Ds 2016:22

Polisens tillgång till information om vissa it-incidenter

REGERINGSKANSLIET
Justitiedepartementet

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Omslag: Regeringskansliets standard
Tryck: Elanders Sverige AB, Stockholm 2016

ISBN 978-91-38-24473-9
ISSN 0284-6012

Förord

Regeringen beslutade den 9 december 2015 att ge Björn Andersson i uppdrag (Ju 2015:K) att bistå Justitiedepartementet med att utreda åtgärder för att öka Polismyndighetens tillgång till information om it-brottslighet. Hovrättsassessorn Malin Stensbäck anställdes för att arbeta som sekreterare inom ramen för uppdraget.

Härmed överlämnas promemorian Polisens tillgång till information om vissa it-incidenter.

Stockholm i juli 2016

Björn Andersson

Malin Stensbäck

Innehåll

Sammanfattning

Statliga myndigheter ska enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap skyndsamt rapportera vissa it-incidenter som inträffat i myndighetens informationssystem till Myndigheten för samhällsskydd och beredskap (MSB).

I promemorian föreslås att MSB ska vara skyldig att lämna uppgifter om sådana rapporterade it-incidenter till Polismyndigheten om det finns anledning att anta att incidenten har sin grund i en brottslig gärning.

Promemorians förslag tar sin utgångspunkt i att det är angeläget att brottsliga gärningar som utgör ett hot mot informationssäkerheten utreds och att de individer som ansvarar för sådana handlingar lagförs. För att öka polisens tillgång till information om it-brott bör polisen ges tillgång till uppgifter om it-angrepp som MSB förfogar över i sin roll som mottagare av obligatoriska it-incidentrapporter.

I promemorian redovisar utredningen sin bedömning att varken bestämmelser om sekretess eller bestämmelser om behandling av personuppgifter normalt utgör ett hinder mot att MSB lämnar information om rapporterade it-angrepp till Polismyndigheten. Utredningen redovisar också sin bedömning att bestämmelserna om sekretess i de brottsbekämpande myndigheternas verksamhet och regelverket i övrigt ger myndigheterna goda förutsättningar att skydda skyddsvärda uppgifter om it-incidenter under utredningen och i domstol vid ett eventuellt åtal.

Statliga myndigheter har en långtgående skyldighet att samarbeta och bistå varandra i den utsträckning som det kan ske. MSB har ett särskilt ansvar att agera skyndsamt vid it-incidenter genom att bl.a. sprida information och samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet.

En naturlig utgångspunkt för utredningen har därför varit att MSB och Polismyndigheten så långt det är möjligt med hänsyn till rättsliga och verksamhetsmässiga förutsättningar själva bör utveckla sin samverkan utifrån sina respektive uppgifter och roller i informationssäkerhetsarbetet. Utredningen har i underhandskontakter med MSB och Polismyndigheten undersökt förutsättningarna för en överenskommelse mellan myndigheterna om ett informationssamarbete om it-incidenter. MSB har emellertid meddelat att myndigheten inte kommer att medverka till en överenskommelse som innebär en skyldighet att lämna uppgifter om rapporterade it-incidenter till Polismyndigheten.

I promemorian lämnas därför förslaget att i förordning reglera en skyldighet för MSB att lämna uppgifter om sådana it-incidenter som rapporterats i enlighet med 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap till Polismyndigheten om det finns anledning att anta att incidenten har sin grund i en brottslig gärning. Utredningen föreslår att uppgiftsskyldighetens närmare omfattning och innebörd, samt formerna för uppgiftslämnandet, inte regleras i förordningen utan bör utformas i samråd mellan myndigheterna.

Som alternativ till en författningsreglerad uppgiftsskyldighet framhåller utredningen möjligheten att regeringen genom myndighetsstyrningen säkerställer att ett effektivt och ändamålsenligt informationssamarbete etableras mellan myndigheterna.

Utredningen bedömer att förslaget får positiva konsekvenser för brottsbekämpningen. Förslagets ekonomiska konsekvenser är sådana att eventuellt ökade kostnader hos berörda myndigheter bedöms kunna finansieras inom befintliga ramar.

Förordningsändringen föreslås träda i kraft den 1 januari 2017.

1 Författningsförslag

1.1 Förslag till förordning om ändring i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

Härigenom föreskrivs att 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
20 § [1]	
Till stöd för arbetet med samhällets informationssäkerhet ska en myndighet till Myndigheten för samhällsskydd och beredskap skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.	
En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapportering enligt första stycket informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.	
Rapporteringsskyldigheten omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633).	
Om det kan antas att en incident som rapporterats till Myndigheten för samhällsskydd	Om det kan antas att en incident som rapporterats till Myndigheten för samhällsskydd

[1] Senaste lydelse 2015:1052.

och beredskap enligt första stycket har sin grund i en brottslig gärning, ska Myndigheten för samhällsskydd och beredskap skyndsamt uppmana den rapporterande myndigheten att anmäla incidenten till polisen	och beredskap enligt första stycket har sin grund i en brottslig gärning, ska Myndigheten för samhällsskydd och beredskap skyndsamt *lämna uppgifter om incidenten till Polismyndigheten.*

Denna förordning träder i kraft den 1 januari 2017.

2 Utredningens uppdrag och genomförande

Som it-incidenter klassificeras händelser som påverkar eller stör olika typer av dataöverföring i it-system, telekommunikationer eller styr- och övervakningssystem m.m. En it-incident kan vara orsakad av handhavandefel, felaktigheter i hård- eller mjukvara eller systemfel, men kan också ha sin grund i en brottslig handling.

Statliga myndigheter är sedan den 1 april 2016 skyldiga att rapportera it-incidenter till Myndigheten för samhällsskydd och beredskap (MSB). Rapporteringsskyldigheten omfattar såväl it-incidenter med antagonistisk bakgrund som övriga incidenter. Jämte denna rapporteringsskyldighet ska myndigheterna anmäla vissa incidenter med koppling till rikets säkerhet till Säkerhetspolisen eller Försvarsmakten i enlighet med bestämmelser i säkerhetsskyddsförordningen (1996:633).

Rapporteringsskyldigheten är en del i en samlad strategi för informations- och cybersäkerhet i staten som föreslogs av NISU 2014 i betänkandet *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (SOU 2015:23).

Med incidentrapporteringen som grund ansvarar MSB bl.a. för att sammanställa information om trender och utveckling avseende it-incidenter och för att i övrigt stödja samhällets informationssäkerhetsarbete.

Det finns även ett samhällsintresse av att it-relaterad brottslighet utreds och att individer som ligger bakom antagonistiska it-angrepp lagförs. Befogenheterna och även skyldigheten att uppdaga, beivra och utreda brott i den digitala miljön åligger de brottsbekämpande myndigheterna.

MSB lämnar inte uppgifter om rapporterade incidenter till Polismyndigheten. MSB är dock skyldig att uppmana rapporterande

myndigheter att anmäla incidenter som kan antas ha sin grund i brottslig gärning till polisen. Sådana uppmaningar lämnades även till myndigheter och andra som frivilligt rapporterade incidenter till MSB före den 1 april 2016. Enligt Polismyndigheten är anmälningar som grundar sig på sådana uppmaningar mycket ovanliga. Den låga anmälningsfrekvensen till polisen och det faktum att det finns ett stort antal it-incidenter som inte utreds utgör enligt Polismyndigheten ett betydande problem.

Regeringen beslutade mot denna bakgrund i december 2015 att ge en utredare i uppdrag att analysera och föreslå åtgärder för att öka Polismyndighetens tillgång till information om it-brottslighet. I detta ligger att överväga om, och i så fall hur, polisen bör kunna få ta del av uppgifter om it-incidenter som rapporteras till MSB av statliga myndigheter och som kan misstänkas ha sin grund i en brottslig handling. En fråga som särskilt ska prövas är om några hinder föreligger på grund av sekretess.

Utredaren ska särskilt analysera och beakta hur en informationsdelning skulle kunna påverka myndigheters benägenhet att rapportera it-incidenter och om MSB skulle bli förhindrad att bistå drabbade myndigheter i händelse av att förundersökning inleds. Utredaren ska också analysera vilka möjligheter som finns att bibehålla sekretess för aktuella uppgifter hos brottsbekämpande myndigheter och hos domstol vid ett eventuellt åtal och även beakta de grundläggande principerna om förhandlingsoffentlighet och parts rätt till insyn i domstolsprocessen.

Utredaren ska föreslå de författningsändringar som övervägandena föranleder. Utredaren ska analysera och redovisa ekonomiska konsekvenser av sina förslag och föreslå hur eventuella kostnader för det allmänna ska finansieras. Uppdraget ska redovisas senast den 11 juli 2016.

Utredningen har under arbetet haft informella möten och täta kontakter med företrädare för MSB och Polismyndigheten. Utredningen har även haft kontakt med företrädare för Säkerhetspolisen, Åklagarmyndigheten, Domstolsverket samt Post- och telestyrelsen. MSB och Polismyndigheten har under arbetet getts tillfälle att under hand lämna synpunkter på bl.a. utredningens bedömning av de rättsliga frågor som uppdraget aktualiserat.

Utredningen har med hjälp av MSB inhämtat information om it-incidentrapportering och frågor om polisiära myndigheters tillgång

till information om sådana incidenter i Nederländerna, Norge och Tyskland. Utredningen har särskilt intresserat sig för frågan om hur CERT-funktionerna i dessa länder samarbetar med polisiära myndigheter.

3 Informations- och cybersäkerhet

3.1 Begrepp och definitioner

I dag betraktar de flesta länder informationssäkerhet som en stor nationell utmaning, och informationssäkerhet inklusive cybersäkerhet anses vara av såväl strategisk som utrikespolitisk och säkerhetspolitisk betydelse. Det är viktigt att ha en helhetssyn på informationssäkerhet eftersom det är ett komplext och gränsöverskridande område, både geografiskt och när det gäller bl.a. teknik, administration, ekonomi, och juridik. Informationssäkerhet är en fråga som berör många områden och verksamheter som bl.a. påverkar svensk säkerhets-, utrikes-, försvars- och näringspolitik.

En storskalig it-incident kan få allvarliga konsekvenser för såväl ekonomi som samhällsviktig verksamhet och kritisk infrastruktur. På grund av samhällets ökade it-beroende är sannolikheten stor att konsekvenserna, genom spridningseffekter, drabbar exempelvis finansiella system, ledningscentraler för trafiksystem, administrativa och medicinska system inom sjukvården, digitala kontrollsystem för el och vatten samt elektroniska kommunikationer.

Informationssäkerhet definieras i detta sammanhang som en strävan efter att skydda information så att den alltid finns tillgänglig när den behövs (tillgänglighet), att det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Informationssäkerhet omfattar såväl administrativa åtgärder för att skydda information som tekniska åtgärder.

Cybersäkerhet omfattar enligt bl.a. EU:s strategi för cybersäkerhet de mekanismer och åtgärder som används för att skydda cyberdomänen mot de hot som är förknippade med eller kan skada dess ömsesidigt beroende nätverk och informationsinfrastruktur.

Cybersäkerhet syftar till att motstå it-angrepp eller it-incidenter, och innebär att upprätthålla förmågan att skydda information som digitalt överförs mellan en eller flera sändare och mottagare samt skyddet av överföringens informationsinfrastruktur likväl som funktionen hos enskilda it-komponenter.

En *it-incident* definieras i Myndigheten för samhällsskydd och beredskaps allmänna råd som en oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet. En it-incident kan vara en händelse som påverkar eller stör data, telekommunikation, hård- eller mjukvara. Orsaken kan vara bristande kompetens, mänskliga misstag, tekniska sammanbrott eller naturhändelser. En it-incident kan också ha sin orsak i en brottslig handling.

3.2 Hot och risker i en digitaliserad värld

I dagens samhälle hanteras större mängder information än någonsin tidigare. Hanteringen sker i allt större omfattning i elektroniska kommunikationsnät och it-system. Det finns stora möjligheter och fördelar med detta. Tekniken gör det möjligt att bl.a. lagra stora mängder information och kunskap som snabbt, även globalt, kan göras tillgänglig för alla. Digitaliseringen av viktiga samhällsfunktioner medför effektivitetsvinster och en ökad öppenhet, tillgänglighet och insyn. Utvecklingen på it-området har bidragit till att förenkla tillvaron för alla; medborgare, företag, organisationer och offentlig sektor.

Den ökade digitaliseringen medför emellertid också en påtagligt ökad sårbarhet för störningar och avbrott. Olika verksamheters beroende av it-system innebär bl.a. att de blir sårbara för handhavandefel, tekniska fel och olyckor. Den ökade öppenheten medför också en större risk för att aktörer med antagonistiska avsikter utnyttjar de möjligheter som den brett åtkomliga informationen ger för hot och angrepp. Brister i säkerheten i informationssystem och nätverk kan få omfattande konsekvenser för såväl samhället i stort som enskilda. Sådana brister kan också leda till att allmänhetens förtroende för offentliga och privata aktörer som tillhandahåller viktiga tjänster försämras.

Många it-incidenter och störningar i informationssystem har icke-antagonistiska orsaker. Sådana it-incidenter kan t.ex. bero på fel i programvara eller hårdvara, eller störningar i stödsystem som t.ex. elförsörjning och kommunikation på grund av väderförhållanden och avgrävda kablar.

Andra it-incidenter kan bero på it-angrepp. Ett it-angrepp är en medveten handling med en antagonistisk viljeyttring från en motståndare som avsiktligt vill visa sin förmåga eller åsamka skada. It-angrepp utförs ständigt och blir alltmer sofistikerade och riktade. Hotutövare finns på alla nivåer. Det kan vara allt från personer som utan egentligt brottsligt uppsåt testar sina kunskaper genom att olovligen försöka ta sig in i informationssystem, till angrepp från stater och statsunderstödda aktörer med bl.a. politiska och militära syften. En stor del av den grova it-brottsligheten riktar in sig på att bl.a. kompromettera informationssystem för att otillbörligen komma åt information. Många terrorgrupper har etablerat sin närvaro på internet.

Att genomföra ett angrepp kräver i dag inte någon stor kompetens eftersom det går att få tag i programvara som är särskilt utvecklad för it-angrepp av olika slag. Angrepp som utförs med hjälp av sådan programvara är relativt osofistikerade och ofta enkla att spåra på internet. Andra angrepp kan utgå från ett ideologiskt eller politiskt betingat motiv och tar sig uttryck i överbelastningsattacker (DDos), lösenordsstöld, intrång i system och manipulering av hemsidor. Det förekommer också att en angripare installerar skadlig kod på offrets dator som gör det möjligt för angriparen att kryptera datorn eller delar av den. Angriparen kräver sedan offret på pengar för att denne ska återfå kontrollen över det som har krypterats.

3.3 Politikens inriktning

Målen för Sveriges säkerhet är att värna befolkningens liv och hälsa, samhällets funktionalitet och förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter (prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292). Målen för samhällets krisberedskap är att minska risken för olyckor och kriser som hotar vår säkerhet samt värna

människors liv och hälsa samt grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter genom att upprätthålla samhällsviktig verksamhet och hindra eller begränsa skador på egendom och miljö då olyckor och krissituationer inträffar (prop. 2015/16:1, utgiftsområde 6 s. 77).

I regeringens skrivelse (skr. 2009/10:124) *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet* anges att målen för samhällets informationssäkerhet är följande:

- Säkra samhällets funktionalitet, effektivitet och kvalitet.
- Bidra till samhällets brottsbekämpning.
- Stärka samhällets förmåga att förebygga och hantera allvarliga störningar och kriser.
- Främja näringslivets tillväxt.
- Värna medborgares fri- och rättigheter och personliga integritet.
- Öka medborgares och verksamheters kunskap om och förtroende för informationshantering och it-system.

När det gäller politikens inriktning uttalas i budgetpropositionen för 2016 (prop. 2015/16:1 utgiftsområde 6 s. 92) bl.a. följande om informationssäkerhet.

> Det förändrade omvärldsläget medför bl.a. att nya konstellationer av aktörer och tillvägagångssätt skapas och att hot och risker uppstår och förändras snabbare. Det blir därför allt svårare att dra en tydlig gräns mellan det civila samhällets behov av informations- och cybersäkerhet, och skyddet för Sveriges säkerhet och skyddet mot terrorism.
>
> Regeringen anser att det för att stärka informations- och cybersäkerheten krävs en förbättrad samordning och samverkan i syfte att få en helhetssyn vad gäller hoten, det som ska skyddas och säkerhetsåtgärderna. Det måste också säkerställas att statens informationstillgångar har ett tillräckligt skydd och att det är tydligt vilka regelverk som ska gälla.
>
> En del i arbetet med att skapa en helhetssyn är att införa ett system för obligatorisk it-incidentrapportering för i första hand statliga myndigheter.

I budgetpropositionen för 2016 uttalar regeringen också att Riksrevisionens rapport *Informationssäkerhet i den civila statsförvaltningen* (RiR 2014:23), betänkandet *Informations- och cyber-*

säkerhet i Sverige. Strategi och åtgärder för säker information i staten (SOU 2015:23) samt betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) visar på att det finns ett behov av att vidta åtgärder för att stärka informations- och cybersäkerheten i Sverige. Regeringen avser därför att även fortsättningsvis prioritera informations- och cybersäkerhetsområdet.

3.4 Riksrevisionens granskningar

Riksrevisionen har vid flera tillfällen sedan 2005 granskat informationssäkerhetsarbetet i statsförvaltningen. Riksrevisionen har också granskat om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott. Granskningarna har visat ett flertal brister.

Riksrevisionens rapport Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen (RiR 2007:10)

Riksrevisionen granskade under 2005–2007 arbetet med informationssäkerhet vid elva myndigheter i statsförvaltningen. Slutsatsen var att myndigheterna inte utifrån gängse normer arbetade systematiskt med sin interna styrning och kontroll av informationssäkerheten. Riksrevisionen rekommenderade regeringen att tydligare fokusera på informationssäkerhetsfrågorna, ge expertmyndigheterna tydligt mandat att följa upp och rapportera om myndigheternas arbete med informationssäkerheten samt ge myndigheterna bättre förutsättningar genom att ställa tydligare krav på arbetet med informationssäkerheten.

Riksrevisionens rapport Informationssäkerheten i den civila statsförvaltningen (RiR 2014:23)

Under 2014 granskade Riksrevisionen om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker.

Riksrevisionens övergripande slutsats var att arbetet med informationssäkerhet inte är ändamålsenligt, sett till de hot och risker som finns. Regeringen har enligt Riksrevisionen inte någon samlad lägesbild som inkluderar hot, i vilken omfattning och mot vilka hoten realiseras samt vilka skyddsåtgärder myndigheterna vidtar. En sådan lägesbild har inte heller någon av regeringens stöd- och tillsynsmyndigheter.

För att förbättra statens informationssäkerhet rekommenderade Riksrevisionen därför regeringen bl.a. att snarast införa en obligatorisk incidentrapportering för samtliga myndigheter och att ge en myndighet i uppdrag att hantera denna rapportering.

Riksrevisionens rapport Informationssäkerhetsarbete på nio myndigheter (RiR 2016:8)

Mot bakgrund av tidigare granskningar har Riksrevisionen återigen granskat hur nio myndigheter arbetar med informationssäkerhet. De granskade myndigheterna är desamma som de som granskades under perioden 2005–2007. Granskningen omfattar också Ekonomistyrningsverket samt regeringen och dess kansli med utgångspunkt från intern styrning och kontroll.

Granskningen visar att myndigheterna har allvarliga brister i sitt informationssäkerhetsarbete. Regeringen har inte heller sett till att nödvändiga förutsättningar finns för myndigheterna att ha ett ändamålsenligt informationssäkerhetsarbete.

Riksrevisionen lämnar med anledning av granskningen också vissa rekommendationer till regeringen i syfte att få till stånd ett förstärkt informationssäkerhetsarbete.

Riksrevisionens rapport It-relaterad brottslighet – polis och åklagare kan bli effektivare (RiR 2015:21)

Riksrevisionen har granskat om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott.

Bakgrunden till granskningen är det växande problemet med it-relaterad brottslighet. I rapporten anges att de personuppklarade brotten för all brottslighet har sjunkit från 18 till 15 procent under

perioden 2006–2014, vilken är den lägsta nivån hittills, och att personuppklaringen för de granskade it-relaterade brotten ligger konstant lägre och var 7 procent år 2014. Riksrevisionen uttalar att det är viktigt att Polismyndigheten och andra delar av rättsväsendet förmår hålla jämna steg med utvecklingen på området för att det brottsutredande arbetet inte ska försämras. När människor drabbas av brott och ärendena skrivs av i stället för att utredas, finns det en risk att förtroendet för rättsväsendet påverkas negativt.

Granskningen omfattar tre brottskategorier; it-bedrägerier, internetrelaterade barnpornografibrott och attacker mot infrastruktur.

Sammantaget visar granskningen att bristen på vedertagna metodstöd, utvecklade arbetssätt, tillräcklig kompetens och specialisering inom området gör att polis och åklagare inte har beredskap och förmåga att utreda och handlägga it-relaterade brott på ett effektivt och ändamålsenligt sätt. De identifierade bristerna riskerar också att leda till att it-relaterade brott inte hanteras likvärdigt och enhetligt, och att det i högre grad blir personberoende hur ett ärende utreds. Samtidigt visar granskningen att det finns möjligheter till förbättrad personuppklaring med ett förändrat arbetssätt.

Riksrevisionen rekommenderar Polismyndigheten och Åklagarmyndigheten att bl.a. identifiera nationella utvecklingsbehov och utveckla den strategiska kompetensförsörjningen för att kunna säkerställa verksamhetens behov, samt att planera, uppmuntra och skapa utrymme för kompetenshöjande åtgärder inom it-området. Polismyndigheten rekommenderas också att utnyttja de fora som finns för internationell samordning och samverkan.

3.5 Aktuella utredningar

För att möta hot och risker inom det informationsteknologiska området har två utredningar nyligen haft i uppdrag att se över frågor som rör samhällets informationssäkerhet.

Utredningen om säkerhetsskyddslagen

För verksamheter som har betydelse för rikets säkerhet finns det regler om informationssäkerhet i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Sedan säkerhetsskyddsregleringen trädde i kraft 1996 har informationstekniken och användningen av den genomgått en betydande utveckling. En särskild utredare har bl.a. mot den bakgrunden haft i uppdrag att göra en översyn av säkerhetsskyddslagstiftningen. En del av utredningens uppdrag har varit att föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade. Utredningen har också haft i uppdrag att se över hur tillsynen över säkerhetsskyddet bör vara utformat och att ta ställning till om ett system med sanktionsåtgärder bör införas.

Utredningen överlämnade sitt betänkande, *En ny säkerhetsskyddslag* (SOU 2015:25) i mars 2015. I betänkandet föreslås en ny och moderniserad säkerhetsskyddslag som bl.a. svarar mot utvecklingen på informationsteknikområdet.

Betänkandet har remissbehandlats och bereds för närvarande i Regeringskansliet.

NISU 2014

I slutet av 2013 gavs en särskild utredare i uppdrag att föreslå en strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system (dir. 2013:110). Uppdraget lämnades mot bakgrund av att informationssäkerhet är en prioriterad fråga och dessutom en del i arbetet med att nå målen för Sveriges säkerhet och samhällets krisberedskap. It-utvecklingens effekter omfattar även utmaningar för svensk säkerhets- och försvarspolitik och arbetet med samhällets informationssäkerhet, som en del i det nationella säkerhetsarbetet, måste fördjupas. (prop. 2014/15:1 utgiftsområde 6 s. 97)

Utredningen, som antog namnet NISU 2014, redovisade betänkandet *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (SOU 2015:23) i mars 2015. Den strategi som föreslås har sex mål:

- att stärka styrning och tillsyn inom området,
- att staten ska ställa tydliga krav vid upphandling på it-området,
- att statliga myndigheter ska kommunicera säkert,
- att samtliga statliga myndigheter rapporterar it-incidenter,
- att arbetet med att förebygga och bekämpa it-relaterad brottslighet stärks och
- att Sverige ska vara en stark internationell partner.

Åtgärderna ska säkerställa att de statliga myndigheterna har ett gemensamt förhållningssätt till informationssäkerhetsfrågor och behovet av skyddad kommunikation samt säkra it-lösningar. Andra åtgärdsförslag innebär att det skapas förutsättningar för de brottsbekämpande myndigheterna att garantera samma skydd mot cyberbrottslighet som mot brottslighet i allmänhet. Exempel på förslag i den delen är att arbetet med ratificering av Europarådets konvention om it-relaterad brottslighet slutförs och att en översyn görs av bestämmelserna om tvångsmedel i 27 och 28 kap. brottsbalken och övriga lagrum för att säkerställa att brottsbekämpande myndigheter kan bedriva sin förebyggande och utredande verksamhet i den digitala miljön. Det föreslås också att regeringen stärker och samordnar insatserna för att främja Sveriges ställning i internationella samarbeten om informations- och cybersäkerhet.

Betänkandet har remissbehandlats.

