Helena Andersson

Avdelningen för cybersäkerhet och säkra kommunikationer

010-240 41 33

Konsekvensutredning rörande reviderade föreskrifter och allmänna råd om informationssäkerhet för statliga myndigheter

Allmänt

Beskrivning av problemet och vad man vill uppnå

Svenska myndigheter hanterar idag en mängd information med stor betydelse för en rad olika samhällsfunktioner. Denna information behöver kunna skyddas mot obehörig åtkomst (skydd av informationens konfidentialitet) men behöver även vara tillgänglig för behöriga när den ska användas (skydd för informationens tillgänglighet). I vissa fall är behovet av tillgänglighet så högt att avbrott i praktiken inte är acceptabla. Informationen behöver även skyddas mot obehöriga förändringar (skydd av informationens riktighet). Bristande säkerhet i en myndighets informationshantering kan få både allvarliga och direkta konsekvenser för såväl enskilda och organisationer som samhället i stort.

En tillräcklig säkerhet för myndighetens information uppnås genom att myndigheten på ett systematiskt sätt arbetar med informationsklassning, riskanalys, inför lämpliga säkerhetsåtgärder och följer upp samt utvecklar informationssäkerhetsarbetet. Detta ger sammantaget möjlighet att upprätthålla en lämplig nivå av säkerhet som är anpassad till bland annat verksamhetens behov, rättsliga krav samt identifierade hot och risker. Som stöd för ett sådant systematiskt arbetssätt används standarden för *ledningssystem för informationssäkerhet* ISO/IEC 27001 och 27002 (LIS).

LIS utgår ifrån att det är nödvändigt med en helhetssyn på informationssäkerhet. Skälet till det är att man inte kan åstadkomma god säkerhet utan tydliga interna regler, personella resurser, tekniska och fysiska skyddsåtgärder, personalsäkerhet, administrativa rutiner och uppföljning, d.v.s. samma styrning som komponenter som krävs i vilket annat kvalitetsarbete som helst.

Informationssäkerhetsarbetet hos statliga myndigheter har reglerats i föreskrifter med krav på att det bedrivs systematiskt och riskbaserat med stöd

av ledningssystem sedan 2008.[1] MSB har utfärdat föreskrifter på området 2009 vilka uppdaterades 2016. Även om inte MSB har haft någon tillsynsuppgift har myndigheten genomfört olika typer av kartläggningar över hur statliga myndigheter bedriver sitt informationssäkerhetsarbete och hur de skyddar sin information. [2] Dessa kartläggningar har visat på brister i hur arbetet bedrivs. Även den samlade bilden av statliga myndigheters incidentrapportering indikerar brister hos statliga myndigheter när det gäller säker informationshantering.[3] Skillnaderna mellan myndigheterna bedöms dock vara stora, vissa bedriver redan ett för sin verksamhet väl anpassat systematiskt och riskbaserat informationssäkerhetsarbete medan andra fortfarande är i en utvecklingsfas.

MSB har inte bara främjat ett systematiskt och riskbaserat informationssäkerhetsarbete genom att utfärda föreskrifter utan även tagit fram omfattande stödmaterial samlat på www.informationssäkerhet.se.

Ett systematiskt och riskbaserat informationssäkerhetsarbete ger en organisation genom informationsklassning, riskanalys med mera, möjlighet att välja olika lämpliga säkerhetsåtgärder. Att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete förutsätter tid och resurser. Verksamheten hos statliga myndigheter är av betydelse för samhällets funktionalitet och bedrivs nästan undantagslöst på ett sätt som gör den starkt beroende av it-system. Säkerhetsbrister skapar inte bara problem för myndigheten utan även potentiellt hos den enskilda medborgaren och andra. Utvecklingen inom e-förvaltning och övrig digitalisering i samhället skapar än fler beroenden och kopplingar mellan olika organisationers it-system. För att kunna nyttja digitaliseringens möjligheter blir arbetet med att säkerställa en åtminstone grundläggande nivå av it-säkerhet hos statliga myndigheter allt viktigare och allt mer brådskande.

Regeringen har i den nationella strategin för samhällets informations- och cybersäkerhet pekat på betydelsen av att höja grundnivån av informationssäkerhet. [4] Detta har enligt strategin inte bara betydelse för den

---

[1] Se Verket för förvaltningsutvecklings föreskrifter om statliga myndigheters arbete med säkert elektroniskt informationsutbyte, (VERVAFS 2007:2).

