Helena Andersson

Avdelningen för cybersäkerhet och säkra kommunikationer

010-240 41 33

Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om it-säkerhet för statliga myndigheter

Allmänt

Beskrivning av problemet och vad man vill uppnå

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.

---

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

[2] Se exempelvis Myndigheten för samhällsskydd 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

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 aktör stöd att ta fram interna regler och arbetssätt för att, genom informationsklassning och riskanalys, få underlag att välja olika lämpliga säkerhetsåtgärder. Att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete förutsätter tid och resurser för analyser och val av säkerhetsåtgärder utifrån myndighetens identifierade behov. Det finns dock en rad säkerhetsåtgärder som i princip är gemensamma och grundläggande för alla organisationer såsom brandväggar, kryptering, behörighetskontroll med mera. Kartläggningarna visar att det även finns brister rörande sådana säkerhetsåtgärder hos myndigheterna, även de bevakningsansvariga myndigheterna. Sådana brister skapar inte bara problem för verksamheten utan även hos andra myndigheter, regioner, länsstyrelser kommuner och företag liksom för den enskilda medborgaren. 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. Utvecklingen inom e-förvaltning och övrig digitalisering i samhället skapar ytterligare beroenden och kopplingar mellan olika organisationers it-system. För att Sverige ska 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 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 genom att förtydliga vad varje myndighet minst behöver göra för att uppnå en godtagbar nivå av säkerhet i sina it-system. Detta görs genom att MSB nu ställer uttryckliga krav på en rad utpekade it-säkerhetsåtgärder som bedöms som vara en del av ett grundskydd för it-miljön. En sådan kravlista bedöms särskilt förenkla för svagare myndigheter att bygga upp en godtagbar nivå av informationssäkerhet. Det är också resurseffektivt att ta fram gemensamma krav. De statliga myndigheter som bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete bedöms redan ha vidtagit de åtgärder som kravställs i föreskrifterna.

Utöver att vidta de grundläggande åtgärderna som specificeras i föreskrifterna åligger det varje myndighet att analysera om de utifrån sin egen verksamhets behov behöver komplettera de föreskrivna åtgärderna med ytterligare

---

[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

säkerhetsåtgärder. De nya föreskrifterna om grundläggande it-säkerhetsåtgärder är inte avsedda att ersätta regleringen om systematiskt informationssäkerhetsarbete. Istället ska de säkerställa att myndigheterna kan uppnå en acceptabel grundnivå av säkerhet i sina it-system. Varje statlig myndighet måste dock alltid bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete som omfattar all informationshantering i myndigheten – oavsett i vilken form.

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

Ett alternativ är att även fortsättningsvis endast reglera det systematiska informationssäkerhetsarbetet och inte ställa några specifika krav på säkerhetsåtgärder. Med hänsyn till de erfarenheter som redovisades ovan, där en sådan reglering har funnits på plats i över tio år liksom att det har funnits en omfattande tillgång till stöd, finner MSB inte att det är tillräckligt. Det finns dessutom en efterfrågan av en tydlig inriktning vad gäller grundnivå för it-säkerhetsåtgärder hos myndigheterna.

En fråga är om motsvarande krav kan tillhandahållas i form av stöd och frivilliga rekommendationer. MSB tar även fram stöd för att införa grundläggande it-säkerhetsåtgärder. MSB gör dock bedömningen att enbart tillgång till en vägledning om grundläggande it-säkerhetsåtgärder inte får samma effekt som ett författningskrav att vidta utpekade it-säkerhetsåtgärder. Att vissa myndigheter har brister i sitt säkerhetsarbete kan inte sällan kopplas till ledningens bristande engagemang i frågorna. Det är just dessa myndigheter som det är viktigast att påverka. Det finns en stor risk att frivilliga säkerhetsåtgärder inte får samma genomslagskraft hos ledningen som bindande reglering. Problematiken har lyfts i många sammanhang av de som arbetar med att samordna och utveckla informationssäkerhetsarbetet i olika organisationer.