I december 2015 beslutade regeringen förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. I och med detta infördes ett system för obligatorisk it-incidentrapportering för statliga myndigheter. Rapporteringsskyldigheten gäller sedan den 1 april 2016 (se avsnitt 4.3.3).

Betänkandet i övrigt bereds för närvarande i Regeringskansliet.

3.6 Internationellt arbete

Cybersäkerhetsfrågor är till sin natur globala och utmaningarna måste bemötas genom internationella samarbeten. I detta avsnitt lämnas en övergripande redogörelse för internationellt arbete med

informationssäkerhetsfrågor där fokus ligger på bekämpningen av cyberbrottslighet. Redogörelsen är inte avsedd att vara en fullständig genomgång. Av redogörelsen framgår dock att arbete med bekämpning av cyberbrottslighet är högst aktuellt och bedrivs i ett flertal olika forum.

3.6.1 Europeiska unionen

Enisa

Inom EU finns ENISA (European Union Agency for Network and Information Security), som är EU:s byrå för nät- och informationssäkerhet och ett expertcentrum för it-säkerheten i Europa. Enisa hjälper EU och EU-länderna att bättre förebygga, upptäcka och åtgärda problem. Enisa tar fram praktiska råd och lösningar för den offentliga och privata sektorn i EU-länderna och för EU-institutionerna och ska bland annat hålla krisövningar, ta fram strategier för it-säkerhet och främja kapacitetsuppbyggnad och samarbete mellan incidenthanteringsorganisationer. Enisa publicerar också rapporter och studier om it-säkerhet om bland annat kartläggning av it-hot. Enisa är med och tar fram EU:s politik och lagstiftning om nät- och informationssäkerhet.

En europeisk cybersäkerhetsstrategi

Europeiska kommissionen och utrikestjänsten (EEAS) presenterade i februari 2013 en övergripande europeisk cybersäkerhetsstrategi – *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd.* Informationssäkerhet, it-relaterad brottslighet och it-relaterade utrikes- säkerhets- och försvarspolitiska frågor är substansmässigt viktiga delar av strategin. Genomförande och uppföljning av strategin, liksom andra frågor som berör EU:s internationella cyberpolitik, hanteras övergripande i den tillfälliga arbetsgruppen inom området, Friends of the Presidency Group on Cyber issues (FoP), som tillsattes i november 2012. Syftet med gruppen är att öka medlemsstaternas insyn, förbättra det horisontella arbetet och stärka samordningen såväl internt som externt avseende cyberfrågor i vid mening.

I strategin tydliggörs de principer som bör styra riktlinjerna för cybersäkerhet inom EU och internationellt. Den vision som presenteras i strategin består av fem strategiska prioriteringar. En av dessa är att drastiskt minska cyberbrottsligheten. Med cyberbrottslighet avses en mängd olika brottsliga aktiviteter där datorer och informationssystem används, antingen som verktyg eller mål. Cyberbrottslighet omfattar enligt strategin traditionella brott som bedrägeri och identitetsstöld, innehållsrelaterade brott som spridning av barnpornografi, samt brott som är unika för datorer och informationssystem, t.ex. angrepp mot informationssystem, överbelastningsattacker och skadlig programvara. En annan strategisk prioritering är att uppnå cyberberedskap. För att främja cyberberedskap inom EU anges att både offentliga myndigheter och den privata sektorn måste utveckla kapacitet och samarbeta effektivt. I strategin anges bl.a. att nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet bör rapportera incidenter som misstänks vara av allvarlig brottslig karaktär till brottsbekämpande myndigheter. De rättsliga skyldigheterna bör enligt strategin vare sig ersätta eller förebygga det informella och frivilliga samarbete, även mellan den offentliga och privata sektorn, som sker i syfte att förbättra säkerheten och utbyta information och bästa praxis.

Direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen – NIS-direktivet

Samtidigt som EU:s cybersäkerhetsstrategi presenterades överlämnade kommissionen ett direktivförslag om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen. Förslaget till direktiv om nät- och informationssäkerhet (NIS-direktivet) är en viktig del i den övergripande cybersäkerhetsstrategin. Syftet med direktivet är att uppnå och vidmakthålla en hög gemensam nät- och informationssäkerhet inom hela EU för att förbättra den inre marknadens funktion.

NIS-direktivet innehåller bl.a. skyldigheter för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem och att utse myndigheter med särskilda uppgifter på detta område. Medlemsstaterna blir vidare skyldiga att identifiera operatörer som bedriver samhällsviktig verksamhet inom sju sektorer och som är

beroende av nätverk och informationssystem. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur. För aktörerna inom de angivna sektorerna innebär direktivet bl.a. att it-incidenter av viss dignitet ska rapporteras till behörig myndighet. Direktivet bedöms träda i kraft under sommaren 2016. Medlemsstaterna är skyldiga att ha genomfört direktivet senast 21 månader därefter.

Kommittédirektiv – Genomförande av EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem

Regeringen har utsett en särskild utredare som ska föreslå hur NIS-direktivet ska genomföras i svensk rätt (kommittédirektiv 2016:29). Uppdraget ska redovisas senast den 1 maj 2017. Frågan om hur en nationell strategi för säkerhet i nätverk och informationssystem bör utformas omfattas emellertid inte av utredarens uppdrag. Regeringen bedömer att det förslag om antagande av en nationell strategi för statens informations- och cybersäkerhet som föreslås i betänkandet *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (SOU 2015:23) bör kunna anpassas för att motsvara direktivets krav på vad en nationell strategi för säkerhet i nätverk och informationssystem ska innehålla. Det betänkandet har remitterats och bereds för närvarande inom Regeringskansliet.

Europol – EC3

I januari 2013 inrättades ett Europeiskt Cybercrime Center (EC3) vid Europol. EC3 utgör knutpunkten för EU:s it-brottsbekämpning och ett stöd för medlemsstaterna i det operativa arbetet. Centret ska bidra till snabbare och effektivare insatser mot den it-relaterade brottsligheten och fokusera på bl.a. brott som påverkar kritisk infrastruktur och informationssystem inom EU. Centret ska bl.a. tillhandahålla strategiska analyser, arbeta med forskning, utveckling och utbildning samt utveckla samarbete med den privata sektorn och andra viktiga funktioner inom området.

I september 2014 inleddes ett sex månader långt pilotprojekt vid EC3, Joint Cybercrime Taskforce (J-CAT), i syfte att effektivisera arbetet med att bekämpa it-brottslighet. I projektet deltog representanter från vissa av EU:s medlemsstater, från brottsbekämpande aktörer utanför EU, bl.a. Federal Bureau of Investigation och Secret Service, samt från EC3. Projektet är nu under utvärdering.

3.6.2 OECD

OECD har sedan 1992 arbetat med att utveckla rekommendationer och riktlinjer för regeringar och andra intressenter i syfte att underlätta hanteringen av säkerhetsutmaningar i den digitala miljön ur ett ekonomiskt och socialt perspektiv.

Ett exempel på sådana rekommendationer är *Digital Security Risk Management for Economic and Social Prosperity*, som antogs 2015. Rekommendationen är ett resultat av arbetet med att uppdatera en tidigare rekommendation på området, *OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* (”Security Guidelines”). Målet med Security Guidelines var bl.a. att främja en säkerhetskultur som ett sätt att skydda informationssystem och nät samt att uppmuntra samarbete och utbyte av relevant information vid utformningen och användningen av regler, åtgärder, rutiner m.m. som rör säkerheten.

I den nya rekommendationen från 2015 uppmanas regeringar att anta en nationell strategi för att hantera digitala säkerhetsrisker. Rekommendationen innehåller vidare generella principer. Principerna handlar bl.a. om att medvetandegöra alla berörda om vilka digitala säkerhetsrisker som de kan utsättas för genom utbildning och därigenom också ge nödvändiga färdigheter för att kunna bedöma och hantera dessa. Alla har ett gemensamt ansvar, utifrån den egna rollen eller verksamheten. Ambitionen är att rekommendationen ska främja ett mer holistiskt synsätt när det gäller hanteringen av säkerhetsrisker på det digitala området. Rekommendationen förväntas också etablera nya samordningsmekanismer såväl inom staten som med icke-statliga intressenter, samt främja ett förbättrat privat-offentligt samarbete på inhemsk, regional och internationell nivå.

Ett annat exempel på rekommendation är *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*, som beskriver olika koncept för skydd av kritiska infrastrukturer och hur dessa definieras i olika länder. Fokus ligger på hur regeringarna kan demonstrera ett ledarskap och engagemang när det gäller riskhantering i samarbete med den privata sektorn. Informationsspridning är exempel på åtgärder som kan initieras.

3.6.3 FN

Inom FN förekommer arbete med informations- och cybersäkerhet på ett flertal sätt. Ett exempel är FN-organet den Internationella teleunionen (ITU) som hanterar vissa frågor relaterade till cybersäkerhet. IMPACT (International Multilateral Partneship Against Cyber Threats) är den verkställande delen av organet och den första internationella alliansen mot digitala hot. IMPACT ger ITU:s medlemsstater tillgång till expertis, utrustning och resurser för att effektivisera hanteringen av cyberhot.

3.6.4 Londonprocessen

Den så kallade Londonprocessen har informellt fått beteckna de internationella cyberkonferenser som tog sin början genom ett brittiskt initiativ 2011. I London anordnades då en konferens för att diskutera normer inom ramen för cybersäkerhetsfrågor, med förhoppningen att öka samstämmigheten inom dessa frågor i den internationella debatten. Diskussionerna fortsatte i Budapest 2012, i Seoul 2013, och med *Global Conference on Cyberspace* i Haag 2015. Samtliga konferenser har berört aspekter angående ekonomiska möjligheter på internet, cyberbrott och internationell säkerhet. Nästa cyberkonferens kommer att hållas i Mexiko 2017.

3.6.5 OSSE

Verksamheten i Organisationen för säkerhet och samarbete i Europa (OSSE) tar sin utgångspunkt i ett brett säkerhetsbegrepp som omfattar militärpolitiska aspekter, demokrati och mänskliga rättigheter samt ekonomi och miljö.

En viktig roll är att bygga förtroende mellan medlemsländerna. Genom ökat förtroende kan risken för konflikter minska. 2013 beslutade medlemsstaterna att anta en första uppsättning av förtroendeskapande åtgärder inom cybersäkerhetsområdet. Åtgärderna syftar till att främja samarbete, transparens, förutsägbarhet och stabilitet och således minska risken för missförstånd, eskalering eller konflikter i cyberrymden. I beslutet betonas att implementeringen av åtgärderna ska vara i linje med internationell rätt. De deltagande åtar sig att frivilligt deklarera aspekter av nationella och transnationella hot angående information- och kommunikationsteknologi. Staterna kan även, på frivillig basis, bistå med konsultationer för att minska riskerna för missförstånd och politisk spänning. För att ytterligare reducera missförstånd i brist på en gemensam syn på terminologifrågor har stater möjlighet att tillkännage nationellt definierade termer relaterade till cybersäkerhet.

3.6.6 Europarådet

Europarådets verksamhet omfattar bl.a. konventioner inom områden som it-brottslighet, dataskydd och skydd för barn. Europarådet är aktivt inom olika internationella internetrelaterade forum.

2001 antogs Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen). Konventionen syftar huvudsakligen till att harmonisera lagstiftning och förenkla internationellt samarbete och därigenom skapa en gemensam straffrättslig policy för skyddet av samhället mot cyberbrottslighet. Majoriteten av EU:s medlemsländer har ratificerat konventionen. Även stater som inte är medlemmar i Europarådet kan ansluta sig till konventionen. Sverige undertecknade Budapestkonventionen 2001 men har inte ratificerat den.

I tilläggsprotokoll till konventionen behandlas frågor om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som begåtts med hjälp av datorsystem.

3.6.7 Interpol

Internationella polissamarbetsorganisationen (Interpol) har cyberbrottslighet som ett särskilt prioriterat brottsområde och fokuserar på att samordna insatser och aktörer, kompetens och kapacitetsbyggande samt operationellt och forensiskt stöd. Genom Interpol Global Complex for Innovation (IGCI) i Singapore och avdelningen Interpol Digital Crime Centre tillhandahåller Interpol en global koordineringsfunktion för cyberbrottslighet. Centrets verksamhet omfattar forskning, utbildningar i den senaste tekniken och koordinering av specifika insatser.

4 Samhällets informationssäkerhet

4.1 Myndighetsorganisationen på informationssäkerhetsområdet

Det finns flera statliga myndigheter med särskilda uppgifter eller uppdrag på informations- och cybersäkerhetsområdet. Myndigheten för samhällsskydd och beredskap (MSB) Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Säkerhetspolisen, Polismyndigheten, Försvarets materielverk (FMV) och Försvarsmakten är sådana myndigheter. Myndigheterna ingår i samverkansgruppen för informationssäkerhet (SAMFI).

4.1.1 SAMFI

SAMFI bildades 2003 sedan regeringen föreslagit en strategi för samhällets informationssäkerhet (prop. 2001/02:158 – *Samhällets säkerhet och beredskap*). Syftet är att underlätta samarbetet mellan vissa myndigheter med uppgifter på informationssäkerhetsområdet.

I samband med att MSB bildades 2009 fick myndigheten ansvaret för SAMFI. SAMFI-gruppen träffas nu sex gånger per år. De myndigheter som medverkar är MSB, PTS, FRA, Säkerhetspolisen, Polismyndigheten, FMV och Försvarsmakten.

MSB har i samverkan med övriga myndigheter i SAMFI tagit fram en strategi för samhällets informationssäkerhet 2010–2015, och 2012 publicerade myndigheterna en handlingsplan i syfte att stärka informationssäkerheten i samhället och förverkliga strategin.

Enligt den vision SAMFI-gruppen har enats om ska SAMFI verka för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt genom informationsutbyte och samverkan stödja

de medverkande myndigheternas arbete avseende samhällets informationssäkerhet i syfte att uppfylla visionen.

SAMFI berör frågeställningar inom huvudsakligen följande aktivitetsområden:

- strategi, handlingsplan och regelverk
- tekniska frågor och standardiseringsfrågor
- nationell och internationell utveckling inom informationssäkerhetsområdet
- informationsaktiviteter
- övningar och utbildning
- hantering och förebyggande av it-incidenter

MSB avsätter resurser för SAMFI:s kansli. Övriga myndigheter bidrar med resurser vid behov och efter förmåga.

4.1.2 Myndigheten för samhällsskydd och beredskap (MSB)

MSB:s ansvarsområden och uppgifter anges i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap. Enligt 1 § har MSB ansvar för frågor om skydd mot olyckor, krisberedskap och civilt förvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris. Myndigheten ska

1. utveckla och stödja samhällets beredskap mot olyckor och kriser och vara pådrivande i arbetet med förebyggande och sårbarhetsreducerande åtgärder,
2. arbeta med samordning mellan berörda aktörer i samhället för att förebygga och hantera olyckor och kriser,
3. bidra till att minska konsekvenser av olyckor och kriser,
4. följa upp och utvärdera samhällets krisberedskapsarbete, och
5. se till att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde.

När det gäller förebyggande och förberedande arbete ska MSB enligt 2 § i samverkan med myndigheter, kommuner, landsting, organisationer och företag identifiera och analysera sådana sårbarheter, hot och risker i samhället som kan anses vara särskilt allvarliga. Myndigheten ska vidare tillsammans med de ansvariga myndigheterna genomföra en övergripande planering av åtgärder som bör vidtas. Myndigheten ska värdera, sammanställa och rapportera resultatet av arbetet till regeringen.

Myndigheten ska se till att utbildning inom krisberedskapsområdet tillhandahålls. Myndigheten ska därtill genomföra övningar inom sitt ansvarsområde. Myndigheten ska vid behov stödja Regeringskansliet i utbildnings- och övningsverksamheten inom krisberedskapsområdet. Vidare ska myndigheten se till att ledningsmetoder, stödsystem och materiel för räddningstjänst och krishantering utvecklas och tillhandahålls. (5 §)

MSB ska ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att

1. samordna krishanteringsåtgärderna,
2. samordna information till allmänhet och media,
3. effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och
4. samordna stödet till centrala, regionala och lokala organ ifråga om information och lägesbilder.

Myndigheten ska ha förmågan att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser. (7 §)

MSB ska såväl områdesvis som på en övergripande samhällsnivå följa upp och utvärdera krisberedskapen och bedöma om vidtagna åtgärder fått önskad effekt. Myndigheten ska kunna göra en samlad bedömning av olycksutvecklingen och det säkerhetsarbete som är kopplat till denna. (10 §)

Myndigheten ska se till att erfarenheter tas till vara från inträffade olyckor och kriser. Till stöd för detta ska myndigheten tillhandahålla tvärsektoriella och samlade bilder och bedömningar

samt utveckla kompetens och metodik inom området som tillgodoser nationella, regionala och lokala behov. (11 §)

När det gäller informationssäkerhet ska MSB 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. Myndigheten ska årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Inför sammanställning av rapporten ska myndigheten inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till de myndigheterna enligt 10 a § säkerhetsskyddsförordningen (1996:633). Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder på olika nivåer och områden i samhället. (11 a §)

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 §). Myndigheten ska

1. agera skyndsamt vid it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,
2. återrapportera till berörda aktörer i samband med att en it-incident har rapporterats,
3. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och
4. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

Myndigheten ska vara Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur enligt artikel 10.1 i rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och

klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (17 a §).

MSB:s arbete med informationssäkerhet, funktionen CERT-SE m.m.

Vid MSB:s avdelning för utveckling av samhällsskydd finns Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet. Dess huvudsakliga uppgift är att stödja och samordna arbetet med samhällets informations- och cybersäkerhet samt arbetet med skydd av samhällsviktig verksamhet. I arbetet ingår att analysera och bedöma omvärldsutvecklingen. Verksamheten svarar för regelgivning och för utveckling av samhällets arbete med kontinuitetshantering och kritiska beroenden. Verksamheten ska lämna råd och stöd i förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Verksamheten svarar för den nationella funktionen för stöd till samhället i arbetet med att hantera och förebygga it-incidenter, CERT-SE. Verksamheten delas in i enheten för operativ cybersäkerhet och it-incidenthantering, enheten för skydd av kritisk infrastruktur och cybersäkerhet, samt enheten för systematiskt informationssäkerhetsarbete. Arbetet inom avdelningen bedrivs nationellt, inom det nordiska samarbetet samt inom EU och internationellt.

Enheten för systematiskt informationssäkerhetsarbete ska lämna råd och stöd om förebyggande informationssäkerhetsarbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. I detta ingår att lämna råd och stöd till statliga myndigheter, kommuner och landsting i arbetet med risk- och sårbarhetsanalyser samt kontinuitetshantering på området informationssäkerhet. Enheten ansvarar för webbplatsen Informationssäkerhet.se. Enheten ansvarar för att analysera och bedöma omvärldsutvecklingen inom sitt område och ska ingå i verksamhetsövergripande analysarbete. Personal från enheten ska vid behov ingå i Nationell operativ samverkansfunktion för cybersäkerhet (NOS).

Enheten för skydd av kritisk infrastruktur och cybersäkerhet ska driva och hålla samman arbetet med skydd av samhällsviktig verksamhet och ansvara för myndighetens uppgifter att vara Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur

enligt Europaparlamentet och rådets direktiv 2008/114/EG. I detta ingår att stödja och utveckla samhällets arbete med kontinuitetshantering och kritiska beroenden samt att arbeta med rymdvädersamordning. Enheten ska, med fokus på kritisk informationsinfrastruktur, lämna råd och stöd till tekniskt förebyggande arbete inom området till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Enheten svarar för myndighetens arbete med säkra kryptografiska funktioner för det civila samhället och för arbetet med myndighetens uppdrag vad avser eter- och medieberedskap. Enheten leder och samordnar arbetet med informationssäkerhet i myndighetens externa kommunikationstjänster för ledning och samverkan så att den externa kravställningen tillgodoses. Enheten ansvarar vidare för att analysera och bedöma omvärldsutvecklingen inom sitt område och ingå i verksamhetsövergripande analysarbete. Personal från enheten ska vid behov ingå i Nationell operativ samverkansfunktion för cybersäkerhet (NOS).

Enheten för operativ cybersäkerhet och it-incidenthantering ska som en del i arbetet med att stödja samhället med att hantera och förebygga it-incidenter upprätthålla funktionen CERT-SE som är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. CERT-SE är en del av det internationella nätverket av Computer Emergency Response Teams (CERT). I detta ingår att upprätthålla Nationell operativ samverkansfunktion för cybersäkerhet (NOS). Enheten ska vara den operativa kontaktpunkten gentemot motsvarande funktioner i andra länder. Enheten ska säkerställa att verksamheten i sin helhet kan agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov samordna åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Enheten har ansvar för att operativt stödja arbetet med it-säkerhet i de av myndighetens externa kommunikationstjänster för ledning och samverkan som kräver detta. Enheten ansvarar för webbplatsen CERT.se. Enheten ansvarar för att analysera och bedöma omvärldsutvecklingen inom sitt område. I detta ingår löpande omvärldsbevakning, att producera och delge anpassad information till relevanta aktörer, samt att ingå i verksamhetsövergripande analysarbete.

Samverkan

MSB deltar i ett flertal samarbeten som rör informations- och cybersäkerhet, både nationellt och internationellt. Bland de internationella samarbetena kan nämnas samarbetet mellan de nordiska CERT-funktionerna, och samarbetet inom nätverket European Government CERTs (EGC) group. CERT-SE är också medlem nätverken TF-CSIRT (Task Force – Collaboration of Security Incident Response Teams), FiRST (Forum of Incident Response and Security Teams) och IWWN (International Watch and Warning Network).

MSB deltar också i EU-kommissionens expertgrupp European forum for member states (EFMS), som utgör en plattform för att främja utbytet mellan medlemsstaterna om god praxis, information och erfarenheter om allmänpolitiska frågor av betydelse för skyddet av kritisk infrastruktur. MSB deltar även i den privat-offentliga plattformen för nät- och informationssäkerhet (NIS-plattformen). NIS-plattformen har samma mål som EU:s strategi för cybersäkerhet samt NIS-direktivet och syftar bl.a. till att säkerställa en harmoniserad tillämpning av åtgärderna i direktivet inom hela EU.

MSB representerar också Sverige i Natos planeringsgrupp för industriella resurser och kommunikation (IRCSG).

När det gäller nationell samverkan ingår MSB bl.a. i den nationella telesamverkansgruppen (NTSG). I gruppen, som har initierats av PTS, ingår utöver MSB operatörer inom sektorn elektronisk kommunikation, Svenska Kraftnät, Teracom, Trafikverket ICT och Försvarmakten. Gruppen verkar i syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället.

MSB har vidare i samverkan med Totalförsvarets forskningsinstitut (FOI) etablerat Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3), som är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Verksamheten vid NCS3 syftar till att minska de risker som nyttjandet av industriella informations- och styrsystem medför för det moderna samhället, speciellt med avseende på avsiktlig störning. Inom NCS3 sker forskning, utbildning och övningar för myndigheter och företag som äger

och/eller arbetar med samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

För att utnyttja samhällets samlade kompetens på informationssäkerhetsområdet har MSB knutit till sig ett informationssäkerhetsråd med representation från både offentlig förvaltning och näringslivet. Rådet består av representanter från Polismyndigheten, PTS, Säkerhetspolisen, FRA, Vattenfall AB, .SE (Stiftelsen för Internetinfrastruktur), Karlstads universitet, Försvarsmakten, Ericsson, Riksbanken, Västra Götalandsregionen, Försvarshögskolan, Riksgälden, FMV och Scania AB. Informationssäkerhetsrådet har i uppgift att bistå MSB med bl.a. information om utvecklingstrender inom området informationssäkerhet samt att bidra till spridning av information om MSB:s arbete med informationssäkerhet i omvärlden.

4.1.3 Polismyndigheten

Den 1 januari 2015 ombildades de tidigare 21 polismyndigheterna, Rikspolisstyrelsen och Statens kriminaltekniska laboratorium till en sammanhållen myndighet, Polismyndigheten. Samtidigt ombildades Säkerhetspolisen till en fristående myndighet.

Polismyndighetens arbete syftar till att upprätthålla allmän ordning och säkerhet samt i övrigt tillförsäkra allmänheten skydd och annan hjälp (1 § polislagen [1984:387]). Till Polismyndighetens uppgifter hör att

1. förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten,
2. övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat,
3. utreda och beivra brott som hör under allmänt åtal,
4. lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen,
5. fullgöra den verksamhet som ankommer på Polismyndigheten enligt särskilda bestämmelser.

Polismyndigheten och Säkerhetspolisen ska samarbeta med varandra och med åklagarmyndigheterna. Polismyndigheten och Säkerhetspolisen ska också samarbeta med andra myndigheter och organisationer vilkas verksamhet berör polisverksamheten. Andra myndigheter ska ge polisen stöd i dess arbete. (6 § polislagen)

Polismyndigheten och Åklagarmyndigheten, och i förekommande fall Säkerhetspolisen, ska tillsammans utveckla verksamheten med att utreda och lagföra brott (22–22 a §§ förordningen [2014:1102] med instruktion för Polismyndigheten).

