden för anslutning och för kostnader som uppstår när systemet löpande anpassas.

Förordningsbestämmelsen bör träda ikraft så snart som möjligt.