Ett annat alternativ är att lägga in krav på it-säkerhetsåtgärder bland nuvarande föreskrifter om statliga myndigheters informationssäkerhet. En uppdelning mellan föreskrifter om systematiskt informationssäkerhetsarbete respektive närmare om specifika säkerhetsåtgärder följer dock samma upplägg som informationssäkerhetsregleringen för leverantörer av samhällsviktiga tjänster. Enligt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster utfärdar MSB föreskrifter om leverantörernas systematiska och riskbaserade informationssäkerhetsarbete och tillsynsmyndigheter samt Socialstyrelsen föreskrifter om säkerhetsåtgärder för respektive sektor. Läggs de nya regleringskraven in i existerande föreskrifter om systematiskt informationssäkerhetsarbete kommer det regelverket bli betydligt mer omfattande och svåröverskådligt. MSB ser därför det som en pedagogisk fördel att skilja på föreskrifter om det övergripande systematiska informationssäkerhetsarbetet och föreskrifter med specifika krav på att vidta it-säkerhetsåtgärder.

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

Flera av paragraferna i de föreslagna föreskrifterna ställer krav på den tekniska miljön och i vissa fall tekniskt stöd för vissa it-säkerhetsåtgärder. Funktionaliteten kan i vissa fall uppnås med både kostnadsfria open source lösningar och kommersiella lösningar. Dessutom kan myndigheter som nyttjar it-resurser hos en annan myndighet eller har utkontrakterat sin it-drift till en extern aktör ofta ha en annan kostnadsbild jämfört med myndigheter som nyttjar egen it-miljö. Till detta kommer att de it-säkerhetsåtgärder som kravställs i föreskrifterna är av den typ som statliga myndigheter, med hänsyn till den verksamhet de bedriver, redan ska ha på plats. Med hänsyn till ovan är det inte möjligt att ge en enhetlig bild av de kostnadsmässiga konsekvenserna som är generellt giltig för alla som berörs av regleringen.

För att ge en så konkret bild som möjligt följer nedan en redogörelse för kostnadsuppskattning för åtgärder som kan komma att kräva anskaffning av tekniskt stöd.

2 kap 3 § inklusive allmänt råd Tekniskt stöd för förteckning över hård- och mjukvara.

Lösningar finns både som open source och som kommersiella produkter. När det gäller hårdvara varierar licenskostnaderna för kommersiella produkter under ett år för cirka 500 enheter mellan 5 000 kr och 100 000 kr. För mjukvara ligger kostnaderna generellt sett lägre. Till detta kommer utbildning av driftpersonal. De flesta myndigheter bedöms redan idag nyttja en teknisk lösning eftersom alternativet att föra en manuell förteckning är tidskrävande. Avsaknad av förteckning över hård- och mjukvara innebär förhöjd risk för att utdaterade eller otillåtna produkter används i myndighetens nätverk.

2 kap 6 § Följa den tekniska utvecklingen

Med detta menas att en funktion aktivt tar del av information som publiceras av t.ex. leverantörer, expertmyndigheter, intresseorganisationer och forskningsområdet rörande aktuella säkerhets- och uppgraderingsversioner, råd kring sårbarheter som ännu inte fått rättningar, publicerade uppdateringar av säkerhetsåtgärder och om hur dessa ska implementeras. Kostnaden för att bedriva sådan omvärldsbevakning består initialt av kostnad för arbetstid för att identifiera de källor som bör användas. Avsaknad av funktionen innebär en förhöjd risk för att kända sårbarheter inte hanteras i myndighetens it-miljö. Att inte ha kunskap om vilka upptäckta sårbarheter eller aktuella hot som finns för den it-miljö organisationen har kan exempelvis resultera i stora dataläckage, vilka kan både vara kostsamt och orsaka förtroendeförluster.

3 kap 5 § Korrekt och tillräcklig dokumentation avseende arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation

Uppdaterad och aktuell dokumentation om hur informationen flödar mellan de olika informationssystemen ska utgöra en del av systemdokumentationen. Dokumentationen kan hanteras på många olika sätt, men bör vara digitaliserad på ett sådant sätt att det ska gå att söka i informationen för att kunna verifiera upptäckta trafikmönster och verifiera övervakad trafik och ev. avvikelser. Det finns både open source och kommersiella lösningar för detta. Kostnaderna varierar för de kommersiella lösningarna. För 100 enheter kan en lösning med server uppgå till 64 000 kr per år och om det handlar om över 500 enheter kan ett datacenter väljas till en kostnad på 120 000 kr per år. Dessutom tillkommer kostnad för utbildning av driftpersonal. Om inte den här funktionaliteten finns på plats kan det finnas oupptäckta kopplingar och dataflöden mellan system vilket kan orsaka dataläckage och att brandväggar inte konfigureras på ett sätt som kan hantera den faktiska it-miljön. Att ha en lista som manuellt uppdateras i exempelvis Excel kan fungera för små organisationer med en möjlighet till överblickbar it-miljö.