Polismyndigheten ska samarbeta med Säkerhetspolisen i den utsträckning som behövs för att polisverksamheten ska kunna bedrivas effektivt. Polismyndigheten och Säkerhetspolisen ska i samråd bestämma och fortlöpande utveckla formerna för samverkan och samordning mellan myndigheterna. (26 § förordningen [2014:1102] med instruktion för Polismyndigheten).

Polismyndigheten ska fortlöpande upplysa Säkerhetspolisen om förhållanden som kan ha betydelse för dess verksamhet. Polismyndigheten ska omedelbart underrätta Säkerhetspolisen om den upptäcker vissa brott, bland annat brott mot 18 eller 19 kap. brottsbalken eller annat brott mot rikets säkerhet samt brott mot lagen (2003:148) om straff för terroristbrott. Säkerhetspolisen får i samråd med Polismyndigheten meddela föreskrifter om vilka andra typer av brott och andra företeelser som kan beröra Säkerhetspolisens ansvarsområde och som Säkerhetspolisen ska underrättas om (27 § förordningen [2014:1102] med instruktion för Polismyndigheten).

Om Säkerhetspolisen i ett enskilt fall begär det och det inte finns särskilda skäl mot det, ska Polismyndigheten bistå vid polisverksamhet som leds av Säkerhetspolisen. Polismyndigheten ska lämna tekniskt biträde och annan hjälp till Säkerhetspolisen i den utsträckning som myndigheterna kommer överens om (28 § förordningen [2014:1102] med instruktion för Polismyndigheten).

4.1.4 Säkerhetspolisen

Säkerhetspolisen bedriver i egenskap av säkerhetstjänst underrättelse- och säkerhetsarbete. Säkerhetspolisens huvudsakliga uppgifter och ansvar framgår av 3 § polislagen (1984:387). Till Säkerhetspolisens uppgifter hör att

1. förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott,
2. utreda och beivra sådana brott som anges i 1 eller som följer av 5,
3. fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
4. fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627),
5. leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för.

Säkerhetspolisen får, utöver vad som följer av 47 § säkerhetsskyddsförordningen (1996:633), ge råd om säkerhetsskydd. Säkerhetspolisen får även i övrigt ge råd för att förebygga brott mot rikets säkerhet eller andra särskilt viktiga samhällsintressen.

Polismyndigheten och Säkerhetspolisen ska samarbeta med varandra och med åklagarmyndigheterna. Polismyndigheten och Säkerhetspolisen ska också samarbeta med andra myndigheter och organisationer vilkas verksamhet berör polisverksamheten. Andra myndigheter ska ge polisen stöd i dess arbete. (6 § polislagen)

Säkerhetspolisen ska samarbeta med Polismyndigheten i den utsträckning som behövs för att polisverksamheten ska kunna bedrivas effektivt. Säkerhetspolisen och Polismyndigheten ska i samråd bestämma och fortlöpande utveckla formerna för samverkan och samordning mellan myndigheterna. Säkerhetspolisen bör, i den utsträckning sekretess inte hindrar det, upplysa Polismyndigheten om förhållanden som kan ha betydelse för dess verksamhet. Om Polismyndigheten i ett enskilt fall begär det och det inte finns särskilda skäl mot det, ska Säkerhetspolisen bistå vid polisverksamhet som leds av Polismyndigheten. Säkerhetspolisen ska lämna tekniskt

biträde och annan hjälp till Polismyndigheten i den utsträckning som myndigheterna kommer överens om (10–12 §§ förordningen [2014:1103] med instruktion för Säkerhetspolisen).

4.1.5 Övriga myndigheter i SAMFI

Post- och telestyrelsen (PTS)

Post- och telestyrelsen (PTS) är den myndighet som bevakar områdena elektronisk kommunikation och post i Sverige. Begreppet elektronisk kommunikation innefattar telekommunikationer, it och radio. PTS ska verka för att målen inom politiken för informationssamhället uppnås. PTS har till uppgift att bl.a. verka för robusta elektroniska kommunikationer och minska risken för störningar samt verka för ökad krishanteringsförmåga. PTS har vidare i uppgift att verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer. PTS har också i uppgift att lämna råd och stöd till myndigheter, kommuner och landsting samt företag, organisationer och andra enskilda i frågor om nätsäkerhet. PTS ska också vara det behöriga organ som får begära råd och stöd enligt Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004. (förordningen [2007:951] med instruktion för Post- och telestyrelsen).

PTS är tillsynsmyndighet enligt lagen (2003:389)om elektronisk kommunikation (LEK). LEK reglerar villkoren för att tillhandahålla elektroniska kommunikationstjänster. Bestämmelserna i LEK syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet (1 §). I lagen finns bl.a. bestämmelser om säkerhet som gäller för den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. Till skillnad från bland andra Säkerhetspolisen, FRA och MSB, har PTS inte något ansvar för att inhämta, analysera eller vidare-

förmedla information om informationssäkerheten på myndigheterna i statsförvaltningen. PTS har i stället ett sektorsansvar som innefattar bland annat tillsyn över de aktörer som tillhandahåller elektroniska kommunikationer (tjänster och nät) oavsett associationsrättslig form.

PTS är mottagare av rapporter om integritetsincidenter respektive driftsincidenter enligt LEK.

PTS utövar tillsyn även enligt bl.a. lagen (2006:24) om nationella toppdomäner för Sverige på Internet.

PTS ansvarade tidigare för Sveriges it-incidentcentrum (Sitic). Sedan 2011 har MSB övertagit denna funktion, som numera benämns CERT-SE.

Försvarsmakten

Försvarsmakten ska upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Försvarsmakten ska försvara Sverige och främja svensk säkerhet.

Bland Försvarsmaktens verksamhetsuppgifter ingår att bedriva omvärldsbevakning och upptäcka och identifiera yttre hot mot Sverige och svenska intressen samt ta fram underlag för beslut om höjd beredskap. Försvarsmakten ska även bedriva försvarsunderrättelseverksamhet, leda och bedriva militär säkerhetstjänst, leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information, samt biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet. (1–3 §§ och 3 b § 1–4 förordningen [2007:1266] med instruktion för Försvarsmakten) Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret, förutom i fråga om verkställigheten av 18 § förordningen (2015:1053) om totalförsvar och höjd beredskap (33 §).

Försvarsmakten har ansvar för kontroll av säkerhetsskyddet när det gäller Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet. Försvarsmakten får också meddela föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) för sitt tillsynsområde, dock inte när det gäller

omfattningen av inventeringen av vissa hemliga handlingar. (39 och 44 §§ säkerhetsskyddsförordningen [1996:633])

Huvuddelen av Försvarsmaktens uppgifter enligt säkerhetsskyddsförordningen hanteras av den militära underrättelse- och säkerhetstjänsten (MUST), som är en del av Försvarsmakten.

Den militära säkerhetstjänstens uppgift är att ta tillvara de säkerhetsintressen som främst berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen samt att samverka rörande skyddet av rikets säkerhet och skydd mot terrorism med Säkerhetspolisen. Den militära säkerhetstjänsten består av säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst, där signalskyddstjänsten är att anse som en säkerhetsskyddsangelägenhet.

I egenskap av tillsynsmyndighet avseende säkerhetsskyddet hos vissa myndigheter är Försvarsmakten mottagare av it-incidentrapporter i vissa fall.

Försvarsmakten ansvarar för skydd av sina egna lednings- och informationssystem.

Försvarets materielverk (FMV)

Försvarets materielverk levererar försvarslogistik genom att utforma och förse försvaret med försvarsmateriel och logistiktjänster. Försvarets materielverk ska på uppdrag av Försvarsmakten vidmakthålla, destruera och kassera varor, upphandla byggentreprenader, varor och tjänster och tillhandahålla logistiktjänster (1 § förordningen [2007:854] med instruktion för Försvarets materielverk). Vid Försvarets materielverk finns ett nationellt certifieringsorgan för it-säkerhet i produkter och system. Materielverket, certifieringsorganet, ska i sin verksamhet beakta nationella säkerhetsintressen, verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat samt vara Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat (CCRA) och motsvarande överenskommelse inom Europa (SOG-IS MRA). Försvarets materielverk får inom sitt verksamhetsområde även tillhandahålla tjänster åt andra än Försvarsmakten. (5–6 §§ förordningen [2007:854] med instruktion för Försvarets materielverk)

Försvarets radioanstalt (FRA)

Försvarets radioanstalt (FRA) har till uppgift att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning (1 § förordningen [2007:93] med instruktion för Försvarets radioanstalt). Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller vissa i lagen särskilt utpekade myndigheter närmare har bestämt inriktningen av signalspaningen. Signalspaningen får vidare ske endast i vissa syften, bl.a. för att kartlägga yttre militära hot mot landet, strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen, allvarliga yttre hot mot samhällets infrastrukturer, främmande underrättelseverksamhet mot svenska intressen, eller främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik. (1 § lagen [2008:717] om signalspaning i försvarsunderrättelseverksamhet) FRA:s signalspaning kräver tillstånd från Försvarsunderrättelsedomstolen och granskas löpande av Siun, Statens inspektion för försvarsunderrättelseverksamheten.

FRA ska särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, och utföra matematiska bedömningar av kryptosystem för totalförsvaret. FRA ska också biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem. (2 och 3 §§ förordningen [2007:937] med instruktion för Försvarets radioanstalt)

FRA ska vidare ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser, och ge annat tekniskt stöd. Myndigheten ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

(4 § förordningen [2007:937] med instruktion för Försvarets radioanstalt)

4.2 Reglering av säkerhetsskydd, krishantering och informationssäkerhetsarbete

Ett flertal författningar berör frågor om samhällets informationssäkerhet. Här redovisas översiktligt ett urval av sådana författningar som bedöms vara av särskilt intresse för utredningen.

4.2.1 Säkerhetsskyddslagstiftningen

Bestämmelser om säkerhetsskydd finns i säkerhetsskyddslagen (1996:627). Med säkerhetsskydd avses skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, och som rör rikets säkerhet, och skydd mot terroristbrott (terrorism) enligt lagen (2003:148) om straff för terroristbrott, även om brotten inte hotar rikets säkerhet (6 §). Lagen gäller för staten, kommunerna och landstingen samt för bolag, föreningar och stiftelser som dessa har ett rättsligt bestämmande inflytande över. Lagen gäller också för enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Säkerhetsskyddet ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet), att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning), och att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet ska även i övrigt förebygga terrorism (7 §). Vid utformningen av informationssäkerheten ska behovet av skydd vid automatisk informationsbehandling beaktas särskilt (9 §).

Närmare bestämmelser om säkerhetsskydd finns i säkerhetsskyddsförordningen (1996:633). Myndigheter och andra som förordningen gäller för ska undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka

anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning (säkerhetsanalys) ska dokumenteras. (5 §)

När det gäller informationssäkerhet gäller bl.a. att hemliga handlingar som är av synnerlig betydelse för rikets säkerhet ska inventeras minst en gång per år (9 §). Om en hemlig uppgift kan ha röjts ska det skyndsamt anmälas till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa (10 §). En myndighet ska skyndsamt anmäla till den myndighet som enligt 39 § utövar tillsyn över säkerhetsskyddet om det inträffat en it-incident i myndighetens informationssystem och incidenten allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa, incidenten allvarligt kan påverka säkerheten i ett informationssystem som särskilt behöver skyddas mot terrorism, eller incidenten upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt. En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med sådan rapportering informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten. Om det har inträffat en sådan incident som ska rapporteras till Försvarsmakten, ska den rapporterande myndigheten också skyndsamt informera Säkerhetspolisen. (10 a §) Innan en myndighet inrättar ett register, som ska föras med hjälp av automatiserad behandling och som kan förutses komma att innehålla sådana uppgifter att utlämnandet av dem var för sig eller sammanställda kan skada totalförsvaret, ska myndigheten samråda med Försvarsmakten och, om uppgifternas natur ger anledning till det, Säkerhetspolisen. I fråga om uppgifter av betydelse för rikets säkerhet i övrigt ska i motsvarande fall samråd ske med Säkerhetspolisen. Ett system som av flera personer ska användas för automatiserad behandling av hemliga uppgifter ska vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten. Systemet får inte tas i drift förrän det har godkänts från säkerhetssynpunkt av den för vars verksamhet systemet inrättas. (12 §) Myndigheter och andra som förordningen gäller för ska, innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll, förvissa sig om att det för uppgifterna där finns en fullgod informationssäkerhet.

Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten. (13 §)

Säkerhetspolisen och Försvarsmaketen har ansvaret för att kontrollera säkerhetsskyddet hos myndigheterna (39 §). Säkerhetspolisen och Försvarsmakten har vidare, med stöd av 43–44 §§ meddelat verkställighetsföreskrifter för respektive tillsynsområde. I föreskrifterna finns bestämmelser om bl.a. informationssäkerhet.

4.2.2 Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap beslutades i december 2015 och ersatte den tidigare gällande förordningen (20016:942) om krisberedskap och höjd beredskap. Förordningen innehåller liksom sin föregångare föreskrifter som bl.a. reglerar krisberedskapen. Bestämmelserna syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och inför och vid höjd beredskap. Med krisberedskap avses förmågan att genom utbildning, övning och andra åtgärder samt genom den organisation och de strukturer som skapas före, under och efter en kris förebygga, motstå och hantera krissituationer. Varje myndighet, vars ansvarsområde berörs av en krissituation, ska vidta de åtgärder som behövs för att hantera konsekvenserna av denna. Myndigheterna ska samverka och stödja varandra vid en sådan krissituation.

När det gäller informationssäkerhet ansvarar varje myndighet för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. (19 §)

Genom förordningen infördes den obligatoriska it-incidentrapporteringen för statliga förvaltningsmyndigheter, se avsnitt 4.3.3.

MSB:s tillämpningsföreskrifter

Med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap har MSB utfärdat föreskrifter på informationssäkerhetsområdet.

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) ansluter till 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Enligt föreskrifterna ska varje myndighet bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Med ledningssystem för informationssäkerhet avses ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet samt löpande och regelbunden information lämnas till myndighetsledningen. Ledningssystemet ska utformas utifrån verksamhetens behov och vara styrande för all hantering av information som myndigheten ansvarar för. En myndighet ska vidare upprätta bl.a. en informationssäkerhetspolicy. Av informationssäkerhetspolicyn ska ansvarsfördelningen för verksamhetens informationsmängder framgå. Myndigheten ska eftersträva en god säkerhetskultur där alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering. I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten bl.a. klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd. Utifrån informationsklassningen ska myndigheten genomföra analys av hot och risker samt identifiera och vidta de åtgärder som krävs för att uppfylla skyddsbehovet. Myndigheten ska också följa upp och utvärdera vidtagna åtgärder och gjorda bedömningar av hot och risker samt kontinuerligt utveckla skyddet för att över tid upprätthålla informationens behov av säkerhet. Myndigheten ska slutligen bl.a. ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten till-

handahåller åt en annan organisation. Myndigheten ska ha rutiner för att lära av sådana inträffade incidenter och utförda åtgärder.

MSB har också utfärdat föreskrifter om civila myndigheters kryptoberedskap (MSBFS 2009:11) och om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2015:3). MSB har också utfärdat föreskrifter om statliga myndigheters rapportering av it-incidenter, se avsnitt 4.3.3.

4.3 Särskilt om obligatorisk it-incidentrapportering

Regeringen beslutade i december 2015 förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Genom förordningen infördes den nya ordningen med obligatorisk it-incidentrapportering för statliga förvaltningsmyndigheter. Samtidigt beslutade regeringen att i säkerhetsskyddsförordningen (1996:633) införa en bestämmelse om skyldighet för myndigheter och andra som omfattas av den förordningen att skyndsamt anmäla vissa it-incidenter med koppling till rikets säkerhet till den myndighet som utövar tillsyn över säkerhetsskyddet. Bestämmelsen är ett förtydligande av vad som även tidigare gällde ifråga om skyldigheten att skyndsamt anmäla till Säkerhetspolisen om en hemlig uppgift kan ha röjts och röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa.

4.3.1 Bakgrund till reformen

Regeringen har vid ett flertal tillfällen under lång tid uttalat behovet av en funktion för it-incidentrapportering.

I prop. 2001/02:158, *Samhällets säkerhet och beredskap*, redovisade regeringen en organisatorisk struktur för informationssäkerheten i samhället. Som ett led i detta inrättades en it-incidentfunktion vid Post- och Telestyrelsen (PTS) under namnet Sitic. Funktion är numera överförd till MSB och benämnd CERT-SE.

I prop. 2003/04:93, *Några frågor om sekretess, m.m.,* framhölls vikten av att myndigheter och enskilda organisationer rapporterade it-incidenter till PTS för att PTS skulle kunna fullgöra sitt uppdrag att stödja samhället i arbetet med skydd mot it-incidenter.

I propositionen 2004/05:175, *Från IT-politik för samhället till politik för it-samhället*, konstaterade regeringen till en början att en ändring i sekretesslagen (1980:100) som trädde i kraft 2004 ökade möjligheterna för Sitic att få in rapporter om it-incidenter, eftersom Sitic då kunde sekretessbelägga rapporter som bedöms känsliga. Regeringen konstaterade också att det visat sig att Sitic:s viktigaste uppgift blivit omvärldsbevakning och informationsspridning, att få sårbarheter upptäcktes genom rapporteringen, men att många var intresserade att ta del av Sitic:s varningar och råd. De delar av uppdraget för Sitic som rörde it-incidentrapportering och statistik borde enligt regeringen därför omformuleras. Genom att sekretesslagen hade ändrats så att möjligheten att sekretessbelägga incidentrapporter blivit större, fanns det en förhoppning om att frekvensen för inrapporteringen skulle öka.

I prop. 2007/08:92, *Stärkt krisberedskap – för säkerhets skull*, uttalade regeringen att en samlad lägesbild utgör grunden för att aktörerna i krisberedskapssystemet ska kunna genomföra lämpliga åtgärder och samverka och att förmågan att skapa samlade lägesbilder borde stärkas. Regeringen uttalade att samhällets resurser behöver samordnas och samverka vid kriser för att utnyttjas på ett effektivt sätt. Det ansågs inte tillräckligt att inom det egna ansvarsområdet ha en uppfattning om vad som har hänt, vilka konsekvenserna blir och vad det ställer för krav på agerande. Det krävs också en uppfattning om hur andra aktörer har uppfattat krisen och vilka åtgärder de vidtar. Det egna agerandet måste sättas in i ett bredare perspektiv. Därför finns det ett behov av samlade lägesbilder och samlad lägesuppfattning som sträcker sig över sektorsgränser och ansvarsnivåer, nationellt och i vissa fall även inom EU och internationellt.

I budgetpropositionen för 2010 (prop. 2009/10:1, utgiftsområde 6) uttalade regeringen återigen att det fanns ett behov av att samla resurserna för att skapa goda förutsättningar för att förebygga it-incidenter liksom för att hantera dem när de inträffar. Rapporteringen av it-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behövde enligt regeringen förbättras.

För att stärka samhällets informationssäkerhet och förmåga att förebygga och hantera it-incidenter beslutade regeringen 2010 att ge MSB i uppdrag att utreda hur ett system för obligatorisk it-

incidentrapportering för statliga myndigheter kunde utformas (Fö2010/701/SSK). MSB redovisade uppdraget 2011 och föreslog en dubbelriktad rapporteringsprocess för inrapportering till MSB/CERT-SE och återkoppling till berörda parter. Systemet föreslogs bli obligatoriskt för statliga myndigheter och frivilligt för andra aktörer i samhället.

I budgetpropositionen för 2012 (prop. 2011/12:1, utgiftsområde 6) angavs beträffande informationssäkerhet att anpassning av skyddsåtgärder är viktigt i arbetet med skydd av samhällsviktig verksamhet. Regeringen uttalade att sådan anpassning förutsätter kännedom om antal incidenter och omfattning, för att förstärka möjligheten till samlat agerande vid it-incidenter där konsekvenserna av dessa bedöms bli omfattande. Obligatorisk it-incidentrapportering ansågs kunna vara en del i det arbetet. Regeringen ansåg dock att det var nödvändigt att göra en fördjupad analys avseende bl.a. vilken typ av information en myndighet ska åläggas att samla in och rapportera och till vilken myndighet som rapportering skulle ske. Regeringen uttalade också att förutom MSB:s behov utifrån myndighetens samordnande roll vid olyckor och kriser och vid hantering av it-incidenter kunde även Rikspolisstyrelsen ha behov av it-incidentrapportering eftersom en it-incident som innefattar en brottslig handling faller inom polisens ansvarsområde.

MSB fick under 2012 i regeringsuppdrag att göra en fördjupad analys av sitt tidigare förslag om obligatorisk it-incidentrapportering för statliga myndigheter (Fö2012/717/SSK). I uppdraget ingick särskilt att utreda de rättsliga förutsättningarna samt att beskriva några centrala begrepp inom området samhällets informationssäkerhet. MSB redovisade uppdraget 2012 (Nationellt system för it-incidentrapportering. Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap).

I budgetpropositionen för 2013 (prop. 2012/13:1 utgiftsområde 6) upprepade regeringen att information om det aktuella läget vid en allvarlig händelse är en förutsättning för att de inblandade aktörerna ska få en ömsesidig förståelse för situationen och kunna bedriva samordnade åtgärder. Regeringen uttalade vidare att det krävs mycket god kunskap om hur normalläget ser ut för att kunna agera vid allvarliga it-incidenter och att en förutsättning för att kunna agera är en bra gemensam lägesbild med många inblandade

aktörer och kontakter med nyckelaktörer både nationellt och internationellt.

I budgetpropositionen för 2014 (prop 2013/14:1, utgiftsområde 6) uttalade regeringen återigen att information om det aktuella läget vid en allvarlig händelse är en förutsättning för att de inblandade aktörerna ska få en ömsesidig förståelse för situationen och kunna bedriva samordnade åtgärder. Ett system för obligatorisk it-incidentrapportering kan bidra i detta avseende.

I budgetpropositionen för 2015 (prop. 2014/15:1, utgiftsområde 6) uttalade regeringen att informationssäkerhet är en prioriterad fråga och dessutom en del i arbetet med att nå målen för Sveriges säkerhet och samhällets krisberedskap. Regeringen hänvisade vidare till utredningen om strategi och mål för överföring av information i elektroniska kommunikationsnät och it-system (dir. 2013:110, NISU 2014) och uttalade att resultatet av utredningen kan komma att bli ett centralt verktyg för att hålla samman det nationella och det internationella arbetet inom informationssäkerhetsområdet och för att nå Sveriges politiska mål.

4.3.2 NISU 2014

I mars 2015 överlämnade NISU 2014 sitt betänkande *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (SOU 2015:23). I betänkandet föreslog utredningen bl.a. att ett obligatoriskt system för it-incidentrapportering skulle inrättas för samtliga statliga myndigheter.

Utredningen konstaterade att det fanns en tydlig politisk vilja i Sverige att genom en förstärkt it-funktion för incidentrapportering öka samhällets förmåga att förebygga och hantera incidenter som hotar eller skadar samhällsviktig verksamhet. Utredningen hänvisade också till den uppdragsredovisning som MSB lämnat 2012 där MSB uttryckt att en obligatorisk it-incidentrapportering är nödvändig för att bedriva ett effektivt arbete med informationssäkerhet i samhället och att en sådan rapportering skulle ge kunskap om hot och risker. Detta skulle ge en bra och underbyggd lägesbild, vilket är en förutsättning för att kunna säkerställa att rätt åtgärder vidtas.

Utredningen hänvisade också till Riksrevisionens rapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23), där det konstateras att varken regeringen eller stöd- eller tillsynsmyndigheterna har den fulla bilden av i vilken omfattning hot realiseras eller vilka skyddsåtgärder som myndigheterna vidtar. Utredningen instämde i Riksrevisionens rekommendation till regeringen om att införa obligatorisk incidentrapporteringför samtliga myndigheter.

Med hänsyn tagen särskilt till Försvarsmaktens och Säkerhetspolisens utpekade uppgifter inom säkerhetsskyddet, borde enligt utredningens mening rapportering av it-incidenter med huvudsaklig koppling till sådana informationssystem i vilka hemliga uppgifter enligt offentlighets- och sekretesslagen (2009:400) behandlas i mer än ringa omfattning i första hand rapporteras till de myndigheter som utövar ett tillsynsansvar över säkerhetsskyddet i berörd verksamhet. Sådana särskilda informationssystem kan ha anordnats för att möta särskilda krav på säkerhet som ställts med stöd av säkerhetsskyddslagen (1996:627) eller för att handha uppgifter om totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

Enligt NISU 2014 borde i övrigt MSB, med hänsyn till det uppdrag som MSB enligt sin instruktion har på informationssäkerhetsområdet, vara den myndighet som tar emot rapporterna. Utredningen föreslog också att MSB skulle ges rätt att utfärda verkställighetsföreskrifter om den närmare utformningen av ett system för obligatorisk incidentrapportering.