[2] Se exempelvis Myndigheten för samhällsskydds och beredskap, Bevakningsansvariga myndigheters informations- och cybersäkerhet https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/utdrag-bevakningsansvariga-myndigheters-informations-och-cybersakerhet.pdf

[3] Se Myndigheten för samhällsskydd och beredskap, Årsrapport it-incidentrapportering 2018 En sammanställning och analys av de statliga myndigheternas it-incidentrapportering, 2018, https://www.msb.se/RibData/Filer/pdf/28822.pdf

[4] Se Nationell strategi för samhällets informations- och cybersäkerhet https://www.regeringen.se/49f22c/contentassets/3f89e3c77ad74163909c092b1beae15e/nationell-strategi-for-samhallets-informations--och-cybersakerhet-skr.-201617213

enskilda organisationen och samhället i stort utan i förlängningen även ur ett cyberförsvarsperspektiv.

Mot denna bakgrund ser MSB ett behov av ytterligare styrning av statliga myndigheternas informationssäkerhetsarbete. Detta sker genom att både revidera nuvarande föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) och ge ut nya föreskrifter om it-säkerhet för statliga myndigheter. De nya föreskrifterna om it-säkerhet för statliga myndigheter fokuserar på it-relaterad informationshantering och specificerar vilka säkerhetsåtgärder som myndigheten ska göra för att trygga sin digitala miljö. De reviderade föreskrifterna om informationssäkerhet kommer att, som tidigare, att ställa krav på att myndigheterna bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete oavsett om det rör sig om information i digital eller annan form.

Revideringen av föreskrifterna om statliga myndigheters informationssäkerhet innebär att kravet på att nyttja standarderna ISO/IEC 27001 och 27002 förtydligas och referensen uppdateras till de nya utgåvorna av standarderna. Dessutom ställs ett nytt krav på att informationssäkerhetsarbetet ska integreras med myndighetens övriga arbete att leda och styra sin organisation. En annan nyhet är att föreskrifterna nu ställer krav på informationssäkerhetsåtgärder i form av fysisk säkerhet och personalsäkerhet. Tillsammans med de nya föreskrifterna om it-säkerhet för statliga myndigheter innebär det att samtliga huvudtyper av informationssäkerhetsåtgärder; organisatoriska, logiska och fysiska, adresseras. Krav på hur arbetet med uppföljning och utvärdering bedrivs har också lagts till. Övriga förändringar består främst av förtydliganden av nu gällande reglering.

De nya kraven på fysisk säkerhet innebär att myndigheterna ska vidta åtgärder som försvårar obehörigt tillträde till lokaler där information hanteras samt, om det inte är uppenbart onödigt, använda larmsystem. Myndigheten ska dessutom, om inte uppenbart onödigt dela in sina lokaler i fysiskt separerade zoner. Detta kan exempelvis innebära att en särskild besökszon inrättas. Något som enligt MSB särskilt bör uppmärksammas är myndigheters förändrade sätt att hantera information där utkontraktering och mobilitet ofta ställer särskilda krav på utformningen av informationssäkerheten. Utformningen av det fysiska skyddet ska genomgående baseras på resultatet från informationsklassning och riskbedömning och motsvara skyddsvärdet på informationen. Den fysiska säkerheten är som nämnts en central förutsättning för att information ska kunna ges ett adekvat skydd, genom de nya kraven säkerställs även denna aspekt.

En annan nyhet består i krav på personalsäkerhet. Att säkerställa att den personal som hanterar myndighetens information är lämplig för denna uppgift är även det en grundläggande förutsättning för att uppnå adekvat nivå av informationssäkerhet. Kravet uppfylls genom exempelvis referenstagning och intervjuer med de personer som ska hantera en viss typ av information, exempelvis forskningsdata, personuppgifter eller annan information som behöver skydd. Bakgrundskontrollen ger även information om personen har kunskap om och förståelse för ev risker som felaktig hantering kan resultera i

sin tur underlättar vid utformningen av utbildning och kompetensutveckling. Kravet ska inte förväxlas med de krav på registerkontroll som ställs inom ramen för säkerhetsskyddsregleringen.