3 kap 7 § Separation av testmiljö

Test av konfiguration och integration ska inte göras i produktionsmiljön, eftersom det kan innebära störningar. Ofta genomförs tester med en lägre skyddsnivå än i produktionsmiljön då informationen som hanteras där bedöms ha lägre skyddsbehov. Testmiljön ska därför hållas skild från produktionsmiljön. En testmiljö kan ofta byggas i en virtuell miljö. Kostnaderna för en separat testmiljö består därför av kostnader för hårdvara och licenser för virtualiseringsprogramvaran. Det finns både kostnadsfria och kommersiella lösningar för virtualisering. Kostnaden för hårdvara (server med mycket RAM-minne och stora hårddiskar) kan uppgå till cirka 50 000-75 000 kronor. Kostnaden för licenser blir ungefär 300 000 kr för 100 licenser. Till detta kommer kostnad för utbildning av driftpersonal samt arbetstid för nätverks- och serveradministratörer. Avsaknad av separat testmiljö innebär att tester av genomförda konfigurationer och integrationer måste göras i den myndighetens produktionsmiljö vilket kan orsaka störningar för ordinarie verksamhet.

4 kap 1 -2 §§ Segmentering och filtrering

Segmentering med tillhörande filtrering av trafik kan byggas på många olika sätt, det är vanligt förekommande att trafiken delas in i olika virtuella lokala nätverk (VLAN) och filtreras i en brandvägg. För mer känslig trafik kan till och med fysisk separering (skilda fysiska nätverk med skild nätverksutrustning och kablar) vara lämpligt utifrån myndighetens egen bedömning. Eftersom dagens brandväggar och nätverksutrustningar som används i produktionsmiljö klarar av ett antal VLAN är det inte säkert att någon ny investering behöver göras. Enheter med Windows har också en inbyggd filtrering. I det fall ytterligare filtreringsfunktioner behövs finns tillgång till kostnadsfria open source-lösningar. Kostnaderna för en kommersiell lösning kan uppgå till cirka 50 000 kr för serverhårdvara. Därutöver kan kostnader för utbildning av driftpersonal tillkomma. Segmentering och filtrering hindrar att enheter som blivit angripna eller drabbats av felfunktion fritt kan kommunicera med myndighetens övriga enheter och på så sätt sprida angreppet eller störningen samt att obehöriga hindras från att få åtkomst till nätverket. Konsekvenserna av en sådan spridning och sådan åtkomst kan bli allvarliga.

4 kap 3 § Behörighetshantering och 4 kap 9 § Flerfaktorsautentisering

Den faktiska säkerheten i flerfaktorsautentisering beror på hur den andra autentiseringsfaktorn är utdelad (t.ex. ett smart kort eller lösenordsdosa) och hur legitimationskontrollen/id-kontrollen sker vid utlämnandet. Ett införande av flerfaktorsautentisering (exempelvis i form av krav på både lösenord och smart kort vid autentisering) minskar risken för lösenordsfiske, eller rättare sagt minskar risken att ett fiskat lösenord kan användas. Det finns många lösningar, både open source-lösningar och kommersiella. Att exempelvis använda BankID i systemen ger en initialkostnad på cirka 15 000 kr, en tillkommande månadskostnad, samt en avgift per autentisering på cirka 15 öre. Att installera mjukvaran förutsätter utrymme på en server och dessutom kan kostnader för utbildning av driftspersonal tillkomma. Beroende på hur infrastrukturen för autentiseringen byggs upp samt hur processen för att dela ut exempelvis lösenordsdosor eller kontrollera legitimation utformas kan förvaltningskostnaderna bli förhållandevis höga. Denna kostnad ska dock ses mot minskade kostnader för att hantera glömda lösenord. Vilket i många organisationen tar tid och resurser från annat arbete i it-miljön. Obehöriga som kommer åt lösenord kan använda dessa för att få tillgång till myndighetens it-miljö genom att logga in på användarkonton. Genom att tillämpa flerfaktorsautentisering säkerställs att enbart tillgång till lösenord inte är tillräckligt för att få åtkomst till ett konto utan det krävs även tillgång till den andra faktorn, exempelvis ett smart kort.