Betänkandet remitterades. Från Polismyndigheten framfördes under remissförfarandet vissa synpunkter på utformningen av utredningens förslag om obligatorisk it-incidentrapportering. Polismyndigheten uttalade att det ur ett strikt polisiärt perspektiv kan vara bättre med ett system som utformats så att allvarliga informationssäkerhetsincidenter som rör misstanke om brott och som inte omfattas av Säkerhetspolisens tillsynsområde istället rapporteras till polisen som första mottagare. Polismyndigheten framhöll att en stor del av de incidenter som MSB kommer att få kännedom om sannolikt kommer att utgöra brott, vilket får till följd att MSB får kännedom om brott mot statliga myndigheter utan krav på, eller på grund av sekretesshinder möjlighet, att överlämna uppgifterna till polisen för utredning och lagföring. Från en polisiär

utgångspunkt är det viktigt att polisen i ett inledande skede får vetskap om incidenterna för att kunna bedöma om brott föreligger. Polismyndigheten betonade att tidsfaktorn ofta är avgörande i ärenden som gäller it-brott. Uppgifter rörande incidenten finns ofta hos flera aktörer och det är tidskritiskt att säkra bevis hos dessa. En angripare kan finnas var som helst i världen och det är avgörande att komma igång snabbt med brottsutredande åtgärder såsom spårningar och begäran om rättshjälp. En konsekvens av att polisen inte får tillgång till information i direkt anslutning till att incidenten inträffat kan enligt remissyttrandet bli att polisen inte klarar av att utreda brottet.

4.3.3 It-incidentrapportering enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

I december 2015 beslutade regeringen förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, och att därvid införa obligatorisk it-incidentrapportering för statliga myndigheter.

En it-incident definieras i detta sammanhang som en oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet. En it-incident kan vara en händelse som påverkar eller stör data, telekommunikation, hård- eller mjukvara. Orsaken kan vara bristande kompetens, mänskliga misstag, tekniska sammanbrott eller naturhändelser. (Myndigheten för samhällsskydd och beredskaps allmänna råd om statliga myndigheters rapportering av it-incidenter)

Förordningen trädde ikraft den 1 april 2016. Statliga myndigheter blev då skyldiga att, till stöd för arbetet med samhällets informationssäkerhet, skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Rapportering ska ske till MSB. (20 § förordningen [2015:1052] om krisberedskap och bevakningsansvariga

myndigheters åtgärder vid höjd beredskap) En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapportering informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.

Rapporteringsskyldigheten omfattar inte incidenter som enligt 10 a § säkerhetsskyddsförordningen (1996:633) ska rapporteras till Säkerhetspolisen eller Försvarsmakten. Exempel på sådana incidenter är incidenter i informationssystem där hemliga uppgifter som rör rikets säkerhet behandlas eller i system som särskilt behöver skyddas mot terrorism.

Om det kan antas att en incident som rapporterats till MSB har sin grund i en brottslig gärning, ska MSB skyndsamt uppmana den rapporterande myndigheten att anmäla incidenten till polisen.

MSB:s tillämpningsföreskrifter

MSB har med stöd av bemyndigande meddelat föreskrifter, MSBFS 2016:2, om statliga myndigheters rapportering av it-incidenter. Enligt 3 § kan de rapporteringspliktiga it-incidenterna utgöras av kategorierna

1. störning i mjuk- eller hårdvara,
2. störning i driftmiljö,
3. informationsförlust eller informationsläckage,
4. informationsförvanskning,
5. hindrad tillgång till information,
6. säkerhetsbrist i en produkt,
7. angrepp,
8. handhavandefel,
9. oönskad eller oplanerad störning i kritisk infrastruktur, eller
10. annan plötslig oförutsedd händelse som lett till skada.

Enligt 4 § ska varje myndighet rapportera en it-incident senast 24 timmar efter det att myndigheten upptäckt incidenten.

Rapporterna ska enligt 5 § lämnas till MSB via anvisade kontaktvägar.

Enligt 6 § ska en rapport innehålla

1. myndighetens namn,
2. en beskrivning av it-incidenten som även inkluderar en övergripande redovisning av händelseförlopp och vidtagna åtgärder,
3. den exakta eller uppskattade tidpunkten för när it-incidenten inträffade,
4. när myndigheten upptäckte it-incidenten och om den alltjämt pågår eller är avslutad,
5. till vilken eller vilka kategorier enligt 3 § som it-incidenten hör, samt
6. myndighetens initiala bedömning av it-incidentens omfattning och konsekvenser, både faktiska och potentiella.

I rapporten ska om möjligt även anges bedömd sekretess för den information som rapporteras in. Om den rapporterande myndigheten vid sin interna incidentutredning konstaterar att inrapporterade uppgifter om kategorier, omfattning och konsekvenser varit missvisande eller felaktiga ska myndigheten komplettera eller korrigera sin rapport så snart som möjligt.

På begäran av MSB ska en rapporterande myndighet enligt 7 § lämna uppgifter som kompletterar rapporteringen enligt 6 §. Sådana uppgifter ska lämnas snarast, om inget annat överenskommits med MSB.

Enligt 8 § får en myndighet som inte kan lämna en rapport enligt 6 § i samråd med MSB lämna en preliminär rapport. Samråd ska ske innan tidsfristen för rapportering enligt 4 § går ut. Rapporten ska innehålla den information som finns att tillgå vid inrapporteringstillfället samt när myndigheten upptäckte it-incidenten, om den fortfarande pågår eller är avslutad, samt vilken eller vilka kategorier i 3 § som orsakat incidenten. Den fullständiga rapporten enligt 6 § ska i ett sådant fall lämnas senast två veckor från det att it-incidenten upptäcktes.

Om en myndighet överlåter en del av sin informationshantering till en icke statlig aktör ska myndigheten, enligt 9 §, i överlåtelse-

avtalet se till att motparten åtar sig att rapportera it-incidenter i berörda system till myndigheten på ett sätt som motsvarar kraven enligt MSB:s föreskrifter. Myndigheten ska utan dröjsmål vidarebefordra en sådan rapport till MSB. Den skyldigheten gäller med avseende på avtal som träffas efter den 4 april 2016.

En myndighet som har polisanmält en it-incident behöver enligt 10 § inte lämna en rapport enligt 6 § utan endast en kopia på polisanmälan.

Något om tillämpningen hittills

Den nya ordningen med obligatorisk it-incidentrapportering har genomförts parallellt med denna utrednings genomförande. MSB har under dessa månader byggt upp och bemannat funktionen och utformat tillämpningsföreskrifter för rapporteringen. MSB har arbetat aktivt i förhållande till rapporteringsskyldiga myndigheter för att underlätta tillämpningen av regelverket och säkerställa en hög rapporteringsgrad.

Utredningen har under arbetets gång tagit del av uppgifter från MSB om omfattningen och karaktären av de it-incidenter som rapporterats under april och maj månad 2016. Utredningen vill med hänsyn till att reformen just trätt i kraft understryka att stor försiktighet måste iakttas när slutsatser av dessa uppgifter ska dras.

MSB har före införandet av obligatorisk it-incidentrapportering tagit del av rapporter om incidenter som myndigheter och andra aktörer frivilligt lämnat till myndigheten. Enligt uppgift till utredningen har MSB under senare år hanterat i storleksordningen 40–80 incidenter per år, där en mindre andel av dessa incidenter av MSB bedömts kunna klassas som angrepp.

Av vad utredningen inhämtat från MSB tyder rapporteringen under april och maj 2016 på att antalet rapporterade incidenter under 2016 kommer att öka i förhållande till tidigare år, men att ökningen inte kommer vara dramatisk. Av de rapporterade incidenterna är en mindre andel sådana att de av rapporterande myndighet har klassats som ett angrepp, där det kan antas att incidenten har sin grund i en brottslig gärning.

MSB har i dessa fall i enlighet med förordningens bestämmelse uppmanat den rapporterande myndigheten att anmäla incidenten

till polisen. MSB har inte lämnat uppgifter om dessa incidenter till Polismyndigheten och heller inte närmare följt upp om rapporterande myndigheter fullföljt uppmaningen att polisanmäla.

Såvitt utredningen har kunnat utröna har ingen av de incidenter som rapporterats till MSB under april och maj månad 2016 anmälts till Polismyndigheten av den rapporterande myndigheten.

4.3.4 Incidentrapportering enligt säkerhetskyddsförordningen och lagen om elektronisk kommunikation

Jämte bestämmelserna i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap finns ytterligare bestämmelser om rapporteringsskyldighet för it-incidenter i vissa fall.

Incidentrapportering enligt säkerhetsskyddsförordningen (1996:633)

Säkerhetskyddsförordningen (1996:633) gäller för myndigheter, kommuner och landsting samt för vissa bolag, föreningar, stiftelser och enskilda enligt bestämmelser i säkerhetsskyddslagen (1996:627).

En myndighet, och andra som omfattas av förordningens krav, ska skyndsamt till den myndighet som utövar tillsyn över säkerhetsskyddet anmäla om det inträffat en it-incident i myndighetens informationssystem och

1. incidenten allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa,
2. incidenten allvarligt kan påverka säkerheten i ett informationssystem som särskilt behöver skyddas mot terrorism, eller
3. incidenten upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt.

Försvarsmakten är tillsynsmyndighet när det gäller Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet. Säkerhetspolisen är tillsynsmyndighet när det gäller övriga myndigheter utom Justitiekanslern. Om incidenten ska rapporteras till Försvarsmakten, ska den rapport-

erande myndigheten också skyndsamt informera Säkerhetspolisen. (10 a § och 39 § säkerhetsskyddsförordningen [1996:633])

Rapportering enligt säkerhetsskyddsförordningen ersätter sådan rapportering som annars enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska göras till MSB.

Incidentrapportering enligt lagen (2003:389) om elektronisk kommunikation

Den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst är skyldig att utan onödigt dröjsmål rapportera störningar eller avbrott av betydande omfattning till PTS (5 kap. 6 c § lagen [2003:389] om elektronisk kommunikation, LEK). Av Post- och telestyrelsens föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2) framgår på vilket sätt den skyldigheten ska fullgöras och om undantag från skyldigheten.

Den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster ska utan onödigt dröjsmål underrätta PTS om integritetsincidenter. Med integritetsincident avses en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster. Om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål. (6 kap. 1 och 4 a §§ LEK).

4.4 Samhällets insatser mot it-relaterad brottslighet

En viktig del av samhällets insatser på informationssäkerhetsområdet är kriminaliseringen av vissa handlingar och de brottsbekämpande myndigheternas verksamhet med att förebygga, ingripa mot och utreda sådan brottslighet. Att it-relaterade brott utreds ger kunskaper om bl.a. tillvägagångssätt och aktörer, vilket är av

stort värde vid utformningen av olika skyddsåtgärder. En effektiv lagföring av it-relaterad brottslighet är viktig för att minska benägenheten att begå sådana brott.

4.4.1 Brottsbalken

Incidenter som omfattas av rapporteringsskyldigheten enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap kan innefatta brottsliga handlingar.

Ett brott med uttrycklig koppling till it och it-incidenter är dataintrång enligt 4 kap. 9 c § brottsbalken. Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Även försök eller förberedelse till dataintrång och grovt dataintrång är straffbart (4 kap. 10 § brottsbalken).

Allvarliga angrepp som riktas mot egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning, förvaltning eller upprättande av allmän ordning och säkerhet kan vara att bedöma som sabotage eller grovt sabotage enligt 13 kap. 4 och 5 §§ brottsbalken.

4.4.2 Polismyndigheten och dess nationella it-brottscentrum

Till Polismyndighetens uppgifter hör bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten. Polismyndigheten ska utreda och beivra brott som hör under allmänt åtal.

Polismyndigheten organiseras i sju polisregioner, sju nationella avdelningar och ett kansli. Myndigheten leds av en rikspolischef.

Polisregionerna har helhetsansvar för polisverksamheten inom ett angivet geografiskt område. Ansvaret omfattar bland annat utredningsverksamhet, brottsförebyggande verksamhet och service. Arbetet i regionen leds av en regionpolischef.

De nationella avdelningarna utgörs av nationella operativa avdelningen (NOA), nationellt forensiskt centrum (NFC), it-avdelningen, rättsavdelningen, ekonomiavdelningen, HR-avdelningen och kommunikationsavdelningen.

Vid Polismyndigheten finns även internrevisionen samt avdelningen för särskilda utredningar, som utreder anmälningar mot anställda inom Polismyndigheten.

Den operativa verksamheten leds av NOA, som stödjer polisregionerna i olika typer av verksamheter. NOA har mandat att besluta om insatser och resursförstärkningar i hela landet. Vidare ska NOA vara nationell kontaktpunkt mot Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt, och ansvara för att hantera känslig information om till exempel terrorism och signalspaning. NOA ska även ansvara för samordning, beredning och uppföljning av den myndighetsgemensamma särskilda satsningen mot grov organiserad brottslighet.

Den 1 oktober 2015 inrättade Polismyndigheten ett nationellt it-brottscentrum vid NOA. Arbetet med inrättandet ska vara fullt genomfört senast den 31 december 2017.

Centret utgör en nationell expertresurs och skapar förutsättningar för en ökad enhetlighet för utredning och uppklarning av it-relaterade brott. It-brottscentrum ska utgöra Polismyndighetens

- nationella deskfunktion för it-relaterad brottslighet,
- expertfunktion för handläggning av komplexa it-brottsärenden och exempelvis barnpornografiärenden och vuxnas kontakt med barn i sexuellt syfte
- samverkanspartner med Säkerhetspolisen när det gäller hot och utredningar rörande kritisk infrastruktur
- nationella kontaktpunkt för andra myndigheter rörande frågor om kritisk infrastruktur och komplex it-brottslighet, t.ex. Myndigheten för samhällsskydd och beredskap (MSB) och försvaret samt för vissa kommunikationstjänstoperatörer (CSP)

- internationell kontaktpunkt för utländska rättsvårdande myndigheter och andra aktörer, t.ex. på sociala medier,

och;

- hantera hot mot it-relaterad kritisk infrastruktur
- samverka med Nationellt forensiskt centrum och Nationellt bedrägericenter
- ansvara för kontakterna med och hanteringen och samordningen av underrättelser inom European Cyber Crime Center (EC3)
- utgöra dess svenska motsvarighet – Swedish Cyber Crime Center (SC3)
- utöva processansvar för myndighetens arbete med komplex it-brottslighet
- uppnå enhetlighet för svensk polis inom ramen för processansvaret genom att sätta förmåga på nationell, regional, område och lokal nivå. På regional, eller på polisområdesnivå ska det finnas förmåga att utreda it-brott, barnpornografibrott, nivå 2 och 3 inhämtning samt hantera annan it-relaterad brottslighet. På lokal nivå ska det finnas förmåga med it-kompetens för anmälningsupptagning av it-relaterad brottslighet samt för initiala åtgärder i beslag av it-utrustning samt för s.k. nivå 2 inhämtning på internet.

4.4.3 Säkerhetspolisen

Säkerhetspolisen är Sveriges civila säkerhetstjänst med uppgift att bedriva personskyddsverksamhet, förebygga och avslöja brott mot rikets säkerhet samt bedriva terrorismbekämpning. Säkerhetspolisen är också utredande polis vid brott mot rikets säkerhet och terroristbrott.

Säkerhetspolisen arbetar bl.a. med att förebygga brottsliga handlingar i form av spionage som sker genom s.k. elektroniska angrepp. Arbetet består i första hand av säkerhetsskyddsåtgärder och utredning av särskilt skyddsvärda verksamheter. Säkerhetspolisen arbetar också med att förebygga allvarliga elektroniska

angrepp riktade mot samhällsviktiga it-system samt med att analysera och utreda allvarliga elektroniska angrepp mot samhällsviktiga verksamheter.

Enheterna informationssäkerhet samt utredning, båda vid avdelningen för åtgärder, ansvarar för bl.a. bevissäkring i it-miljö, tekniska säkerhetsgranskningar av it-system och undersökningar av skadlig kod respektive för att hantera förundersökningar inom myndighetens ansvarsområde. Den operativa chefen, som är direkt underställd säkerhetspolischefen, har ett övergripande ansvar för den operativa verksamheten. För att fullgöra det ansvaret finns en biträdande operativ chef och en operativ ledningsstab.

Säkerhetspolisen har ett omfattande samarbete såväl nationellt som internationellt. En stor del handlar om informations- och erfarenhetsutbyte. Det handlar också om att bistå och själva få hjälp av andra i olika utredningar eller insatser.

Nationellt samarbetar Säkerhetspolisen främst med underrättelsemyndigheter och brottsbekämpande organ som Militära underrättelse- och säkerhetstjänsten, Försvarets radioanstalt, Polismyndigheten och Ekobrottsmyndigheten. En stor del av samarbetet handlar om informations- och erfarenhetsutbyte men är också operativt, till exempel stöd till Polismyndigheten i brottsutredningar i form av expertkunskaper, hotbilder, spaning och analys. Säkerhetspolisen samverkar också med dem som omfattas av säkerhetsskyddslagstiftningen, dvs. myndigheter, kommuner och landsting samt vissa företag.

Säkerhetspolisen ingår tillsammans med Militära underrättelse- och säkerhetstjänsten och Försvarets radioanstalt i samverkansgruppen Nationell samverkan till skydd mot allvarliga it-hot (NSIT). NSIT analyserar och bedömer hot och sårbarheter när det gäller allvarliga eller kvalificerade it-angrepp mot de mest skyddsvärda nationella intressena. Syftet är att utveckla samverkan för att försvåra för en kvalificerad angripare att komma åt eller skada svenska skyddsvärda civila och militära resurser.

4.4.4 Åklagarmyndigheten

Det övergripande målet för kriminalpolitiken är att minska brottsligheten och att öka människors trygghet. Åklagarväsendet ska bidra genom att de som begår brott ställs till ansvar och att detta sker på ett effektivt och rättssäkert sätt.

Åklagarmyndigheten omfattar samtliga åklagare i Sverige med undantag för de som är anställda på Ekobrottsmyndigheten. Riksåklagaren är landets högsta åklagare och enda allmänna åklagare i Högsta domstolen. Riksåklagaren är också chef för Åklagarmyndigheten.

Den operativa åklagarverksamheten utövas i sju geografiska åklagarområden och en nationell åklagaravdelning. Åklagarområdena består av landets 32 allmänna kammare, som har ett geografiskt arbetsfält ungefär motsvarande ett län. De allmänna åklagarkammarna handlägger i stort sett samtliga brott inom sitt geografiska område.

Myndigheten har också tre internationella åklagarkammare. Här finns specialistkompetens för att bekämpa den organiserade, gränsöverskridande brottsligheten och för det internationella åklagarsamarbetet. Internationella åklagarkamrarna i Malmö och Göteborg ingår i Åklagarområde Syd respektive Väst.

Nationella åklagaravdelningen består av de riksenheter som har ett nationellt ansvar. De handlägger samtliga brott, oavsett geografisk hemvist, inom sina respektive ansvarsområden. De kammare som ingår i Nationella avdelningen är Riksenheten för miljö- och arbetsmiljömål, Riksenheten mot korruption och Riksenheten för säkerhetsmål. Dessutom ingår Internationella åklagarkammaren Stockholm.

Särskilda åklagarkammaren är en nationell operativ enhet inom Åklagarmyndigheten. Kammaren är direkt underställd riksåklagaren och handlägger främst misstankar om brott av poliser, åklagare, domare, riksdagsmän och vissa andra befattningshavare.

Åklagarmyndighetens tre utvecklingscentrum har i uppgift att bedriva metod- och rättsutveckling inom olika brottsområden. Rättslig uppföljning och tillsyn utövas också här. Ett exempel är att alla överprövningar av åklagarbeslut handläggs av utvecklingscentrumen. Utvecklingscentrumen svarar för den samlade kunskapen inom sina ansvarsområden.

På huvudkontoret finns centrala funktioner för bland annat information, ekonomi, personal och it. Dessutom finns en rättsavdelning för rättslig information, verksamheten i Högsta domstolen och centrala internationella frågor samt en tillsynsavdelning för rättslig tillsyn.

Vid Åklagarmyndigheten finns ett insynsråd. Ledamöterna utses av regeringen. Insynsrådets uppgift är att utöva insyn och ge myndighetschefen råd. Rådet har inga beslutsbefogenheter. Ärenden om åklagaruppgiften eller tillsynsfrågor i enskilda fall behandlas inte i insynsrådet.

4.5 Brottsutredning och lagföring

Polismans rapporteringsskyldighet

När en polisman får kännedom om ett brott som hör under allmänt åtal, ska han lämna rapport om det till sin förman så snart det kan ske. En polisman får lämna rapporteftergift om brottet med hänsyn till omständigheterna i det särskilda fallet är obetydligt och det är uppenbart att brottet inte skulle föranleda annan påföljd än böter. (9 § polislagen [1984:387])

Förundersökning

Till Polismyndighetens uppgifter hör bland annat att utreda och beivra brott som hör under allmänt åtal (2 § 3 polislagen). Den del av verksamheten som utgör förundersökning är reglerad i 23 § rättegångsbalken.

Polisen bedriver också s.k. underrättelseverksamhet. Med underrättelseverksamhet avses polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken (se definitionen i 3 § i den gamla polisdatalagen).

Förundersökning ska inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Det föreligger alltså förundersökningsplikt. Undantag från förundersökningsplikten gäller om det är

uppenbart att brottet inte går att utreda eller om det finns förutsättningar för så kallad förundersökningsbegränsning, eller saken rör brott som kan antas leda bara till böter eller brott som begås under rättegång. Om det krävs angivelse för att brottet ska höra under allmänt åtal, får förundersökning trots det inledas utan angivelse, om det innebär fara att avvakta en angivelse. I så fall ska målsäganden underrättas snarast. Om målsäganden då inte anger brottet till åtal, ska förundersökningen läggas ned. (23 kap. 1 § rättegångsbalken med hänvisningar)

Under förundersökningen ska utredas vem som skäligen kan misstänkas för brottet och om tillräckliga skäl finns för åtal. Förundersökningen ska bedrivas så att bevisningen kan läggas fram i ett sammanhang vid huvudförhandling i domstol. (23 kap. 2 § rättegångsbalken)

Beslut att inleda förundersökning fattas av Polismyndigheten, Säkerhetspolisen eller åklagaren. Har förundersökningen inletts av Polismyndigheten eller Säkerhetspolisen och är saken inte av enkel beskaffenhet, ska ledningen av förundersökningen om brottet övertas av åklagaren, så snart någon skäligen kan misstänkas för brottet. (23 kap. 3 § rättegångsbalken) Oavsett vem som leder förundersökningen utförs som regel själva utredningsarbetet av polismän eller andra anställda inom polisväsendet.

Under en förundersökning används straffprocessuella tvångsmedel i brottsutredande syfte eller för att en rättegång i brottmål ska kunna genomföras. Exempel på sådana tvångsmedel är beslag, avspärrning av brottsplats m.m., hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning (27 kap. rättegångsbalken). En grundläggande förutsättning för att använda straffprocessuella tvångsmedel är normalt att en förundersökning har inletts. Användningen ska då ytterst ha till syfte att utreda eller lagföra ett visst brott. Undantag finns dock. I vissa fall får hemliga tvångsmedel användas utan att det pågår förundersökning, då i syfte att förhindra särskilt allvarlig brottslighet.

I fråga om tvångsmedel gäller samma befogenheter och skyldigheter på det digitala området som i övriga fall. Med hänvisning bl.a. till att dessa verktyg i sin utformning inte är skapade för eller anpassade för den digitala miljön, föreslog NISU 2014 i sitt betänkande *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder*

för säker information i staten (SOU 2015:23), en översyn av bl.a. bestämmelserna i 27 kap. rättegångsbalken. Regeringen har i maj 2016 beslutat att en särskild utredare ska undersöka om bestämmelser om hemlig dataavläsning bör införas i svensk rätt för att säkerställa att de brottsbekämpande myndigheterna kan upprätthålla sin förmåga att bekämpa brott.

När förundersökningen avslutas, ska beslut meddelas, huruvida åtal ska väckas (23 kap. 20 § rättegångsbalken).

Lagföring

Leder förundersökning om brott där allmänt åtal får ske fram till att åklagaren på objektiva grunder kan förutse en fällande dom är åklagaren som huvudregel skyldig att föra talan mot brottet vid domstol (20 kap. 6 § rättegångsbalken).