Utöver krav på fysisk säkerhet och personalsäkerhet har föreskrifterna kompletterats med ytterligare reglering rörande uppföljningen av informationssäkerhetsarbetet och dess resultat. Genom att ställa krav på att åtminstone årligen göra en sammanställning av central information får myndigheten en samlad bild av både hur arbetet bedrivs och underlag för att bedöma vilka brister som behöver åtgärdas. Med hänsyn till myndighetsledningens centrala uppgift att utifrån kunskap om risker och brister i myndighetens informationssäkerhet besluta om förbättringsåtgärder har det även i regleringen tydliggjorts vad ledningen bör informera sig om i sin löpande bedömning av informationssäkerheten.

Beskrivning av alternativa lösningar för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd

Istället för att göra en mer grundlig översyn över föreskrifterna om statliga myndigheters informationssäkerhet (MSBFS 2016:1) skulle regleringsarbetet kunna begränsas till att endast uppdatera hänvisningen till standarderna med referens till de senaste utgåvorna av ISO/IEC 27001 och 27002. Med hänsyn till att MSB även utfärdar nya föreskrifter om it-säkerhet för statliga myndigheter är en sådan lösning mindre lämplig. Det bedöms som centralt att föreskrifterna som ställer krav på hur en myndighet ska bedriva sitt systematiska och riskbaserade informationssäkerhetsarbete i sin helhet och föreskrifterna som reglerar hur säkerheten i it-miljön ska utformas är väl anpassade till varandra. Föreskrifterna om informationssäkerhet och it-säkerhet är tänkta att användas som ett sammanhängande paket tillsammans med föreskrifterna om incidentrapportering för statliga myndigheter. Gemensam terminologi, inbördes referenser och sammanhängande struktur ska underlätta för de myndigheter som ska tillämpa regleringen. Exempelvis är de krav på informationsklassning och riskbedömning som ställs i föreskrifterna om informationssäkerhet centrala ingångsvärden för utformningen av säkerhetsåtgärder i föreskrifterna om it-säkerhet. Det har även setts som fördelaktigt att, där så är lämpligt, harmonisera terminologi och struktur i regleringen för statliga myndigheter med motsvarande reglering av informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8) som utfärdats med stöd av förordning 2018:1175 om informationssäkerhet för samhällsviktiga och digitala tjänster.[5] Sammantaget ger detta ett behov av att se över och revidera språkbruk och upplägg i föreskrifterna om informationssäkerhet för statliga myndigheter. Alternativet

[5] Se även lag 2018:11714 om informationssäkerhet för samhällsviktiga och digitala tjänster samt NIS-direktivet - Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

att endast förändra referensen till standarderna har därför inte bedömts vara ändamålsenligt ur målgruppens perspektiv.

Samtliga nya delar i föreskrifterna, fysisk säkerhet, personalsäkerhet och uppföljning, har det redan tidigare funnits stöd för i form av olika typer av vägledningar, exempelvis i det metodstöd som MSB tillhandahåller på www.informationssäkerhet.se. Det har dock inträffat incidenter som pekat på att brister fortfarande finns inom alla dessa områden. Det handlar om stölder, personer som på bristfälliga grunder har placerats i befattningar med känslig information och myndigheter som på grund av bristande uppföljningsrutiner inte har uppmärksammat behov av att utveckla och uppdatera sin informationssäkerhet. En komplettering på föreslagna områden ligger i linje med standarderna vilka även reglerar dessa frågor. Föreskrifterna blir på detta sätt mer heltäckande. I samband med att kraven på it-säkerhet konkretiseras i de nya föreskrifterna om it-säkerhet behöver även kraven på fysisk säkerhet och personalsäkerhet adresseras för att säkerställa att samtliga typer av säkerhetsåtgärder omhändertas.

Uppgifter om vilka som berörs av regleringen

Föreskrifterna rör sådana säkerhetskrav som avses i 19 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Enligt 3 § andra stycket samma förordning gäller 19 § för samtliga statliga myndigheter under regeringen.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Enligt 19 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap 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. MSB har med stöd av 21 § p 2 samma förordning rätt att utfärda föreskrifter om sådana säkerhetskrav som avses i 19 § med beaktande av nationell och internationell standard.

Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

Idag är det en självklarhet att en myndighet har kostnader för att skydda sin information. I denna kostnad ingår till exempel tekniska skyddsåtgärder i it-system och administrativa kostnader för rutiner samt förvaltning av tekniken. En stor del av utgifterna för informationssäkerhet består av personalkostnader. Utöver kostnader för personal som är särskilt utsedd att samordna och leda säkerhetsarbetet måste även ledningen ägna sig åt säkerhetsfrågor. Dessutom behövs personal som handlägger behörighetsadministration, övervakar brandväggar, uppdaterar virusskydd, följer upp säkerheten, utbildningar, etc.

Det är svårt att på ett normerande sätt ange hur stor del av en verksamhets kostnader som bör läggas på informationssäkerhet. Varje organisation har att förhålla sig till en unik situation när det gäller verksamhet, geografisk och fysisk placering av lokaler, förhållanden till omvärlden m.m. En vanlig modell är att bedöma minskade skadekostnader som resultat av skyddsåtgärder. Exempelvis kan negativa effekter av incidenter av olika slag såsom rättsförluster, störningar i verksamheten, obehörig åtkomst och skada för tredje man i många fall bedömas kostnadsmässigt.

Ett väl genomfört, riskbaserat och systematiskt informationssäkerhetsarbete kan innebära minskade kostnader. Det finns exempel på att organisationer efter informationsklassning och riskbedömning upptäckt att man tillämpat skyddsåtgärder som inte varit relevanta eller helt verkningslösa när det gäller de hot som identifierats, med möjlighet till besparingar som följd.

I förslaget till reviderade föreskrifter skärps, i vissa avseenden, kraven på informationssäkerhetsarbetets utformning. Som nämnt handlar det om krav på fysisk säkerhet, personalsäkerhet och utökad uppföljning av informationssäkerheten. Kraven på fysisk säkerhet kan generera kostnader för larm samt indelning i fysiskt separerade zoner. När det gäller larm torde de flesta myndigheter redan ha en sådan lösning på plats. Den närmare kostnaden för att installera ett larm som är kopplat till en intern eller extern larmcentral kan skilja sig beroende på storlek och utformning. Kostnad för att installera larm hos myndighet där larm helt saknas bedöms minst uppgå till 50 000 kronor. Statliga myndigheter har tillgång till ramavtal för området. Detsamma gäller fysiskt separerade zoner. I det fall myndigheten, baserat på sin informationsklassning och riskbedömning, har identifierat ett behov av separerade zoner som inte redan är omhändertaget kan arbetet bli mer kostnadskrävande. Kraven på personalsäkerhet, det vill säga krav på bakgrundskontroll, bör endast generera begränsade merkostnader eftersom det i stort sett torde ligga i linje med ordinarie rutiner vid anställning och förändring av arbetsuppgifter. Kraven kan kortsiktigt innebära viss kostnadsökning för myndigheterna jämfört med kraven i nuvarande reglering men kan i förlängningen bidra till att minska kostnader för it-incidenter. Det finns flera indikationer på att hoten som riktas mot och riskerna kring myndigheternas informationshantering stadigt ökar, bland annat på grund av den tekniska utvecklingen. Föreskriftsförslaget har som övergripande syfte att ytterligare förbättra stödet för myndigheternas systematiska och effektiva informationssäkerhetsarbete och därmed minska risken för kostnader och förtroendeförluster samt andra konsekvenser orsakade av avbrott, störningar och andra it-incidenter.

Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Föreskrifterna om informationssäkerhet för statliga myndigheter är nationella och bedöms inte påverka de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Det bedöms inte krävas några särskilda hänsyn till tidpunkten för ikraftträdandet. Däremot finns det behov av informationsinsatser som stöd för myndigheternas arbete.

Företag

Beskrivning av antalet företag som berörs, vilka branscher företagen är verksamma i samt storleken på företagen

Föreskrifterna gäller endast statliga myndigheter.

Beskrivning av hur regleringen i andra avseenden kan komma att påverka företagen

Föreskrifterna kan komma att bidra till en mer ensad kravställning på företag som levererar olika typer av it-tjänster.

Kommuner och regioner

Föreskrifterna gäller endast statliga myndigheter.

Kontaktpersoner

Kontaktperson vid frågor om konsekvensutredningen och de nya föreskrifterna om informationssäkerhet för statliga myndigheter är Helena Andersson som lämpligast nås på helena.andersson@msb.se eller 010-240 41 33. Det går också bra att kontakta Tove Wätterstam, på tove.watterstam@msb.se eller 010-240 41 82, alternativt Andreas Häll, på andreas.hall@msb.se eller 010-240 42 13.