Åklagare får besluta att underlåta åtal för brott (åtalsunderlåtelse) under förutsättning att något väsentligt allmänt eller enskilt intresse ej åsidosätts om det kan antas att brottet inte skulle föranleda annan påföljd än böter, om det kan antas att påföljden skulle bli villkorlig dom och det finns särskilda skäl för åtalsunderlåtelse, om den misstänkte begått annat brott och det utöver påföljden för detta brott inte krävs påföljd med anledning av det föreliggande brottet, eller om psykiatrisk vård eller insatser enligt lagen (1993:387) om stöd och service till vissa funktionshindrade kommer till stånd. Åtal får underlåtas även i andra fall, om det av särskilda skäl är uppenbart att det inte krävs någon påföljd för att avhålla den misstänkte från vidare brottslighet och att det med hänsyn till omständigheterna inte heller krävs av andra skäl att åtal väcks. (20 kap. 7 § rättegångsbalken)

Åtal väcks genom att åklagaren hos rätten skriftligen ansöker om stämning mot den som ska tilltalas. Stämningsansökan ska avvisas, om rätten finner uppenbart, att den som väcker åtalet inte har rätt att föra talan angående brottet eller att målet på grund av annat rättegångshinder inte kan tas upp till prövning. Avvisas inte ansökan, ska rätten utfärda stämning på den tilltalade att svara på åtalet. Som huvudregel gäller att ett mål ska avgöras efter huvudförhandling. (45 kap. 1, 8–9 och 10 a §§ rättegångsbalken)

5 Ordningen i några andra länder

I utredarens uppdrag ligger att undersöka vilken ordning för informationsdelning mellan motsvarande myndigheter som förekommer i några andra, med Sverige jämförbara, länder samt om det i dessa länder finns andra sätt för polisen att få information om it-brottslighet.

Utredningen har med hjälp av Myndigheten för samhällsskydd och beredskap (MSB) inhämtat information om it-incidentrapportering i Tyskland, Nederländerna och Norge. Utredningen har särskilt intresserat sig för frågan om hur CERT-funktionerna i dessa länder samarbetar med polisiära myndigheter. Utredningen har inte funnit något exempel där CERT-funktioner frivilligt eller till följd av lagstiftning regelmässigt informerar polisiära myndigheter om antagonistiska it-incidenter överlag. Utredningen noterar dock att det av EU:s strategi för cybersäkerhet framgår bl.a. att nationella myndigheter som ansvarar för nät- och informationssäkerhet bör rapportera incidenter som misstänks vara av allvarlig brottslig karaktär till brottsbekämpande myndigheter.

5.1 Tyskland

I juli 2015 trädde en ny it-säkerhetslag i kraft i Tyskland. Skyldigheten att rapportera it-incidenter beror på vilken typ av verksamhet som drabbats och hur allvarlig incidenten är.

Operatörer av kritisk infrastruktur inom sektorerna energi, informationsteknik och telekommunikation, transport, hälsa, vatten, näring och finans och försäkring måste uppfylla en minimistandard för it-säkerhet samt rapportera allvarliga it-incidenter till den federala byrån för informationssäkerhet (Bundesamt für Sicherheit in der Informationstechnik [BSI]). För att rapporteringsskyldigheten ska

inträda krävs att incidenten är allvarlig, t.ex. att en verksamhet är utsatt för kraftiga störningar. Att hanteringen av en incident kräver stora resurser kan vara en indikator på att incidenten är allvarlig. Även incidenter som skulle kunna få allvarliga konsekvenser ska rapporteras. Incidenter som inte under några omständigheter kan påverka kritisk verksamhet behöver inte rapporteras.

Om den rapporterande aktören redan har hanterat incidenten kommer incidenten endast att ingå i BSI:s lägesbild. I andra fall påbörjar BSI omedelbart en analys. Analysen kan i vissa fall leda till att det utfärdas en varning till en berörd målgrupp, t.ex. statliga myndigheter, tillhandahållare av kritisk infrastruktur, den privata sektorn, osv.

BSI har bilaterala relationer till andra säkerhetsmyndigheter. I vissa fall ska BSI vidarebefordra uppgifter till andra myndigheter, t.ex. departement och tillsynsmyndigheter, i andra fall lämnar dessa uppgifter till BSI.

Om det finns starka bevis för att en incident har koppling till terrorism eller för att incidenten innebär en fara för rikets säkerhet eller har koppling till spionage, måste BSI vidarebefordra uppgiften till den federala kriminalpolisen, Bundeskriminalamt (BKA) respektive underrättelsetjänsten (Bundesamt für Verfassungsschutz [BfV]). Om namnet på den rapporterande aktören måste lämnas ut ska denne underrättas om det. Obegränsad informationsdelning med tredje myndighet kräver godkännande från den rapporterande aktören.

När det gäller incidenter som har sin grund i annan brottslighet än sådan som har koppling till terrorism, rikets säkerhet eller spionage, kan BSI vidarebefordra uppgifter till andra myndigheter när den rapporterande aktören har gjort en polisanmälan och indikerat i rapporten att uppgifterna kan vidarebefordras till BKA. BSI kontaktar alltså inte de brottsbekämpande myndigheterna beträffande sådan brottslighet, utan den drabbade måste göra en formell anmälan. BSI rekommenderar starkt den drabbade att göra en polisanmälan. På BSI:s hemsida finns också en länk till en broschyr från BKA.

Utöver skyldigheten för ovan nämnda operatörer av kritisk infrastruktur att rapportera vissa it-incidenter är telekomföretag skyldiga att rapportera allvarliga it-incidenter och att varna kunder vars datorer är del av är ett botnet (datornätverk av datorer infekterade

av datavirus eller trojanska hästar). Övriga aktörer har möjlighet att rapportera it-incidenter frivilligt.

5.2 Nederländerna

I Nederländerna är det i dagsläget frivilligt att rapportera it-incidenter. Det pågår dock lagstiftningsarbete när det gäller obligatorisk rapportering. Enligt lagförslaget kommer operatörer av kritisk infrastruktur att bli skyldiga att rapportera it-incidenter. Rapporteringsskyldigheten kommer att omfatta aktörer inom sektorerna elektricitet, gas, dricksvatten, telekom, finans, regeringen, transport och kärnkraft. Rapporteringen hanteras av National Cyber Security Centre (NCSC), som upprätthåller den nederländska CERT-funktionen. Funktionen är en del av National Coordinator for Security and Counterterrorism (NCTV), som i sin tur är en del av Ministry of Security and Justice.

Skyldigheten att rapportera kommer enligt förslaget att uppstå när incidenten innebär eller kan innebära att tillgången till en produkt eller tjänst riskerar eller kommer att bli utsatt för kraftiga störningar. Enligt förslaget ska rapporteringsskyldigheten vara begränsad till sådana incidenter som innebär ett allvarligt hot mot det nederländska samhället. Det förväntas därför inte att väldigt många rapporter kommer att ske. Rapporteringsskyldigheten är kopplad till ett faktiskt säkerhetsintrång (security breach) eller en faktisk integritetsförlust i ett elektroniskt informationssystem (loss of integrity of an electronic information system). Incidenter som beror på ett internt misstag av en anställd kommer som huvudregel inte att vara rapporteringspliktiga. Rapporteringsplikt kan dock komma att uppstå om misstaget innebär att någon person utanför den drabbade aktören får tillgång till systemet.

Förslaget innebär inte någon skyldighet att rapportera avbrott som beror på DDoS-attacker, eftersom sådana attacker inte innebär något intrång. En DDoS-attack innebär att tillgången till systemen hindras utan att själva systemet påverkas i sig. Det har ansetts viktigt att begränsa rapporteringen till de fall där NCSC:s insatser innebär tillräckligt mervärde. DDos-attacker kommer dock att kunna rapporteras frivilligt.

NCSC är del av ett offentlig-privat samarbete. Information delas med t.ex. polisen och med operatörer av kritisk infrastruktur. Samverkansgruppen fungerar som länk och kontaktpunkt mellan NCSC och andra samverkande aktörer. Delning av konfidentiell, identifierande, information är dock begränsad till en liten krets. Polisen ingår inte i den kretsen. Utöver samverkansgruppen samverkar NCSC med polisen även i tillfälliga operativa samarbeten.

Enligt lagförslaget ska NCSC vidarebefordra information från rapporterna till aktörer som har i uppgift att informera allmänheten eller andra relevanta aktörer, till CERT:ar och till tillhandahållare av internetkommunikation. Det kommer inte heller fortsättningsvis att finns någon skyldighet för NCSC att informera polisen om en incident. Det ansvaret kommer den rapporterande aktören att ha, även om NSCS i de flesta fall uppmanar denne att göra en polisanmälan. Syftet med detta är att bibehålla förtroende från de rapporterande aktörerna gentemot NCSC och att undvika möjliga, för rapporeringsbenägenheten, avskräckande faktorer.

5.3 Norge

I Norge är verksamheter som lyder under ”lov om forebyggende sikkerhetstjeneste” (sikkerhetsloven) skyldiga att till Nasjonal sikkerhetsmyndighet (NSM) rapportera händelser som hotar säkerheten, t.ex. spionage, sabotage och terrorhandlingar samt förberedelse och försök till dessa brott, liksom händelser kopplade till hemlig information. Vid NSM finns den norska CERT-funktionen, NSM NorCERT. Rapporteringsplikten omfattar också IKT-relaterade händelser. IKT-relaterade händelser ska rapporteras även till andra berörda verksamheter. Det finns också flera sektorsvisa bestämmelser om rapporteringsplikt till tillsynsorgan inom olika sektorer.

Rapportering av it-incidenter som inte omfattar hemliga uppgifter är frivillig. Frivillig rapportering sker till NSM NorCERT.

NSM NorCERT detekterar också själv händelser genom Varslingssystem for digital infrastruktur (VDI). VDI är ett sensorsystem som är utplacerat hos vissa offentliga och privata tillhandahållare av kritisk infrastruktur. VDI gör det möjligt att tidigt upptäcka och varna om allvarliga it-angrepp. Systemet är baserat på

frivillighet och parteras rättigheter och skyldigheter i samarbetet regleras genom avtal.

Vid allvarliga händelser ska NSM Nor-CERT ge råd och stöd i incidenthanteringen. NSM NorCERT ska dela information med annan verksamhet när det är nödvändigt för att förebygga och hantera allvarliga it-incidenter som drabbat samhällskritisk infrastruktur och samhällskritiska funktioner.

Det krävs som huvudregel samtycke från den drabbade aktören för att delning av information om konkreta inrapporterade incidenter eller händelser som detekterats med hjälp av VDI-systemet ska kunna ske. Verksamheter som är knutna till VDI-systemet har i avtalen accepterat att information kan lämnas vidare till säkerhetstjänsten och underrättelsetjänsten inom ramen för ändamålet, dvs. att förebygga och hantera allvarliga it-incidenter som drabbat samhällskritisk infrastruktur och samhällskritiska funktioner. De tre aktörerna har utarbetat egna riktlinjer som reglerar samarbete dem emellan och har etablerat en egen grupp, Cyberkoordineringsgruppen, som koordinerar samarbetet mellan dem.

Delning av inrapporterad information med andra aktörer, t.ex. polisen, förutsätter normalt samtycke från den rapporterande aktören. Tillåtelse till informationsdelning kan lämnas genom användning av Trafikklysprotokollen (TLP), eller genom samtycke inhämtat av NSM NorCERT i det enskilda fallet. Om informationsdelning kan ske i anonymiserad form eller inte kan knytas till en viss verksamhet kan informationsdelning dock ske utan samtycke.

6 Utredningens principiella utgångspunkter

Den grundläggande utgångspunkten för utredningens uppdrag är att det är angeläget att brottsliga gärningar som utgör ett hot mot informationssäkerheten utreds och att de individer som ansvarar för sådana handlingar lagförs.

I kontakter med Polismyndigheten och Åklagarmyndigheten har företrädare för myndigheterna framfört att de bedömer att denna typ av brottslighet i begränsad utsträckning anmäls till polis och åklagare. Den låga anmälningsbenägenheten kan ha flera orsaker. Brott som dataintrång och andra brott som utgör ett hot mot informationssäkerheten är typiskt sett svårutredda, och möjligheterna att framgångsrikt föra brottsutredningen till åtal och fällande dom är ofta små. Den som drabbas av ett brott kan ha begränsad kunskap om hur de brottsutredande myndigheterna arbetar, och vilka möjligheter de har att skydda känsliga uppgifter som behandlas inom ramen för brottsutredningen. Det går heller inte att bortse från risken att den som drabbats av ett it-angrepp kan vilja undvika att anmäla incidenten för att inte riskera att eventuella säkerhetsbrister och sårbarheter i verksamheten exponeras.

Framgång i den brottsutredande verksamheten är i hög utsträckning beroende av att polis och åklagare får information om att brott har begåtts och att den som drabbats av brott medverkar i utredningen. Polismyndigheten har genom bildandet av det nationella it-brottscentret skapat förutsättningar för att utveckla sin verksamhet och för ökad enhetlighet i verksamheten. Genom att verksamheten hålls samman i en och samma organisatoriska enhet utgör it-brottscentret både en viktig nationell kontaktpunkt för andra myndigheter rörande frågor om exempelvis kritisk infrastruktur och komplex it-brottslighet, men också en internationell kontaktpunkt

för utländska rättsvårdande myndigheter och andra aktörer. Utredningen bedömer att den nya organisationen härmed också skapar förutsättningar för att i förhållande till statliga myndigheter och andra viktiga aktörer arbeta förtroendeskapande, och därmed bidra till att benägenheten att anmäla it-incidenter till polisen i denna krets ökar.

Utredningen har inte funnit anledning att inom ramen för uppdraget lämna förslag till hur Polismyndigheten genom egna åtgärder kan utveckla verksamheten i syfte att öka anmälningsbenägenheten. I fokus för utredningens arbete står i stället frågan i vilken mån den nya ordningen med obligatorisk incidentrapportering till Myndigheten för samhällsskydd och beredskap (MSB) kan bidra till att öka Polismyndighetens tillgång till information om it-brottslighet.

Polismyndighetens uppgift är bl.a. att utreda brott som hör under allmänt åtal och att förebygga och ingripa mot brott. Verksamheten är beroende av att underrättelser och uppgifter om misstänkta brott lämnas till polisen. Ofta lämnas sådana uppgifter av den som drabbats av brottet, men uppgifterna kan också komma till polisen från exempelvis den som bevittnat ett brott eller från den som av annan anledning fått anledning att misstänka att ett brott har begåtts.

Myndigheter och andra organ kan i många fall komma att hantera uppgifter som ger dem anledning att misstänka att ett brott har begåtts. Endast i en begränsad omfattning har lagstiftaren valt att i lag eller annan författning slå fast en skyldighet för myndigheter eller andra att lämna uppgifter om misstänkta eller pågående brott till de brottsutredande myndigheterna. Nedan beskrivs några exempel på sådana författningar.

På informationssäkerhetsområdet har i 10 § säkerhetsskyddsförordningen (1996:633) stadgats en skyldighet för myndigheter med flera att om en hemlig uppgift kan ha röjts skyndsamt anmäla det till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa. Skälet till bestämmelsen är dels att kunna utreda det eventuella straffrättsliga ansvaret för röjande, dels att kunna vidta åtgärder för att minska skadan i det enskilda fallet och om möjligt minska risken för framtida röjande.

Den 15 augusti 2016 träder en ny lag om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet i kraft. Lagen syftar

bl.a. till att underlätta informationsutbyte mellan vissa myndigheter i kampen mot organiserad brottslighet.

När det gäller penningtvätt och finansiering av terrorism ska en verksamhetsutövare granska transaktioner för att kunna upptäcka sådana som den misstänker eller har skälig grund att misstänka utgör ett led i penningtvätt eller finansiering av terrorism. Om misstanke efter närmare analys kvarstår, ska uppgifter om alla omständigheter som kan tyda på penningtvätt eller finansiering av terrorism utan dröjsmål lämnas till Polismyndigheten. När sådana uppgifter har lämnats, ska även vissa andra fysiska eller juridiska personer lämna de uppgifter för utredningen om penningtvätt eller finansiering av terrorism som myndigheten begär. På begäran av Polismyndigheten ska vidare verksamhetsutövaren eller den som yrkesmässigt driver lotteri- och spelverksamhet utan dröjsmål lämna alla uppgifter som behövs för en utredning om penningtvätt eller finansiering av terrorism. (3 kap. 1 § lagen [2009:62] om penningtvätt) Uppgiftsskyldigheten infördes i svensk rätt första gången i den numera upphävda lagen (1993:768) om åtgärder mot penningtvätt, till uppfyllande av Sveriges förpliktelser enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES).

Bestämmelser om revisors anmälningsskyldighet finns i aktiebolagslagen (2005:551). Om en revisor finner att t.ex. en styrelseledamot eller den verkställande direktören gjort sig skyldig till vissa brott ska revisorn vidta vissa åtgärder. Revisorn ska bl.a. under vissa förutsättningar anmäla misstänkt brottslighet till åklagare. (9 kap. 42–44 §§ aktiebolagslagen)

Även vissa tillsynsmyndigheter är skyldiga att anmäla eller verka för att brott beivras i vissa fall. Offentlig kontroll av efterlevnaden av djurskyddslagen (1988:534) m.m. utövas av bl.a. länsstyrelserna. I sin egenskap av kontrollmyndighet ska länsstyrelserna verka för att överträdelser av djurskyddslagen beivras (24 och 24 b §§ djurskyddslagen). Detta innebär att misstänkta överträdelser av lagen ska anmälas till åklagare eller polis (se JO 2014/15 s. 525). I samband med att bestämmelsen infördes hänvisades till den likalydande bestämmelsen i livsmedelslagen (2006:804). Enligt 13 § den lagen ska den myndighet som utövar offentlig kontroll verka för att överträdelser av lagen, av de föreskrifter eller beslut som har meddelats med stöd av lagen eller av de EG-bestämmelser som kompletteras av lagen, beivras. I förarbetena uttalades att det inte

får vara en undantagsföreteelse att lagföring sker när det gäller överträdelse av livsmedelslagens bestämmelser, utan att det istället ska vara regel. Bestämmelsen i livsmedelslagen infördes i sin tur efter mönster i miljöskyddslagen.

Enligt miljöbalken (1998:808) gäller att tillsynsmyndigheten, som ett led i tillsynen, ska anmäla överträdelser av bestämmelser i balken eller i föreskrifter som har meddelats med stöd av balken till polis- eller åklagarmyndigheten, om det finns misstanke om brott. Tillsynsmyndigheten ska inte själv göra någon bedömning av om överträdelsen kan föranleda fällande dom eller om det är ett ringa brott utan anmäla de faktiska förhållandena så snart en straffbar överträdelse kan konstateras.

Finansinspektionen övervakar att lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument följs. När det finns anledning att anta att brott enligt lagen har begåtts, ska Finansinspektionen enligt 19 § anmäla detta till åklagare.

Värdepappersinstitut och börser enligt lagen (2007:528) om värdepappersmarknaden och sådana utländska företag som har tillstånd enligt samma lag att driva en reglerad marknad från filial i Sverige samt kreditinstitut enligt lagen (2004:297) om bank- och finansieringsrörelse ska snarast rapportera till Finansinspektionen, om det kan antas att en transaktion utgör eller har samband med insiderbrott eller otillbörlig marknadspåverkan. Inspektionen ska snarast överlämna uppgifterna till åklagare. (10 § lagen [2005:377] om straff för marknadsmissbruk vid handel med finansiella instrument)

I 23 kap. 6 § brottsbalken finns en skyldighet för envar att anmäla eller avslöja vissa brott som håller på att ske. Som exempel kan anges att underlåtenhet att anmäla eller avslöja sabotage, grovt sabotage, spionerі, grovt spionerі och grov obehörig befattning med hemlig uppgift är straffbelagt. En förutsättning för att skyldigheten ska uppstå är att anmälan eller avslöjandet kan ske utan fara för den som skyldigheten åligger eller någon av dennes närmaste. En annan förutsättning är att gärningen i fråga fortskridit så långt att straff kan följa på den. Den åtgärd som i första hand bör komma i fråga är att anmäla brottet för polisen. Avslöjande på annat sätt, såsom genom meddelande till den som hotas av brottet, är emellertid tillräckligt för straffrihet.

Det finns även bestämmelser om skyldigheter i vissa fall att lämna uppgifter om brott till icke brottsbekämpande myndigheter. Vissa myndigheter och yrkesverksamma är skyldiga att genast anmäla till socialnämnden om de i sin verksamhet får kännedom om eller misstänker att ett barn far illa. De anmälningspliktiga aktörerna är myndigheter vars verksamhet berör barn och unga, andra myndigheter inom hälso- och sjukvården, annan rättspsykiatrisk undersökningsverksamhet, socialtjänsten, Kriminalvården, Polismyndigheten och Säkerhetspolisen, anställda hos dessa myndigheter samt de som är verksamma inom yrkesmässigt bedriven enskild verksamhet och fullgör uppgifter som berör barn och unga eller inom annan sådan verksamhet inom hälso- och sjukvården eller på socialtjänstens område. (14 kap. 1 § socialtjänstlagen [2001:453]).

Socialtjänstens möjlighet att lämna uppgifter om misstänkta brott vidare till de brottsutredande myndigheterna regleras av socialtjänstsekretessen i 26 kap. 1, 3, 4 och 6 §§ offentlighets- och sekretesslagen (2009:400), OSL. Denna sekretess hindrar inte att en uppgift lämnas till åklagarmyndighet eller Polismyndigheten, om uppgiften angår misstanke om brott som riktas mot någon som inte fyllt arton år och det är fråga om brott mot liv och hälsa (3 kap. brottsbalken), brott mot frihet och frid (4 kap. brottsbalken) eller sexualbrott (6 kap. brottsbalken) eller brott som avses i lagen med förbud mot könsstympning av kvinnor (10 kap. 21 § OSL).

Frånvaron av en skyldighet för myndighet eller annan att lämna uppgift till de brottsutredande myndigheterna utgör inget hinder att lämna uppgiften. För statliga myndigheter är utgångspunkten att myndigheter har en långtgående skyldighet att samarbeta och bistå varandra i den utsträckning som kan ske, en princip som bl.a. kommer till utryck i 6 § förvaltningslagen (1986:223). Principen omfattar också frågor om samarbete och informationsutbyte med brottsbekämpande myndigheter, ett förhållande som återspeglas i bestämmelsen i 6 § polislagen (1984:387) om att myndigheter ska ge polisen stöd i dess arbete. Det är i många fall en naturlig utgångspunkt att myndigheter och tjänstemän som i sin tjänsteutövning får anledning att misstänka att ett brott har begåtts får vidta åtgärder för att brottet ska kunna utredas.

I samband med tillkomsten av den bestämmelse som reglerar förutsättningarna för myndigheter att utan hinder av sekretess lämna information om misstänkta brott till brottsutredande myn-

digheter (om nuvarande bestämmelse i 10 kap. 24 § OSL se avsnitt 7.2.1 nedan) uttalas i förarbetena följande (prop. 1983/84:142 s. 19 och 21).

> För att ett rättssamhälle skall fungera på ett tillfredsställande sätt fordras att samhället ingriper mot brott. Uppgiften att bekämpa brottsligheten ligger i första hand på polisen och åklagarna.
>
> – – –
>
> Brottsbekämpningen bygger […] inte enbart på polisens övervakande och brottsspanande verksamhet. En solidarisk medverkan från allmänheten utgör en förutsättning för att brottsligheten skall kunna bekämpas effektivt. Även insatser från andra myndigheter är betydelsefulla. Andra myndigheter har i många fall en rätt och ibland t.o.m. en skyldighet att lämna ut uppgifter om brott till polis eller åklagare. Detta gäller inte sällan även om uppgifterna i övrigt är skyddade av sekretess.
>
> – – –
>
> Myndigheterna kan delta i kampen mot brottsligheten på många olika sätt. En betydelsefull form av medverkan består i att lämna uppgifter om brott till de direkt brottsbekämpande myndigheterna.

Samhällsutvecklingen har på senare år tydligt gått i riktning mot att myndigheter fördjupat och utvecklat sin samverkan med de brottsbekämpande myndigheterna. En av de mest strukturerade formerna är den nationella satsningen mot den grova organiserade brottsligheten där Polismyndigheten, Säkerhetspolisen, Åklagarmyndigheten, Ekobrottsmyndigheten, Skatteverket, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Tullverket, Försäkringskassan och Migrationsverket deltar. Ett annat exempel på myndighetssamverkan är det lokala brottsförebyggande arbetet som polisen och kommunerna bedriver genom s.k. samverkansöverenskommelser. Ett viktigt led i alla former av samverkan är möjligheten att kunna utbyta information.

MSB:s verksamhet förutsätter en bred samverkan med myndigheter och andra aktörer. På informationssäkerhetsområdet uttalas i 11 a och b §§ förordningen (2008:1002) med instruktion för MSB särskilt att myndigheten ansvarar för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten ska

1. agera skyndsamt vid it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och med-

verka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,

2. återrapportera till berörda aktörer i samband med att en it-incident har rapporterats,
3. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och
4. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

Den obligatoriska it-incidentrapporteringen har tillkommit mot bakgrund av behovet att öka samhällets förmåga att förebygga och hantera incidenter som hotar samhällsviktig verksamhet. När NISU 2014 lämnade sitt betänkande med förslag att MSB bör vara den myndighet som även i fortsättningen tar emot de it-incidentrapporter som lämnas från myndigheterna uttalade utredningen också att systemet bör utformas så att det säkerställer behovet hos de brottsbekämpande myndigheterna av att kunna informera sig om brottsliga angrepp (SOU 2015:23 s. 261).

Även i den europeiska cybersäkerhetsstrategi som EU-kommissionen presenterade 2013 anges att nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet bör rapportera incidenter som misstänks vara av allvarlig brottslig karaktär till brottsbekämpande myndigheter.

Utredningens utgångspunkt är mot denna bakgrund att det är en viktig del av samhällets informationssäkerhetsarbete att myndigheter med uppgifter på området så långt möjligt samverkar och delar information och uppgifter med varandra. Detta gäller även samverkan mellan brottsbekämpande och icke brottsbekämpande myndigheter med ansvar på informationssäkerhetsområdet såsom Polismyndigheten och MSB.

Ett informationssamarbete kan dock förhindras eller försvåras till följd av bestämmelser om sekretess, eller andra rättsregler. Utredningen presenterar i nästa kapitel sin analys av de rättsliga förutsättningarna för MSB att lämna uppgifter om it-incidenter som kan antas ha sin grund i en brottslig handling till Polismyndigheten.

7 Rättsliga hinder mot ett informationssamarbete mellan MSB och Polismyndigheten

Utredningen analyserar i detta kapitel frågan om det föreligger några rättsliga hinder mot ett informationssamarbete mellan Myndigheten för samhällsskydd och beredskap (MSB) och Polismyndigheten. Särskilt prövas frågan om några hinder föreligger på grund av sekretess.

7.1 Sekretess i MSB:s verksamhet

Många av de uppgifter som lämnas till MSB inom ramen för såväl frivillig som obligatorisk incidentrapportering omfattas av sekretess. Till varje sekretessgrund hör ett s.k. skaderekvisit. Är rekvisitet i det enskilda fallet uppfyllt innebär sekretessen ett förbud att röja uppgiften, oavsett om det sker genom utlämnande av en handling eller genom att uppgiften lämnas muntligt eller på något annat sätt. Sekretess gäller såväl mot enskilda som mot andra myndigheter. Sekretess kan även gälla mellan olika verksamhetsgrenar inom en myndighet.

7.1.1 18 kap. 8 § 3 och 4 OSL

I 18 kap. 8 § offentlighets- och sekretesslagen (2009:400), OSL, finns bestämmelser om sekretess för olika brottsförebyggande åtgärder som i huvudsak hänför sig till annan verksamhet än polisens. Vissa av åtgärderna syftar endast mera indirekt till att förebygga brott. De åtgärder som aktualiseras i samband med it-incidentrapporteringen återfinns i punkterna 3 och 4. Bestämmelserna är

tillämpliga både hos den myndighet som upprättar och skickar in en it-incidentrapport och hos MSB eller annan myndighet som tar emot rapporten.

Sekretess gäller enligt 18 kap. 8 § OSL 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 telekommunikation eller system för automatiserad behandling av information, (tredje punkten) eller behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling (fjärde punkten).

Som exempel på säkerhets- eller bevakningsåtgärder nämns i förarbetena 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. Både uppgifter som direkt lämnar upplysningar om säkerhets- eller bevakningsåtgärder avseende sådana system och uppgifter som kan bidra till att lämna upplysningar om sådana åtgärder kan hemlighållas om det kan antas att syftet med de vidtagna åtgärderna motverkas om uppgifterna röjs. Som exempel på uppgifter som kan bidra till att lämna upplysningar om säkerhets- eller bevakningsåtgärder avseende t.ex. ett operativsystem nämns i förarbetena uppgift om vilken typ och version av operativsystem som använts. Sådana uppgifter kan hemlighållas om t.ex. en viss version av ett operativsystem har visat sig ha svagheter som gör att det är lätt att olovligen ta sig in i systemet trots de vidtagna skyddsmekanismerna. En uppgift om vilket operativsystem som används skulle i ett sådant fall indirekt innebära en anvisning för den datatekniskt kunnige om hur man kringgår de vidtagna skyddsåtgärderna. Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör dock alltid kunna lämnas utan att det kan antas att vidtagna säkerhetsåtgärder motverkas.

Den för it-incidentrapporteringen allra mest relevanta sekretessbestämmelsen är bestämmelsen i tredje punkten, angående system för automatiserad behandling av information. Med system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka och distribuera information. Om en myndighets it-säkerhetssystem har slutat att fungera eller om vissa

svagheter i systemet har upptäckts och en it-incidentrapport lämnas till MSB kan uppgiften om vem som har lämnat rapporten utgöra en säkerhetsrisk, eftersom uppgiften innebär en upplysning om att den aktuella organisationens säkerhetssystem är sårbart. Även en sådan uppgift kan falla under bestämmelsen under förutsättning att skaderekvisitet är uppfyllt.

Bestämmelsen i tredje punkten tillkom mot bakgrund av att Post- och Telestyrelsen (PTS) tilldelades uppdraget att inrätta en rikscentral för it-incidentrapportering (Sitic). PTS skulle stödja samhället i arbetet med skydd mot it-incidenter genom att bl.a. inrätta ett system för informationsutbyte mellan samhällets organisationer och rikscentralen avseende it-incidenter. För att myndigheter och enskilda organ skulle vara villiga att lämna rapporter i en sådan omfattning och med ett sådant innehåll som behövdes för att PTS skulle kunna fullgöra sitt uppdrag, ansågs det viktigt att PTS hade möjlighet att hemlighålla sådana uppgifter i rapporterna som var känsliga från säkerhetssynpunkt. 2011 omorganiserades Sitic till MSB och bytte namn till CERT-SE .

Sekretessen under fjärde punkten, avseende uppgift om åtgärd som avser behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling, gäller i första hand uppgifter om behörighetskoder och behörighetsnycklar samt arrangemang och fördelning av dessa, däremot inte generellt program för hemliga upptagningar. Bestämmelsen gäller inte bara behörighet avseende upptagningar som utgör hemliga, allmänna handlingar i tryckfrihetsförordningens mening, utan gäller behörighet avseende alla typer av handlingar.

7.1.2 18 kap. 9 § OSL

Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod, om det kan antas att syftet med metoden motverkas om uppgiften röjs och metoden har till syfte att antingen underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, eller göra det möjligt att kontrollera om data i elektronisk form har förvanskats (18 kap. 9 § OSL). Sekretessen gäller oberoende av hos vilken myndighet uppgifterna finns. Inom ramen för it-incident-

rapporteringen kan uppgifter om chiffer, kod eller liknande metoder som används av informationssäkerhetsskäl komma att hanteras i samband med en teknisk analys av en incident.

7.1.3 18 kap. 13 § OSL

Sekretess gäller för uppgift som hänför sig till en myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer, om det kan antas att det allmännas möjligheter att förebygga och hantera fredstida kriser motverkas om uppgiften röjs (18 kap. 13 § OSL). Med begreppet fredstida krissituationer avses mycket allvarliga kriser, alltså inte olyckor och andra händelser av mer vardaglig karaktär. Verksamhet i form av risk- och sårbarhetsanalyser syftar till att minska samhällets sårbarhet, bl.a. genom att öka myndigheternas förmåga att förutse och hantera fredstida krissituationer. För att uppgifter i denna verksamhet inte ska kunna utnyttjas till angrepp mot myndigheter, enskilda eller samhället i stort är det i viss utsträckning nödvändigt att begränsa insynen i denna verksamhet. Eftersom sekretessen gäller för uppgifter som hänför sig till verksamhet för risk- och sårbarhetsanalyser, följer sekretessen med en uppgift som lämnas till en annan myndighet. När det gäller it-incidentrapporteringen kan bestämmelsen aktualiseras när det gäller allvarliga brister eller attacker mot samhällsviktiga anläggningar.

7.1.4 21 kap. 7 § OSL

Sekretess gäller för personuppgift, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen (1998:204), PUL (21 kap. 7 § OSL). Bestämmelsen innehåller ett förbud mot att lämna ut personuppgifter och är tillämplig hos sådana myndigheter som är personuppgiftsansvariga eller som annars har tillgång till personuppgifter. Med personuppgifter avses, liksom i PUL, all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Bedömningen ska inte ta sikte på om myndighetens utlämnande av uppgifter skulle strida mot PUL. Enligt 8 § PUL ska bestäm-

melserna i den lagen inte tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Bedömningen enligt 21 kap. 7 § OSL ska alltså avse om det kan antas att uppgifterna efter utlämnandet kommer att behandlas i strid med personuppgiftslagen.

7.1.5 Andra sekretessbestämmelser som kan aktualiseras

I 15 kap. 1 och 2 §§ OSL regleras utrikes- och försvarssekretessen. Där finns regler om sekretess till skydd för Sveriges säkerhet och Sveriges förhållande till andra stater eller mellanfolkliga organisationer. Utrikessekretessen gäller uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Försvarssekretessen gäller uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Förekommer sådana uppgifter, t.ex. uppgifter om funktionssätt och säkerhet i system som har betydelse för samhällets försörjning eller infrastruktur, omfattas de av dessa sekretessbestämmelser. Bestämmelserna gäller oberoende av hos vilken myndighet uppgifterna finns.

När MSB arbetar med incidentrapportering från enskilda, som lämnar incidentrapporter frivilligt, kan bestämmelser till förmån för intresset att skydda enskild i verksamhet som avser tillsyn m.m. aktualiseras. Enligt 30 kap. 23 § OSL gäller sekretess för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs (första punkten), och för uppgift om andra ekonomiska eller personliga förhållanden än som avses i första punkten för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet (andra punkten). Sekretessen gäller oberoende av hos vilken myndighet uppgifterna finns. Den typ av uppgifter som det i första han handlar om att hemlighålla är sådana som typiskt sett kan vara av intresse för

konkurrenter och som skulle skada verksamheten om de blev kända.

Även andra sekretessbestämmelser kan bli aktuella i MSB:s verksamhet kring it-incidentrapportering.

7.2 Sekretessbrytande bestämmelser

Sekretess gäller i förhållande till enskilda, men också mellan myndigheter. Syftet är i första hand att värna om den enskildes integritet. Om sekretess inte skulle gälla mellan myndigheter skulle uppgifter hos en myndighet kunna läggas till grund för åtgärder av en annan myndighet som skulle kunna vara till nackdel för den enskilde. Även den omständigheten att ett större antal tjänstemän kan få kunskap om ett känsligt förhållande kan vara skäl att upprätthålla sekretess mellan myndigheter.

En grundläggande princip är dock att myndigheter är skyldiga att samarbeta och bistå varandra i den utsträckning som kan ske, en princip som bl.a. kommer till uttryck i 6 § förvaltningslagen (1986:223). En precisering av den bestämmelsen finns i 6 kap. 5 § OSL, som innebär att en myndighet på begäran ska lämna uppgift som den förfogar över om inte uppgiften är sekretessbelagd, eller det skulle hindra arbetets behöriga gång.

I många fall måste myndigheter kunna utbyta information för att kunna utföra sina uppgifter. För att tillgodose myndigheters behov av information och informationsutbyte i sin verksamhet finns flera undantag från huvudregeln om sekretess mellan myndigheter. Sådana sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess finns i 10 kap. OSL. Sekretessbrytande bestämmelser finns även i andra författningar som OSL hänvisar till, eller som en uppgiftsskyldighet varvid 10 kap. 28 § OSL blir tillämplig. Nedan följer en redogörelse för de huvudsakliga sekretessbrytande bestämmelser i OSL som är av intresse när det gäller MSB:s förutsättningar att lämna ut uppgifter om rapporterade it-incidenter till Polismyndigheten eller till andra myndigheter.

7.2.1 10 kap. 24 § OSL

Bestämmelsen i 10 kap. 24 § OSL gör det möjligt för myndigheter att under vissa förutsättningar lämna uppgifter om misstankar om ett begånget brott till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som har till uppgift att ingripa mot brottet. En förutsättning för utlämnande är att fängelse ingår i straffskalan för brottet. En annan förutsättning är att brottet i fråga kan antas föranleda någon annan påföljd än böter.

Bestämmelsen innebär en möjlighet att lämna ut uppgifter om brottsmisstankar under angivna förutsättningar. Det är alltså inte fråga om någon uppgiftsskyldighet. Uppgiftslämnandet förutsätter inte att misstanken är av viss grad, eller att bedömningen av handlingens straffvärde ska kunna göras med viss säkerhet, utan det är myndigheten som avgör om uppgiften har sådan karaktär att den kan lämnas.

Den obligatoriska it-incidentrapporteringen omfattar it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Det är alltså fråga om allvarligare händelser som om de har sin grund i brottsliga angrepp i många fall kan antas föranleda strängare straff än böter. De brottsrubriceringar som främst kan antas aktualiseras är framför allt dataintrång och grovt dataintrång (4 kap. 9 c § brottsbalken). För dataintrång döms till böter eller fängelse i högst två år. För grovt dataintrång döms till fängelse lägst sex månader och högst sex år. Även andra brott som spionerі, sabotage, skadegörelse m.fl. brott kan aktualiseras i it-incidentsammanhang.

Utredningen gör bedömningen att flertalet rapporterade incidenter som kan antas ha sin grund i ett brottsligt angrepp, och de ur ett polisiärt perspektiv mest angelägna incidenterna, är sådana att MSB kan lämna uppgifter om incidenten till Polismyndigheten med stöd av den sekretessbrytande bestämmelsen i 10 kap. 24 § OSL.

7.2.2 10 kap. 27 § OSL – generalklausulen

För det fall att en it-incident inte bedöms innefatta gärning som föranleder annan påföljd än böter och i fall då uppgiften avser misstankar om förestående brottslighet kan 10 kap. 24 § OSL inte

läggas till grund för ett uppgiftslämnande. I dessa fall kan dock andra sekretessbrytande bestämmelser aktualiseras.

Enligt den s.k. generalklausulen i 10 kap. 27 § OSL får en sekretessbelagd uppgift lämnas till en annan myndighet om det är uppenbart att intresset av att lämna uppgiften har företräde framför det intresse som sekretessen har att skydda. Generalklausulen tillkom mot bakgrund av att sekretess inte bör hindra myndigheter från att utväxla uppgifter i situationer där intresset av att uppgifterna lämnas ut bör ha företräde framför intresset av att uppgifterna inte lämnas ut.

Generalklausulen kan inte tillämpas om utlämnandet strider mot lag eller förordning eller föreskrift som har meddelats med stöd av personsuppgiftslagen. Har det t.ex. i en lag föreskrivits att en viss myndighet för sin verksamhet på vissa villkor kan få ta del av även hemliga uppgifter hos en annan myndighet, kommer det givetvis inte på fråga att, när de angivna villkoren inte är uppfyllda, lämna ut uppgifterna med stöd av generalklausulen i stället. Om det i en lag eller förordning uttömmande anges i vilka fall uppgifter får lämnas mellan myndigheter kan generalklausulen inte heller tillämpas i andra fall.

Bestämmelsen är subsidiär i förhållande till andra sekretessbrytande bestämmelser och ska alltså inte tillämpas om någon annan sekretessbrytande bestämmelse kan tillämpas.

Med stöd av generalklausulen kan en myndighet lämna ut uppgifter om brottsmisstankar även utan någon uttrycklig begäran om det. Uppgifter kan lämnas ut inte bara beträffande begångna brott, utan även för att avvärja brott. Detta gäller oavsett vilken påföljd det misstänkta brottet kan antas föranleda. Om det hos en myndighet uppkommer misstankar om att ett brott har begåtts som inte kan antas föranleda annan påföljd än böter, kan myndigheten alltså ändå rapportera sina misstankar, om det är uppenbart att intresset av att uppgifterna lämnas ut har företräde framför det intresse som sekretessen ska skydda. Frågan om uppgifterna ska lämnas ut blir då beroende av en avvägning mellan dessa båda intressen. I praktiken torde det ofta finnas situationer där uppgifter kan lämnas ut därför att det finns ett intresse av att beivra även bötesbrottlighet samtidigt som sekretessintresset inte är särskilt framträdande.

Möjligheten att utväxla hemliga uppgifter får utnyttjas mera sparsamt och med större försiktighet om informationen inte är sekretesskyddad hos den mottagande myndigheten. Detta gäller särskilt i fråga om uppgifter som är hemliga av hänsyn till enskildas intressen. Om den uppgift som överlämnandet gäller inte blir sekretesskyddad hos den mottagande myndigheten kan risken för att skada ska uppkomma vara så stor att uppgiften inte bör lämnas ut. Att sekretessen hos den mottagande myndigheten är något svagare än hos den utlämnande myndigheten har inte ansetts spela så stor roll i praktiken.

Vid prövningen av en utlämnandefråga enligt generalklausulen ska en avvägning göras mellan den mottagnade myndighetens behov av uppgifterna och det intresse som sekretesskyddet typiskt sett tillgodoser. Ytterligare omständigheter som är av betydelse är uppgifternas art och i vilket syfte de ska användas.

Generalklausulen hindrar inte att utbyte av uppgifter mellan myndigheter sker rutinmässigt även utan särskild författningsreglering, även om det i förarbetena uttalas att rutinmässigt uppgiftsutbyte i regel ska vara författningsreglerat. I de fall där ett rutinmässigt uppgiftslämnande inte är författningsreglerat men ändå kan anses tillräckligt motiverat måste den intresseavvägning som ska göras ske på förhand. Den behöver då inte avse prövning av individuella fall. Bedömningen kan då göras på ett sätt som liknar den som ska ske i fråga om massuttag. I situationen med massuttag kan emellertid den berörde tjänstemannen av naturliga skäl inte bilda sig en uppfattning om den särskilda skaderisk som kan vara förbunden med en enskild uppgift. Å andra sidan har tjänstemannen alltid kännedom om beställarens identitet och oftast också om beställarens avsikt med uppgifterna. Dessa kunskaper i förening med en bedömning av den skaderisk som typiskt sett är förbunden med uppgifter av det slag som avses med beställningen bör enligt förarbetsuttalanden i de allra flesta fall ge fullt tillräckligt underlag för bedömningen av om sekretessregleringen ska anses hindra ett utlämnande eller inte.

När det gäller förutsättningarna för ett informationsutbyte mellan MSB och Polismyndigheten är syftet med ett sådant att öka Polismyndighetens tillgång till information om it-brottslighet, med en högre andel utredda och lagförda individer och därmed också en högre nivå av informationssäkerhet i samhället som följd. Detta är

ett intresse som vid tillämpning av generalklausulen typiskt sett får anses ha avsevärd vikt. När det i vart fall gäller statliga myndigheter som rapporterar it-incidenter till MSB finns inget traditionellt tungt integritetsintresse kopplat till enskilda att skydda. Den sekretess som uppgifterna omfattas av hos MSB gäller vidare oavsett hos vilken myndighet uppgifterna finns (se ytterligare härom avsnitt 8.1 nedan). Risken för skada vid ett överlämnande av uppgifterna från MSB till Polismyndigheten hindrar alltså inte ett överlämnande med stöd av generalklausulen.

Sammanfattningsvis gör utredningen bedömningen att för det fall bestämmelsen i 10 kap. 24 § OSL inte kan läggas till grund för ett uppgiftslämnande från MSB till Polismyndigheten kan detta uppgiftslämnande i de allra flesta fall stödjas på generalklausulen. Inte heller om uppgiftslämnandet är omfattande och rutinmässigt hindrar sekretessen att uppgifter hos MSB lämnas till Polismyndigheten.

7.2.3 10 kap. 28 § OSL

Enligt 10 kap. 28 § OSL hindrar sekretess inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Genom införandet av rapporteringsskyldigheten i 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap har en sådan sekretessbrytande bestämmelse som avses i 10 kap. 28 § OSL införts. Myndigheterna kan alltså med stöd av förordningen överlämna de uppgifter som avses där till MSB, även om uppgifterna omfattas av sekretess hos myndigheterna.

Det kan diskuteras om bestämmelsen också kan vara tillämplig på ett uppgiftslämnade från MSB till Polismyndigheten och andra myndigheter. För att bestämmelsen ska vara tillämplig krävs att uppgiftsskyldigheten uppfyller vissa krav på konkretion, som att exempelvis avse en myndighets skyldighet att lämna andra myndigheter information. Med hänsyn till MSB:s uppdrag enligt sin instruktion att bl.a. agera skyndsamt vid inträffade it-incidenter, sprida information och vid behov arbeta med samordning av åtgärder och medverka i arbetet som krävs för att avhjälpa eller lindra effekter av det inträffade kan möjligen en sådan tydlig uppgiftsskyldighet

anses föreligga att den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL är tillämplig i dessa fall.

7.2.4 10 kap. 2 § OSL

Med hänsyn till det uppdrag som MSB har enligt sin instruktion är även bestämmelsen i 10 kap. 2 § OSL av intresse. Sekretess enligt denna bestämmelse hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen kan vara tillämplig i fall där någon av de övriga sekretessbrytande reglerna inte gäller, men ska tillämpas restriktivt. En uppgift får lämnas ut med stöd av bestämmelsen bara när utlämnandet av uppgiften är en nödvändig förutsättning för att myndigheten ska kunna fullgöra ett visst åliggande. Bara bedömningen att effektiviteten i myndighetens handlande sätts ned genom en föreskriven sekretess får inte leda till att sekretessen åsidosätts.

7.2.5 6 kap. 5§ OSL

Ett uppgiftslämnande från en myndighet kan ske på eget initiativ, men också som ett resultat av att annan myndighet begär att få ta del av viss uppgift. En myndighet ska på begäran lämna uppgift den förfogar över om inte uppgiften är sekretessbelagd, eller det skulle hindra arbetets behöriga gång (6 kap. 5 § OSL). Är någon sekretessbrytande bestämmelse tillämplig, även generalklausulen 10 kap. 27 § OSL, ska uppgiften lämnas ut enligt denna bestämmelse. En myndighets beslut att inte lämna ut en uppgift kan överklagas.

7.3 Personuppgiftslagen

De it-incidentrapporter som MSB tar emot kan i vissa fall innehålla personuppgifter. Behandling av personuppgifter regleras i svensk rätt i första hand genom personuppgiftslagen (1998:204), PUL. Genom PUL genomfördes Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria

flödet av sådana uppgifter (dataskyddsdirektivet). Syftet med PUL är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. PUL innehåller generella bestämmelser och gäller inte i den utsträckning det har meddelats avvikande bestämmelser i någon annan lag eller förordning (2 § PUL).

Personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Enligt den s.k. finalitetsprincipen får personuppgifter inte heller behandlas för något ändamål om är oförenligt med det för vilket uppgifterna samlades in. (9 § första stycket c och d PUL) Undantag från finalitetsprincipen får dock göras om det är nödvändigt av hänsyn till bl.a. förebyggande, undersökning och avslöjande av brott.

Offentlighets- och sekretesskommittén (OSEK) behandlade i sitt huvudbetänkande (SOU 2003:99) finalitetsprincipens förhållande till sekretessregleringen, bl.a. 15 kap. 5 § i dåvarande sekretesslagen (nuvarande 6 kap. 5 § OSL). Enligt denna bestämmelse ska en myndighet på begäran av en annan myndighet lämna en uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra ärendets behöriga gång. Bestämmelsen omfattar såväl uppgifter som inte är sekretessreglerade som uppgifter som kan lämnas ut med tillämpning av en sekretessbrytande bestämmelse. OSEK anförde att regering och riksdag redan vid personuppgiftslagens tillkomst tagit ställning för att bestämmelsen i 15 kap. 5 § sekretesslagen inte strider mot dataskyddsdirektivet. Enligt OSEK ska således ett utlämnande av uppgifter till en annan myndighet, som är tillåtet enligt sekretessregleringen, anses vara förenligt med finalitetsprincipen (SOU 2003:99 s. 231 och prop. 1997/98:44 s. 116). Kommittén tillade att finalitetsprincipen har utformats i en politisk miljö där majoriteten av medlemsstaterna inte har någon offentlighetsprincip och därmed inte heller någon sekretessreglering. Kommittén ansåg att den svenska sekretessregleringen, vilken även gäller mellan myndigheter, fyller samma syfte som finalitetsprincipen eftersom den hindrar myndigheterna från att lämna ut integritetskänsliga uppgifter till andra myndigheter för ändamål som av lagstiftaren bedömts vara oförenliga med de ändamål för vilka uppgifterna samlats in (a.a. s. 232).

Behandling av personuppgifter i form av utlämnanden av uppgifterna är alltså förenliga med finalitetsprincipen så länge som ut-

lämnandena sker i överensstämmelse med lag eller förordning enligt vilken uppgifterna får eller ska lämnas ut. Härmed avses i första hand utlämnanden till annan myndighet enligt 6 kap. 5 § OSL och utlämnanden av sekretessreglerade uppgifter till en annan myndighet eller enskild, på begäran eller på eget initiativ, som sker med stöd av någon sekretessbrytande bestämmelse. Genom att reglera ett uppgiftslämnande får lagstiftaren anses ha tagit ställning till att sådana utlämnanden som ska eller får ske inte är oförenliga med ursprungliga ändamål. Myndigheterna är alltså bundna av den prövning enligt finalitetsprincipen som lagstiftaren gjort genom exempelvis en sekretessbrytande bestämmelse. (jfr Informationshanteringsutredningens slutbetänkande, *Myndighetsdatalag*, SOU 2015:39, s. 283 f.)

7.4 Utredningens bedömning

Utredningen bedömer att varken bestämmelser om sekretess eller bestämmelser om behandling av personuppgifter utgör hinder mot ett omfattande informationssamarbete rörande antagonistiska it-incidenter mellan MSB och Polismyndigheten.

De uppgifter som myndigheterna lämnar till MSB inom ramen för incidentrapporteringen omfattas normalt av sekretess. Sekretess gäller som huvudregel även mellan myndigheter. För att tillgodose myndigheters behov av information och informationsutbyte i sin verksamhet finns sekretessbrytande bestämmelser. Utredningens bedömning är att MSB utan hinder av sekretess kan lämna uppgifter om it-incidenter som har sin grund i brottsliga angrepp till Polismyndigheten i betydande utsträckning. Överlämnande av sådana uppgifter kan ske med stöd av bl.a. 10 kap. 24 § OSL och generalklausulen i 10 kap. 27 § OSL, och möjligen också med stöd av 10 kap. 28 § OSL. Som vid all tillämpning av denna lagstiftning måste frågan om att lämna ut en uppgift alltid bedömas i det konkreta fallet.

Eftersom uppgifterna kan lämnas ut med stöd av bestämmelser i OSL strider ett utlämnande inte heller mot finalitetsprincipen i PUL.

Det ska i sammanhanget också framhållas att MSB i sin roll att stödja och samordna arbetet med samhällets informationssäkerhet

också kan ha behov av att lämna uppgifter med anknytning till it-incidentrapporteringen till andra myndigheter än Polismyndigheten, för att exempelvis avvärja ett hot mot it-säkerheten eller att stödja en myndighet i arbetet med att förebygga incidenter. Ofta kan sådant utlämnande ske med stöd av generalklausulen, eller med stöd av bestämmelsen i 10 kap. 28 § OSL.

Sammanfattningsvis är det utredningens bedömning att bestämmelserna om sekretess normalt inte utgör ett hinder mot att MSB lämnar uppgifter om it-incidenter som har sin grund brottsliga angrepp till Polismyndigheten. Denna bedömning gäller med betydande säkerhet för de uppgifter som MSB förfogar över som ett resultat av den obligatoriska it-incidentrapporteringen från statliga myndigheter, där integritetsintressen till förmån för enskilda normalt inte gör sig gällande.

Vid underhandskontakter med MSB och Polismyndigheten har företrädare för båda myndigheterna delat utredningens bedömning att ett omfattande informationssamarbete mellan myndigheterna inte hindras av bestämmelser om sekretess. Det har i dessa kontakter inte framkommit att man inom myndigheterna finner gällande bestämmelser svårtillämpade, och man är inom MSB organiserad på ett sådant sätt att frågor om utlämnande bedöms kunna hanteras på ett effektivt och rättssäkert sätt.

8 Sekretessen hos brottsbekämpande myndigheter och hos domstol

En viktig del av samhällets informationssäkerhet är möjligheten att skydda känsliga uppgifter om bl.a. säkerhetssystem och sårbarheter. I kapitel 7 ovan har utredningen beskrivit de sekretessbestämmelser som är aktuella för uppgifter om it-incidenter hos Myndigheten för samhällsskydd och beredskap (MSB). I utredningens uppdrag ingår även att analysera vilka möjligheter som finns att bibehålla sekretess för aktuella uppgifter hos brottsbekämpande myndigheter och hos domstol vid ett eventuellt åtal, och därvid beakta de grundläggande principerna om förhandlingsoffentlighet och parts rätt till insyn i domstolsprocessen.

8.1 Sekretessen för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd gäller hos alla myndigheter

En grundläggande princip i offentlighets- och sekretesslagen (2009:400), OSL, är att sekretess som huvudregel inte följer med en uppgift när den lämnas till en annan myndighet. Sekretessintresset måste i varje sammanhang vägas mot intresset av insyn i myndighetens verksamhet. Om en sekretessreglerad uppgift lämnas från en myndighet till en annan gäller sekretess för uppgiften hos den mottagande myndigheten antingen om sekretess följer av en sekretessbestämmelse som är tillämplig hos den myndigheten, eller om sekretess följer av en bestämmelse om överföring av sekretess. Om ingen av dessa förutsättningar är uppfyllda blir uppgiften offentlig hos den mottagande myndigheten.

Räckvidden av de sekretessbestämmelser som redovisats i kapitel 7 är inte begränsad till någon viss typ av verksamhet eller ärende eller till att gälla hos viss myndighet. Bestämmelserna är tillämpliga hos alla myndigheter där uppgifterna finns. Sekretessen gäller följaktligen för uppgifterna oavsett i vilket sammanhang de förekommer. De uppgifter från it-incidentrapporteringen som omfattas av sekretess hos MSB kommer alltså att omfattas av sekretess även hos Polismyndigheten efter ett eventuellt överlämnande av uppgifterna dit, liksom hos Åklagarmyndigheten i de fall där den myndigheten ansvarar för brottsutredningen eller uppgifterna i samband med beslut i åtalsfrågan överlämnas dit. Uppgifterna i Polismyndighetens och Åklagarmyndighetens verksamhet skyddas emellertid också av förundersökningssekretess och av bestämmelser om sekretess till skydd för underrättelseverksamhet.

Uttrycket myndighet i OSL syftar även på domstolarna. De sekretessbestämmelser som kan vara tillämpliga på uppgifter i it-incidentrapporterna gäller därmed också hos domstolarna. Det finns emellertid bestämmelser som begränsar tillämpligheten av sekretessbestämmelser på uppgifter som läggs fram vid en domstolsförhandling eller som tas in i en dom eller ett beslut i ett mål eller ärende. Även parts rätt till insyn i förfarandet kan få betydelse för frågan om möjligheterna att bibehålla sekretess för uppgifterna.

8.2 Förundersökningssekretess och sekretess till skydd för underrättelseverksamhet

Jämte sekretessen enligt 18 kap. 8 §, som gällt för uppgifterna hos MSB och som gäller hos alla myndigheter, kan uppgifterna hos polis och åklagare också omfattas av förundersökningssekretess. Sekretess gäller bl.a. för uppgift som hänför sig till förundersökning i brottmål, till angelägenhet som avser användning av tvångsmedel och i annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av Polismyndigheten eller Åklagarmyndigheten, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (18 kap. 1 § OSL). Med förundersökning menas förundersökning enligt rättegångsbalken (RB). Med annan verksamhet som syftar till att förebygga uppdaga,

utreda eller beivra brott åsyftas brottsförebyggande och brottsbeivrande verksamhet i allmänhet utan anknytning till något konkret fall. Det kan gälla t.ex. arbetsrutiner, spaningsmetoder och uppgifter om namn på personer som biträder polisen vid spaningsarbete.

Sedan åtal har väckts gäller, på grund av skaderekvisitets utformning, sekretess enligt 18 kap. 1 § OSL bara för uppgifter som har generell betydelse för brottsspaning och brottsutredning. Efter åtal finns inte några utredningsåtgärder att skydda. De skyddsvärda uppgifterna från it-incidentrapporteringen kommer i de flesta fall troligen inte att omfattas av förundersökningssekretess sedan åtal väckts.

Sekretess gäller vidare för uppgift som hänför sig till Polismyndighetens arbete med att förebygga, förhindra eller upptäcka brottslig verksamhet, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas (10 kap. 2 § OSL). Det polisarbete som åsyftas är i första hand underrättelseverksamhet, dvs. arbete med insamling, bearbetning och analys av information för att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts.

Förundersökningssekretess och sekretess till skydd för underrättelseverksamhet gäller även hos andra myndigheter. Sådan sekretess kan gälla också hos myndigheter som inte bedriver brottsbekämpande verksamhet. Sekretessen gäller nämligen för uppgift som hänför sig till förundersökning eller underrättelseverksamhet hos bl.a. Polismyndigheten och Åklagarmyndigheten. Det innebär att sekretessen följer med uppgiften när den lämnas vidare till en annan myndighet.

8.3 Sekretess under och efter en huvudförhandling

En förhandling vid domstol ska vara offentlig (2 kap. 11 § andra stycket regeringsformen). Förhandlingsoffentligheten får dock begränsas genom lag (2 kap. 20 § första stycket 4 regeringsformen).

Som huvudregel upphör en sekretessbestämmelse som gäller för en uppgift i ett mål eller i ett ärende i en domstols rättskipande eller rättsvårdande verksamhet att vara tillämplig om uppgiften

läggs fram vid en offentlig förhandling (43 kap. 5 § första stycket OSL). Huvudregeln gäller dock inte för uppgifter som lagts fram vid en förhandling inom stängda dörrar.

En domstol får hålla förhandling inom stängda dörrar, om det kan antas att det vid förhandlingen kommer att läggas fram uppgifter för vilka hos domstolen gäller sekretess enligt OSL (5 kap. 1 § andra stycket RB). För ett beslut om stängda dörrar krävs som huvudregel dessutom att det bedöms vara av synnerlig vikt att uppgiften hålls hemlig.

Om en uppgift för vilken det gäller sekretess läggs fram vid en förhandling inom stängda dörrar är sekretessbestämmelsen tillämplig även under domstolens fortsatta handläggning av målet eller ärendet, om domstolen inte beslutar annat (43 kap. 5 § andra stycket OSL). När domstolen skiljer målet eller ärendet från sig måste sekretessfrågan slutligt prövas. Sekretessbestämmelsen fortsätter att vara tillämplig i den utsträckning som domstolen beslutar om det. Utan ett sådant särskilt beslut upphör alltså sekretessbestämmelsen att vara tillämplig även för sådana uppgifter som lagts fram vid en förhandling inom stängda dörrar.

Överklagas ett avgörande i vilket en domstol har beslutat att en sekretessbestämmelse som gäller för en viss uppgift ska vara tillämplig även i fortsättningen, ska den högre domstolen pröva om beslutet ska fortsätta att gälla när den skiljer målet eller ärendet från sig (43 kap. 10 § OSL).

8.4 Sekretess för uppgifter i domar och beslut

En sekretessbestämmelse som gäller för en uppgift i ett mål eller ärende upphör som huvudregel att vara tillämplig i målet eller ärendet om uppgiften tas in i en dom eller ett beslut (43 kap. 8 § första stycket OSL). Bestämmelsen om detta s.k. offentlighetsdop gäller i fråga om uppgifter som inte tidigare blivit offentliga genom att de lagts fram vid en offentlig förhandling.

Domstolen har dock möjlighet att besluta att en sekretessbestämmelse som gäller för en viss uppgift ska fortsätta att vara tillämplig på uppgiften när den ingår i en dom eller ett beslut (43 kap. 8 § andra stycket första meningen OSL). Denna prövning är fristående i förhållande till den prövning domstolen gör när den

överväger om hela eller delar av en förhandling ska hållas inom stängda dörrar. Genom konstruktionen med ett offentlighetsdop och en möjlighet för domstolarna att besluta om fortsatt sekretess ges ett utrymme för domstolarna att i rimlig utsträckning ta hänsyn till såväl de intressen som talar för att domstolarnas domar och beslut i så stor utsträckning som möjligt ska vara offentliga, som de intressen som talar för att bevara sekretessen när det behövs med hänsyn till omständigheterna i det enskilda fallet.

Trots ett beslut om fortsatt sekretess är inte frågan om sekretess för en uppgift i domen eller beslutet avgjord en gång för alla. Sekretessfrågan ska prövas varje gång det blir aktuellt att lämna ut domen eller beslutet. Om en sådan prövning resulterar i att domstolen helt eller delvis vägrar lämna ut uppgiften eller lämnar ut den med förbehåll får beslutet normalt överklagas. Ett beslut om en sekretessbestämmelses fortsatta tillämplighet är alltså en förutsättning för att en viss sekretessbestämmelse ska få tillämpas. Ett sådant beslut medför dock inte att sekretess gäller med automatik.

Även om sekretessen för uppgifterna skulle upphöra i målet eller ärendet hos domstolen, kan sekretess för uppgifterna fortsätta att gälla hos andra myndigheter där uppgifterna finns.

Det kan också nämnas att vid domstolsförhandling under pågående förundersökning får rätten besluta om stängda dörrar med hänsyn till förundersökningssekretess, även om det inte bedöms vara av synnerlig vikt att uppgiften hålls hemlig.

8.5 Allmänt om partsinsyn

Med begreppet partsinsyn avses en parts rätt att på olika sätt få insyn i det förfarande där han eller hon är part. Partsinsynen kan t.ex. innebära en rätt att få ta del av handlingar eller annat material som finns i ett mål eller ärende, s.k. aktinsyn. Partsinsynen syftar bl.a. till att tillgodose partens behov av insyn för att kunna föra sin talan och är alltså något annat än den rätt till insyn som enskilda har i allmänna handlingar enligt tryckfrihetsförordningen och i domstolsförhandlingar enligt regeringsformen. Den som är part i ett mål eller ärende hos domstol eller annan myndighet har mot den bakgrunden under vissa förutsättningar en mera långtgående rätt än andra att få ut hemliga handlingar och uppgifter. Som

huvudregel hindrar sekretess inte att den som är part i ett mål eller ärende hos domstol eller annan myndighet och som på grund av sin partsställning har rätt till insyn i handläggningen, tar del av en handling eller annat material i målet eller ärendet. Rätt till insyn kan följa av föreskrifter i annan författning än OSL, praxis eller av allmänna rättsgrundsatser.

Insynsrätten kan sträcka sig olika långt beroende på vilket skede det rättsliga förfarandet befinner sig i. En misstänkt har t.ex. efter delgivning av misstanke enligt 23 kap. 18 § RB rätt att fortlöpande, i den mån det kan ske utan men för utredningen, ta del av det som har förekommit vid undersökningen. När förundersökningen är färdig, och den misstänkte slutdelges enligt samma bestämmelse, går det inte längre att hävda att ett röjande av uppgifter i förundersökningen är till men för utredningen. Det går då inte att med stöd av rättegångsbalkens bestämmelser undanhålla den misstänkte något material i förundersökningen, utan utredningsmaterialet omfattas av insynsrätten, även så kallat sidomaterial.

Rätten att ta del av de omständigheter som ligger till grund för ett beslut om anhållande eller häktning kan inte begränsas med hänsyn till utredningen(24 kap. 9 a § RB). Den som anhålls eller häktas har alltså en mer omfattande insynsrätt än en misstänkt som inte frihetsberövats.

Det är först i och med ett positivt åtalsbeslut som den misstänkte har rätt att få en kopia av förundersökningsprotokollet (23 kap. 21 § 4 RB). För det fall åklagaren beslutar att inte väcka åtal pågår inte längre något undersökningsförfarande, vilket innebär att den misstänktes insynsrätt enligt 23 kap. 18 § RB upphör. Det har då inte heller uppkommit någon rätt enligt rättegångsbalken för den misstänkte att få en kopia av förundersökningsprotokollet.

Även om insynsrätten upphört enligt rättegångsbalken kan det enligt praxis ändå föreligga insynsrätt efter det att ett ärende har avslutats. Utgångspunkten är då att den privilegierade ställningen som part bör bestå om den enskilde har beaktansvärda motiv för sin begäran om insyn.

I rättegångsbalken finns inte några uttryckliga bestämmelser vare sig om en tilltalads rätt till insyn i brottmålsprocessen eller om tilltalads rätt att få del av processmaterial eller annat aktmaterial i ett mål eller ärende vid domstol. En sådan rätt finns dock och kan

härledas både från rättegångsbalken och från Europakonventionen. Insynsrätten följer av bl.a. principerna om muntlighet och omedelbarhet. Den tilltalades insynsrätt enligt 23 kap. 18 § RB upphör när brottmålsdomen vinner laga kraft.

8.6 Partsinsyn och sekretess – kollisionsbestämmelsen

Att det finns en rätt enligt rättegångsbalken eller annars enligt allmänna rättsgrundsatser att ta del av utredningsmaterial utesluter inte att det kan finnas hinder mot att få ut uppgifter som omfattas av särskilda sekretessbestämmelser i OSL. De sekretessbestämmelser som utredningen redogjort för i avsnitt 7.1.1–7.1.5 är exempel på sådana särskilda sekretessbestämmelser.

Konflikten mellan parts rätt till insyn och den sekretess som kan gälla enligt bestämmelser i OSL regleras i den s.k. kollisionsbestämmelsen i 10 kap. 3 § OSL. Där anges att sekretess inte hindrar att en enskild som är part i ett mål eller ärende hos domstol eller annan myndighet och som på grund av sin partsställning har rätt till insyn i handläggningen, tar del av en handling eller annat material i målet eller ärendet. En sådan handling eller ett sådant material får dock inte lämnas ut till parten i den utsträckning det av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att sekretessbelagd uppgift i materialet inte röjs. I sådana fall ska myndigheten på annat sätt lämna parten upplysning om vad materialet innehåller i den utsträckning det behövs för att parten ska kunna ta till vara sin rätt och det kan ske utan allvarlig skada för det intresse som sekretessen ska skydda. Sekretess hindrar aldrig att en part i ett mål eller ärende tar del av en dom eller ett beslut i målet eller ärendet. Inte heller innebär sekretess någon begränsning i en parts rätt enligt rättegångsbalken att få del av alla omständigheter som läggs till grund för avgörande i ett mål eller ärende. Om det i lag finns bestämmelser som avviker från det som nu nämnts, gäller de bestämmelserna.

Det är inte bara slutliga avgöranden i mål eller ärenden som omfattas av bestämmelsen. Även beslut under förundersökning och rättegång omfattas, t.ex. beslut om anhållande och häktning. Bestämmelsen ger inte i sig någon rätt till insyn i förfaranden enligt

rättegångsbalken, utan rätten till insyn måste grunda sig på rättegångsbalken eller de principer som den vilar på.

Genom vägledande praxis anses det numera klarlagt att förundersökningsförfarandet är ett ärende där den misstänkte är part och har en insynsrätt enligt rättegångsbalken. 10 kap. 3 § OSL är alltså tillämplig på förundersökningsförfarandet. I och med att den misstänkte är att anse som part kan hans eller hennes insyn endast inskränkas med stöd av en sekretessbestämmelse om det är av synnerlig vikt att uppgiften inte röjs.

8.7 Utredningens bedömning

Utredningen bedömer att bestämmelserna om sekretess i de brottsbekämpande myndigheternas verksamhet och bestämmelserna om förhandlingsoffentlighet och parts rätt till insyn i domstolsprocessen inte utgör ett hinder mot ett omfattande informationsutbyte mellan MSB och Polismyndigheten.

En hög informationssäkerhetsnivå kräver att samhället kan skydda känsliga uppgifter om bl.a. säkerhetsåtgärder och sårbarheter i våra it-system. Räckvidden av de sekretessbestämmelser som är tillämpliga på skyddsvärda uppgifter i MSB:s verksamhet med incidentrapporteringen är inte begränsad till någon viss typ av verksamhet eller ärende eller till att gälla hos viss myndighet. Sekretess för uppgifterna gäller alltså även hos de brottsbekämpande myndigheterna och hos domstol. I polisens och Åklagarmyndighetens verksamhet gäller därutöver förundersökningssekretess fram till dess att åtal väckts. Uppgifterna torde i vissa fall och under vissa förutsättningar kunna hemlighållas även gentemot part.

Regelverket ger de brottsbekämpande myndigheterna goda förutsättningar att skydda de skyddsvärda uppgifterna från it-incidentrapporteringen genom hela rättskedjan. Hur väl dessa uppgifter skyddas avgörs dock av hur polis och åklagare bedriver den brottsutredande verksamheten i praktiken.

Utredningen har i underhandskontakter med företrädare för Polismyndigheten och Åklagarmyndigheten undersökt hur dessa myndigheter ser på möjligheterna att utifrån gällande lagstiftning skydda känsliga uppgifter i brottsutredningar om dataintrång eller liknande brottslighet. I den brottsutredande verksamheten måste

ständigt svåra avvägningar göras, t.ex. när det gäller vilka delar av förundersökningsmaterialet som ska åberopas som bevis i domstol, vad som ska tas in i ett förundersökningsprotokoll och när och på vilket sätt den som misstänks för brott ska få ta del av utredningsmaterialet. Det gäller vid all typ av brottslighet där uppgifter som omfattas av sekretess förekommer, och är inte en utmaning enbart i samband med utredningar om dataintrång eller liknande brottslighet.

Både inom polisen och hos åklagarväsendet finns uppfattningen att det nuvarande regelverket ger ett tillräckligt stort utrymme för de brottsutredande myndigheterna att skydda känslig information, både i förhållande till allmänheten och i förhållande till eventuell part. Myndigheterna har inte sett behov av förändringar av regelverket mot denna bakgrund.

En samstämmig uppfattning hos Polismyndigheten och Åklagarmyndigheten är vidare att en ökad medvetenhet och till en sådan medvetenhet kopplade utbildningsinsatser skulle ge polis och åklagare än bättre förutsättningar att klara både uppdraget att klara upp fler it-brott och att skydda känslig information i ärenden om it-brottslighet.

Sammanfattningsvis anser utredningen att möjligheterna att bibehålla sekretess för aktuella uppgifter hos brottsbekämpande myndigheter och hos domstol är sådana att det inte finns anledning att avstå åtgärder i syfte att fler it-incidenter som har sin grund i brottsliga handlingar ska komma till Polismyndighetens kännedom. Genomförs sådana åtgärder ser utredningen inte några behov av förändringar av regelverket kring den brottsutredande verksamheten.

9 Överväganden och förslag

9.1 En uppgiftsskyldighet för Myndigheten för samhällsskydd och beredskap införs

Förslag: Myndigheten för samhällsskydd och beredskap (MSB) ska vara skyldig att lämna uppgifter om sådana it-incidenter som rapporterats i enlighet med 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap till Polismyndigheten om det finns anledning att anta att incidenten har sin grund i en brottslig gärning.

Skälen för promemorians förslag

Utredningens uppdrag har varit att analysera och föreslå åtgärder för att öka Polismyndighetens tillgång till information om it-brottslighet. Utgångspunkten för uppdraget har varit att en hög nivå av informationssäkerhet i samhället förutsätter att it-angrepp kan förebyggas, upptäckas och hindras, men också att individer som ägnar sig åt sådan brottslig verksamhet kan utredas och lagföras.

Det faktum att ett stort antal it-incidenter som har sin grund i brottsliga gärningar inte kommer till polisens kännedom är ett betydande hot mot informationssäkerheten. En viktig del av samhällets insatser på informationssäkerhetsområdet är kriminaliseringen av vissa handlingar och de brottsbekämpande myndigheternas verksamhet med att förebygga, ingripa mot och utreda sådan brottslighet. Att it-angrepp utreds ger utöver möjligheten till att brottet klaras upp också kunskaper om bl.a. tillvägagångssätt och aktörer, vilket är av stort värde vid utformningen av olika skydds-

åtgärder. En effektiv lagföring av it-angrepp är viktig för att minska benägenheten att begå sådana brott.

Den nya ordningen med obligatorisk it-incidentrapportering innebär att MSB inom ramen för sin verksamhet bl.a. kommer att samla in och hantera uppgifter om att statliga förvaltningsmyndigheter utsatts för brott. Dessa brott kan utgöra allvarliga hot och innebära betydande skada utifrån ett informationssäkerhetsperspektiv, och det är angeläget att denna brottslighet bekämpas. Om det kan antas att den rapporterade incidenten har sin grund i en brottslig gärning har MSB en skyldighet att uppmana den rapporterande myndigheten att anmäla händelsen till Polismyndigheten. Den rapporterande myndigheten har dock ingen skyldighet att följa MSB:s uppmaning. Utredningen ser stora risker med att denna ordning också i framtiden kommer att innebära att många allvarliga it-incidenter inte polisanmäls.

För sådana it-incidenter som faller under säkerhetsskyddsförordningens krav på obligatorisk rapportering till Säkerhetspolisen eller Försvarsmakten gäller redan en ordning där vissa incidenter ska rapporteras till en brottsutredande myndighet. När Säkerhetspolisen får del av sådana uppgifter kan myndigheten agera både i egenskap av tillsynsmyndighet för säkerhetsskyddet och i egenskap av brottsutredande myndighet. Säkerhetspolisen samverkar i dessa brottsutredningar ofta nära med Polismyndigheten och resurser och kompetens inom båda myndigheterna kan tas i anspråk. Denna samverkan innefattar ett omfattande utbyte av information mellan myndigheterna, vilket sker med stöd av de sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Kravet på rapportering enligt säkerhetsskyddsförordningen gäller bl.a. för sådana incidenter som allvarligt kan påverka säkerheten i ett system där hemliga uppgifter behandlas i en omfattning som inte är ringa eller om incidenten allvarligt kan påverka säkerheten i ett informationssystem som särskilt behöver skyddas mot terrorism. Sådana incidenter utgör typiskt sett mycket allvarliga hot mot informationssäkerheten där särskilda intressen att utreda bakomliggande brott gör sig gällande. Utredningen vill dock framhålla att även sådana incidenter som faller utanför säkerhetsskyddsförordningens tillämpningsområde, och som därför ska rapporteras till MSB, kan vara väl så angelägna att utreda ur ett brottsbekämpande perspektiv.

Utredningen har i kapitel 7 ovan, med instämmande av både MSB och Polismyndigheten, bedömt att bestämmelser om sekretess normalt inte hindrar att uppgifter om sådana it-incidenter som rapporteras till MSB med stöd av 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap lämnas till Polismyndigheten. Såsom tillämpningsföreskrifterna till förordningen utformats ska rapporterande myndigheter rapportera it-incidenten senast 24 timmar efter att myndigheten upptäckt incidenten. Rapporten ska bl.a. innehålla en beskrivning av it-incidenten som även inkluderar en övergripande redovisning av händelseförlopp och vidtagna åtgärder, den exakta eller uppskattade tidpunkten för när it-incidenten inträffade, uppgift om när myndigheten upptäckte it-incidenten och om den alltjämt pågår eller är avslutad. Rapporten ska även innehålla myndighetens initiala bedömning av it-incidentens omfattning och konsekvenser, både faktiska och potentiella. Utredningen bedömer mot den bakgrunden att rapporterna ofta kan innehålla uppgifter av stort värde för den polisiära verksamheten.

Till MSB:s uppdrag hör att stödja samhället i arbetet med att förebygga och hantera it-incidenter, och i MSB:s instruktion preciseras särskilt myndighetens ansvar att agera skyndsamt vid it-incidenter genom att bl.a. sprida information och samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet. Utredningen har i kapitel 6 ovan redogjort för de statliga myndigheternas grundläggande skyldighet att samarbeta och bistå varandra i den utsträckning som kan ske. För utredningen har det varit en naturlig utgångspunkt att MSB och Polismyndigheten så långt det är möjligt med hänsyn till rättsliga och verksamhetsmässiga förutsättningar bör utveckla sin samverkan utifrån sina respektive uppgifter och roller i informationssäkerhetsarbetet.

Utredningen har därför i underhandskontakter med MSB och Polismyndigheten undersökt förutsättningarna för en överenskommelse mellan myndigheterna om ett informationssamarbete om it-incidenter. Utredningen har med instämmande av myndigheterna konstaterat att ett informationssamarbete myndigheterna emellan inte förutsätter några författningsändringar. Ett arbete mellan myndigheterna har också inletts med att utveckla samverkansformer på informationssäkerhetsområdet för att jämte gemensamma forum som SAMFI m.fl. stärka sina bilaterala kon-

taktytor på såväl operativ som strategisk nivå. När denna promemoria lämnas till regeringen är arbetet med en sådan överenskommelse inte avslutat.

Från MSB:s sida har dock meddelats att myndigheten inte kommer att medverka till en överenskommelse som innebär en skyldighet att lämna uppgifter om rapporterade it-incidenter till Polismyndigheten. Som grund för sin inställning har MSB i huvudsak anfört att en ordning där uppgifter om rapporterade it-incidenter lämnas vidare till Polismyndigheten innebär en risk för att myndigheternas benägenhet att rapportera it-incidenter till MSB minskar. Det finns också en risk att kvaliteten i rapporterna påverkas genom att myndigheterna blir mer knapphändiga i sin informationslämning för att inte riskera att känslig information sprids till fler aktörer. MSB ser det som viktigt att hanteringen av informationen i systemet för obligatorisk it-incidentrapportering åtnjuter största förtroende hos de myndigheter som rapporterar it-incidenter, och att de rapporterande myndigheterna kan bibehålla en kontroll över hanteringen av den känsliga information som rapporterna innehåller.

MSB framhåller vidare att kraven på obligatorisk it-incidentrapportering infördes den 1 april 2016 och att arbetet med att etablera och skapa förtroende för systemet är inne i ett känsligt skede. Att redan nu genomföra betydande förändringar bedömer MSB som olämpligt.

MSB framhåller också att myndigheten uppmanar myndigheter som drabbats av brott att polisanmäla. MSB har påpekat att man i det sammanhanget kan agera mer aktivt än tidigare genom att jämte uppmaningen också lämna viss information om polisens verksamhet och även förmedla kontaktuppgifter till Polismyndigheten till de myndigheter som önskar sådana.

Utredningen anser i likhet med MSB att det finns utrymme att mer aktivt än tidigare verka för att rapporterande myndigheter polisanmäler. Enkla åtgärder som att förmedla kontaktuppgifter till Polismyndighetens nationella it-brottscenter kan i det sammanhanget ha betydelse. Utredningen har också noterat att MSB inte närmare följer upp om rapporterande myndigheter går vidare med en polisanmälan, en åtgärd som sannolikt skulle kunna påverka anmälningsbenägenheten i positiv riktning.

Det har inte varit möjligt för utredningen att inom uppdragets tidsram dra säkra slutsatser om de rapporterande myndigheternas benägenhet att enligt den nya ordningen med obligatorisk it-incidentrapportering följa MSB:s uppmaningar att anmäla incidenter till polisen. De angrepp som rapporterats till MSB under april och maj månad 2016 har dock såvitt utredningen kunnat utröna inte i något fall anmälts till polisen (se avsnitt 4.3.3 ovan).

Utredningen har övervägt att föreslå regeringen att cirka ett år efter ikraftträdandet utvärdera den nya ordningen innan andra åtgärder vidtas. Utredningen bedömer emellertid att risken är stor att även mer aktiva åtgärder från MSB:s sida för att få myndigheter att polisanmäla inte kommer att vara tillräckligt effektiva. Frågan om myndigheternas benägenhet att anmäla är komplex, och risken finns att enskilda myndigheters agerande styrs av andra faktorer än sådana som är till gagn för samhällets samlade informationssäkerhetsarbete. Av liknande skäl som ligger till grund för införandet av obligatorisk it-incidentrapportering till MSB bör därför åtgärder vidtas för att säkerställa att Polismyndigheten får tillgång till den information om it-incidenter som MSB förfogar över och där det finns anledning att anta att incidenten har sin grund i en brottslig gärning.

Ytterst handlar dessa frågor om en politisk avvägning av vilken vikt brottsbekämpningen ska tillmätas i förhållande till andra delar av samhällets informationssäkerhetsarbete. Utgångspunkten för denna utrednings uppdrag är att det är angeläget att brottsliga gärningar som utgör ett hot mot informationssäkerheten utreds, och att de individer som ansvarar för sådana handlingar lagförs. Denna utgångspunkt kan tyckas självklar, men utredningen har också noterat att det länge har varit en omdiskuterad fråga, både nationellt och internationellt, vilken vikt de brottsbekämpande myndigheternas insatser tillmäts i informationssäkerhetsarbetet.

Detta förhållningssätt återspeglas i MSB:s farhågor om vad det skulle betyda för myndigheternas rapporteringsvilja om uppgifter om it-incidenter lämnas vidare till Polismyndigheten. Som utredningen konstaterat under kapitel 8 har de brottsbekämpande myndigheterna med gällande regelverk goda förutsättningar att skydda känsliga uppgifter under en brottsutredning och hos domstol vid ett eventuellt åtal. Utredningen har inte heller kunna finna några risker i förhållande till verksamhetsintressen hos MSB eller rap-

porterande myndigheter för det fall att polis och åklagare i fler fall än i dag skulle utreda sådana brott. Självfallet förutsätter polis och åklagares verksamhet med att utreda it-angrepp och liknande brott både professionalism och ett nära och förtroendefullt samarbete med den myndighet eller annan som drabbats av brott. Utredningen kan inte utgå från något annat än att de brottsbekämpande myndigheterna kan bära det ansvaret.

Utredningen anser mot denna bakgrund att MSB, trots de invändningar som myndigheten framfört, ska lämna uppgifter om sådana it-incidenter som rapporterats i enlighet med 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap till Polismyndigheten om det finns anledning att anta att incidenten har sin grund i en brottslig gärning. Uppgiftslämnandet ska inte förutsätta den rapporterande myndighetens samtycke.

I kapitel 5 ovan redovisas en undersökning av ordningen för informationsdelning i Nederländerna, Norge och Tyskland. I dessa länder finns ingen eller endast mer begränsade skyldigheter för behöriga myndigheter med ansvar för nät- och informationssäkerhet att rapportera incidenter till brottsbekämpande myndigheter än vad som här föreslås. I den europeiska cybersäkerhetsstrategi som EU-kommissionen presenterade 2013 anges emellertid att nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet bör rapportera incidenter som misstänks vara av allvarlig brottslig karaktär till brottsbekämpande myndigheter.

Polismyndigheten framförde i sitt remissvar på förslaget om obligatorisk incidentrapportering att systemet borde utformas så att incidenter som rör misstanke om brott och inte faller inom Säkerhetspolisens tillsynsområde borde rapporteras direkt till Polismyndigheten som första mottagare. Regeringen beslutade att även sådana incidenter ska rapporteras till MSB. Utredningen anser att det inte finns skäl att nu göra en annan bedömning, utan att Polismyndighetens behov av information om sådana incidenter väl tillgodoses av en uppgiftsskyldighet för MSB.

9.2 Uppgiftsskyldigheten regleras i förordning

Förslag: MSB:s skyldighet att lämna uppgifter till Polismyndigheten regleras i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Uppgiftsskyldighetens närmare omfattning och innebörd samt formerna för uppgiftslämnandet regleras inte.

Skälen för promemorians förslag

En författningsreglerad uppgiftsskyldighet är som beskrivits ovan inte nödvändig för att MSB ska kunna lämna uppgifter om it-incidenter till Polismyndigheten. Att MSB har sådana möjligheter följer redan av MSB:s uppdrag och av att bestämmelser om sekretess normalt inte hindrar ett sådant uppgiftslämnande. Att uppgiftsskyldigheten författningsregleras innebär dock att uppgifter som omfattas av sekretess kan lämnas till Polismyndigheten även med stöd av 10 kap. 28 § offentlighets- och sekretesslagen (2009:400), OSL.

Flera invändningar kan resas mot att författningsreglera en uppgiftsskyldighet mellan MSB och Polismyndigheten. Ett syfte med regler om uppgiftsskyldighet mellan myndigheter är normalt att undanröja eventuella sekretesshinder för ett informationssamarbete, vilket inte är fallet här. MSB:s verksamhet på informationssäkerhetsområdet och i övrigt förutsätter vidare att myndigheten i många sammanhang lämnar uppgifter till och samverkar med andra myndigheter. En bestämmelse om MSB:s skyldighet att lämna vissa uppgifter till Polismyndigheten, och frånvaron av bestämmelser om uppgiftslämnande till andra myndigheter och i andra sammanhang, riskerar att skapa otydlighet om räckvidden av MSB:s samverkansansvar.

Utredningen har därför övervägt alternativet att regeringen i stället genom myndighetsstyrningen säkerställer att ett effektivt och ändamålsenligt informationssamarbete etableras mellan MSB och Polismyndigheten. Myndighetsstyrningen kan i så fall ske genom ett gemensamt särskilt uppdrag till MSB och Polismyndigheten att säkerställa att Polismyndigheten får tillgång till sådana uppgifter om it-angrepp som MSB förfogar över genom den obligatoriska incident-rapporteringen. Ett gemensamt uppdrag, med krav på åter-

rapportering till regeringen, lämnar också ett utrymme för myndigheterna att flexibelt hitta en effektiv och ändamålsenlig lösning. Utredningen bedömer att ett sådant uppdrag är en väl så effektiv åtgärd som en författningsreglerad uppgiftsskyldighet.

Ska uppgiftsskyldigheten författningsregleras förordar utredningen att bestämmelsen tas in i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap i anslutning till bestämmelsen om obligatorisk incidentrapportering. Att bestämmelsen avser lämnande av uppgifter om misstänkt brottslighet till en brottsbekämpande myndighet och bestämmelsens sekretessbrytande karaktär hindrar inte att den meddelas i form av förordning (jfr 10 kap. 28 § OSL).

Bestämmelsen bör utformas så att uppgiftsskyldigheten endast omfattar sådana uppgifter som MSB inhämtat med stöd av bestämmelsen om obligatorisk it-incidentrapportering, och inte sådana it-incidenter som MSB får information om på andra sätt, som när andra än statliga förvaltningsmyndigheter frivilligt lämnar uppgifter till MSB.

En särskild utredare har fått i uppdrag att senast den 1 maj 2017 lämna förslag till hur EU:s direktiv om nät- och informationssäkerhet (NIS-direktivet) ska kunna genomföras i svensk rätt. Utredningen finner inte anledning att här närmare överväga omfattningen av MSB:s uppgiftsskyldighet gentemot Polismyndigheten för det fall att även kommuner, landsting och vissa enskilda till följd av genomförandet blir skyldiga att rapportera it-incidenter till MSB. Utredningen förordar att denna fråga övervägs närmare inom ramen för utredningen om genomförandet av NIS-direktivet.

Skyldigheten för MSB att lämna uppgift till Polismyndigheten ska gälla då det finns anledning att anta att incidenten har sin grund i en brottslig gärning. Av 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap följer att den obligatoriska incidentrapporteringen i sig avgränsats till allvarliga incidenter. Utredningen ser inte anledning att bland dessa incidenter avgränsa MSB:s uppgiftsskyldighet i förhållande till Polismyndigheten ytterligare, till exempel genom att endast omfatta vissa brott eller brott av visst straffvärde. Uppgiftsskyldigheten bör i stället gälla generellt.

Av MSB:s tillämpningsföreskrifter framgår att rapporterande myndigheter ska klassificera incidenten, varvid en kategori utgör

angrepp. Det är normalt i dessa fall som skyldigheten att lämna uppgift till Polismyndigheten kommer att inträda. Den föreslagna uppgiftsskyldigheten är alltså avsedd att gälla i de situationer där MSB enligt gällande förordning har en skyldighet att uppmana den rapporterande myndigheten att anmäla incidenten till polisen.

Införs en skyldighet för MSB att lämna uppgift om incidenten till Polismyndigheten saknas skäl att föreskriva att MSB ska uppmana den rapporterande myndigheten att polisanmäla.

Uppgiftsskyldighetens närmare omfattning och innebörd bör inte regleras i förordningen utan utformas i samråd mellan myndigheterna. För polisens verksamhet är den grundläggande informationen att incidenten inträffat, vilken myndighet som rapporterat incidenten och hur Polismyndigheten kan kontakta myndigheten de mest centrala uppgifterna som MSB förfogar över. Även annan information som MSB inhämtar om incidentens karaktär, tidpunkt när den inträffade, om den pågår eller är avslutad och incidentens konsekvenser kan vara av stor betydelse för polisen i ett inledande skede.

En uppgiftsskyldighet för MSB syftar inte till att ersätta polisens behov av att inhämta uppgifter direkt från den rapporterande myndigheten. Uppgiftsskyldighetens främsta funktion är enligt utredningen att den ger Polismyndigheten förutsättningar att etablera en egen kontakt med den rapporterande myndigheten. Utredningen bedömer att en sådan kontakt sannolikt kommer att påverka myndighetens vilja och benägenhet att bistå polis och åklagare i utredningen av brottet. En erfarenhet som ofta framhållits i våra kontakter med både Polismyndigheten, Åklagarmyndigheten och Säkerhetspolisen är att det inom de allra flesta brottsutredningar etableras ett nära och förtroendefullt samarbete med den drabbade myndigheten. Ofta finns initialt ett flertal frågeställningar om hur brottsutredningen kan komma att påverka myndighetens verksamhet och om de brottsutredande myndigheternas förutsättningar att bl.a. skydda känsliga uppgifter, men när väl en dialog etablerats fungerar samarbetet i de allra flesta fall mycket väl.

Förordningen bör inte reglera formerna för hur uppgifterna lämnas till Polismyndigheten, utan även detta bör utformas i samråd mellan myndigheterna. En naturlig ordning är att tjänstemän vid MSB:s Verksamhet för cybersäkerhet och skydd av samhällsviktig verksamhet och poliser vid Polismyndighetens nationella it-

brottscenter gemensamt utarbetar formerna för denna samverkan. Beroende på situation, informationens karaktär och komplexitet och övriga omständigheter kan både muntligt och skriftligt uppgiftslämnande komma ifråga.

Brottsbekämpning är en tidskritisk verksamhet och utredningen vill därför framhålla vikten av att stor skyndsamhet i uppgiftslämnandet iakttas. Mellan MSB och Polismyndigheten behöver därför utformas rutiner för att undvika onödig tidsspillan. Utredningen ser dock inte att den föreslagna uppgiftsskyldigheten aktualiserar behov att göra förändringar i MSB:s föreskrifter och rutiner kring incidentrapporteringen i förhållande till rapporterande myndigheter, utan den gällande ordningen med rapportering till MSB inom 24 timmar bedöms rimlig och ändamålsenlig också i förhållande till Polismyndighetens verksamhet och behov.

Utredningen bedömer att antalet rapporterade incidenter kommer vara av en sådan omfattning att informationshanteringen inte förutsätter administrativa åtgärder eller att ytterligare resurser tillförs myndigheterna, utöver de som redan finns vid MSB och Polismyndighetens nationella it-brottscenter.

Jämte att utveckla former för överlämnandet av uppgifter ser utredningen ett behov av att MSB och Polismyndigheten även utvecklar sin samverkan i såväl operativa som strategiska frågor. Diskussioner om en överenskommelse med den inriktningen pågår mellan myndigheterna.

Att polisen får information om en incident där anledning finns att anta att incidenten har sin grund i en brottslig gärning kan beroende på uppgiftens konkretion innebära att polisen i enlighet med bestämmelsen i 9 § polislagen (1984:387) ska upprätta en rapport om detta. Informationen kan också ge polis eller åklagare anledning fatta beslut om att inleda förundersökning.

10 Konsekvenser

Bedömning: Förslaget väntas få positiva konsekvenser för brottsbekämpningen. Förslagets ekonomiska konsekvenser är sådana att eventuellt ökade kostnader hos berörda myndigheter bedöms kunna finansieras inom befintliga ramar.

I kommittéförordningen (1998:1474) och förordningen (2007:1244) om konsekvensutredning vid regelgivning finns bestämmelser om hur konsekvenser av lämnade förslag ska redovisas. I uppdragsbeskrivningen anges därutöver särskilt att utredaren ska analysera och redovisa vilka ekonomiska konsekvenser som förslagen kan komma att medföra och föreslå hur eventuella kostnader för det allmänna ska finansieras.

I promemorian föreslås att en skyldighet införs för Myndigheten för samhällsskydd och beredskap (MSB) att lämna uppgifter om sådana it-incidenter som rapporterats i enlighet med 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap till Polismyndigheten om det finns anledning att anta att incidenten har sin grund i en brottslig gärning.

Förslaget bedöms ha positiva konsekvenser för brottsbekämpningen. Förslaget kommer att leda till en viss ökning av antalet anmälda brott. Fler brott kommer att utredas av polis och åklagare och förutsättningar ges för en ökning av antalet uppklarade brott och för att fler individer lagförs.

Förslaget förväntas medföra en ökad arbetsbelastning för främst Polismyndighetens nationella it-brottscentrum och i någon mån även vid MSB och Åklagarmyndigheten. Även verksamheten vid domstolarna kan påverkas av förslaget. Förslaget berör förhållandevis få medarbetare vid dessa myndigheter och bedöms därför inte för-

anleda några betydande kostnader för utbildningsinsatser eller liknande.

Antalet rapporterade it-incidenter med antagonistisk bakgrund förväntas vara relativt litet i förhållande till berörda verksamheters omfattning i övrigt. Eventuella ökade kostnader till följd av förslaget bedöms för samtliga berörda myndigheter kunna finansieras inom befintliga ramar.

Förslaget föranleder behov av vissa begränsade informationsinsatser från främst MSB:s och Polismyndighetens sida till de statliga myndigheter som är skyldiga att rapportera it-incidenter till MSB. Även dessa insatser bedöms rymmas inom befintliga ramar.

Förslaget gäller överlämnande av uppgifter om it-angrepp mot statliga förvaltningsmyndigheter från en myndighet till en annan. Det är inte fråga om utlämnande av uppgifter om eller till enskilda. Förslaget bedöms därför inte medföra några konsekvenser för den personliga integriteten.

Förslaget bedöms inte medföra några konsekvenser för den kommunala självstyrelsen, sysselsättning och offentlig service i olika delar av landet, små företag, jämställdheten mellan kvinnor och män eller möjligheten att nå de integrationspolitiska målen. Utredningens förslag påverkar inte heller Sveriges åtaganden till följd av medlemskapet i Europeiska unionen.

Utredningens överväganden om tidpunkten för ikraftträdande av förslaget och konsekvenserna därav framgår av kapitel 11.

11 Ikraftträdande

Förslag och bedömning: Förordningen om ändring i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska träda i kraft den 1 januari 2017. Några övergångsbestämmelser behövs inte.

Den föreslagna förordningsändringen innebär att skyldigheten för Myndigheten för samhällsskydd och beredskap att enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap uppmana en myndighet som rapporterar en it-incident att anmäla händelsen till polisen upphör och ersätts med en skyldighet att lämna uppgifter till Polismyndigheten om incidenten. Det är angeläget att den föreslagna ändringen träder i kraft så snart som möjligt. Det bör inte vara nödvändigt med några större praktiska förberedelser som gör att det finns anledning att avvakta med ikraftträdandet. Med beaktande av den tid som behövs för den fortsatta beredningen inom Regeringskansliet bör bestämmelsen kunna träda i kraft den 1 januari 2017. Det är inte nödvändigt med några övergångsbestämmelser.

12 Författningskommentar

12.1 Förslaget till förordning om ändring i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

20 § Till stöd för arbetet med samhällets informationssäkerhet ska en myndighet till Myndigheten för samhällsskydd och beredskap skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapportering enligt första stycket informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.

Rapporteringsskyldigheten omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633).

Om det kan antas att en incident som rapporterats till Myndigheten för samhällsskydd och beredskap enligt första stycket har sin grund i en brottslig gärning, ska Myndigheten för samhällsskydd och beredskap skyndsamt *lämna uppgifter om incidenten till Polismyndigheten.*

I bestämmelsen stadgas en skyldighet för statliga förvaltningsmyndigheter att rapportera vissa it-incidenter till Myndigheten för samhällsskydd och beredskap (MSB).

Första till och med tredje stycket är oförändrade.

Av de skäl som anges i kapitel 9 ändras fjärde stycket på så sätt att skyldigheten för MSB att uppmana en myndighet som lämnat en rapport enligt första stycket att anmäla incidenten till polisen om det kan antas att incidenten har sin grund i en brottslig gärning ersätts med en skyldighet för MSB att i dessa fall lämna uppgifter om incidenten till Polismyndigheten.

Bestämmelsen har utformats så att uppgiftsskyldigheten endast omfattar sådana uppgifter som MSB inhämtat med stöd av denna förordning, och omfattar således inte sådana it-incidenter som andra än statliga förvaltningsmyndigheter frivilligt lämnar till MSB.

Uppgiftsskyldighetens närmare omfattning och innebörd regleras inte i förordningen utan bör utformas i samråd mellan MSB och Polismyndigheten.

Departementsserien 2016

Kronologisk förteckning

1. Kontroller och inspektioner i Sverige av Europeiska byrån för bedrägeribekämpning. Fi.
2. Några frågor om offentlighet och sekretess. Ju.
3. Uppföljning av återvändandedirektivet och direktivet om varaktigt bosatta tredjelandsmedborgares ställning. Ju.
4. Effektivare hyres- och arrendenämnder. Ju.
5. Mer tydlighet och aktivitet i sjuk- och aktivitetsersättningen. S.
6. Entreprenörsansvar och svenska kollektivavtals-villkor vid utstationering. A.
7. Tolktjänst för vardagstolkning. S.
8. Hälsoväxling för aktivare rehabilitering och omställning på arbetsplatserna. S.
9. Ny lag om tilläggsavgift i kollektivtrafik. N.
10. Nya regler för europeiska småmål – lättare att pröva tvister inom EU. Ju.
11. Anpassningar av svensk rätt till EU-förordningen om kliniska läkemedelsprövningar. S.
12. Etisk granskning av klinisk läkemedelsprövning. U.
13. Nya möjligheter till operativt polissamarbete med andra stater. Ju.
14. Förtydliganden av lönestöden för personer med funktionsnedsättning som medför nedsatt arbetsförmåga. Byte av benämningar på lönebidrag, utvecklingsanställning och trygghetsanställning. A.
15. Normgivningen inom åklagarväsendet m.m. Ju.
16. Ersättning vid expropriation av bostäder. Ju.
17. Otillåtna bosättningar. Ju.
18. Ytterligare åtgärder för att genomföra EU-direktiv om mänskliga vävnader och celler. S.
19. Jämställda pensioner? S.
20. Strada. Transportstyrelsens olycksdatabas. N.
21. Ändringar i fråga om sysselsättning för asylsökande och kommunplacering av ensamkommande barn. A.
22. Polisens tillgång till information om vissa it-incidenter. Ju.

Departementsserien 2016

Systematisk förteckning