4 kap 11 § Lösenord och koder

För att kunna ställa krav på långa och unika lösenord till varje tjänst behöver lösenorden hanteras digitaliserat i skyddade lagringsmiljöer med stöd av lösenordshanterare. Open source-lösningar finns tillgängliga på marknaden liksom kommersiella lösningar. Kostnaden för de sistnämnda kan uppgå till cirka 60 kronor per användare och månad. Mjukvaran kan antingen installeras på egen server, vilket då skapar tilläggskostnader för servern, eller på en server

som redan har andra tjänster installerade. Till detta kommer kostnader för utbildning av driftpersonal. Avsaknad av tekniskt stöd för lösenordshantering gör det svårare att upprätthålla krav på långa och unika lösenord till varje tjänst i myndigheten. Den administrativa kostnaden, tid som behöver avsättas för att manuellt hantera detta är hög. Dessutom har manuell lösenordshantering brister ur säkerhetssynpunkt.

4 kap 14 - 15 § Kryptering och DNSSEC

Lösningar för kryptering finns idag i princip i varje tjänst som installeras. Det finns exempelvis stöd för krypteringslösningen *https* i webbservrar och webbläsare, kryptering av e-post görs genom *S/MIME* i Outlook och funktioner för kryptering av VPN-tunnlar finns i brandväggar. Utöver det kan det finnas ytterligare behov av kryptering exempelvis för lagringsmedier, enskilda filer och lösningar för anställda som distansarbetar. Till krypteringslösningar hör också nyckellagringsutrustning exempelvis Hardware Security Module (HSM), en kryptografisk hårdvarumodul vilken tillhandahåller tekniska och administrativa åtkomstbegränsningar till de digitala nycklarna. HSM:er finns på marknaden från cirka 50 000 och uppåt, det finns inte några open source lösningar tillgängliga. För kryptering av VPN-tunnlar finns både kommersiella och open source-lösningar, både som moduler till brandväggar eller som enskilda produkter. Kryptering är en grundläggande åtgärd för att hindra obehörig åtkomst trygga riktighet och spårbarhet hos informationen. Avsaknad av krypteringslösningar kan få stora konsekvenser för myndighetens informationssäkerhet.

DNSSEC är en särskild krypteringsfunktion som försvårar manipulation av information som trafikerar domännamnssystemet (DNS). För att visa att den DNS-information som är publicerad för organisationen är korrekt så signeras den med tekniken DNSSEC. Dagens DNS-servrar har, eventuellt med något undantag, möjlighet att signera innehållet med DNSSEC. Vid egen drift av DNS-server är investeringskostnaden därför låg men innebär särskilt initialt och därefter årligen kostnader för arbetstid i samband med administration. För organisationer som inte själva handhar sin DNS-server utan köper in tjänsten kan kostnaderna för att aktivera DNSSEC variera. Det finns även leverantörer som inte har möjlighet att aktivera DNSSEC. Avsaknad av DNSSEC innebär en risk för att en angripare till exempel kan dirigera besökare till myndighetens webbtjänster till fel ip-adress.

4 kap 23 § Säkerhetskopiering

Digital data kan lätt förstöras, bli oåtkomlig, korrupt eller raderas. Genom säkerhetskopiering lagras informationen på mer än en plats och ska kunna återläsas. Det finns open source-lösningar för klienter och servrar som stödjer Windows. Det finns även en stor mängd kommersiella lösningar. För produktionsmiljöer som använder virtuell teknik krävs sannolikt kommersiella lösningar för säkerhetskopiering. Det behövs utrustning för att spara säkerhetskopiorna, t.ex. i form av hårddiskar (kostar ca 2000 kronor per hårddisk) eller band. Säkerhetskopiorna behöver även förvaras åtskilt från det som säkerhetskopieras. Detta kan generera investeringskostnader i form av hyra av lokal och utrustning med tillhörande kostnader för lås, larm,

passagekontroll, bevakning, brandlarm osv. För myndigheter som har gjort en bedömning att data kan hanteras i molntjänster är det även möjligt att nyttja sådan tjänst för förvaring av säkerhetskopior. Kostnaden beror på vilka funktioner som väljs. Priset för ett enklare alternativ uppgår till runt 22 öre per GB. Avsaknad av säkerhetskopiering innebär en risk för att information som blir oåtkomlig, korrupt eller raderad inte kan återskapas. Förvaras inte säkerhetskopiorna avskilt från det som säkerhetskopierats riskerar både originalinformation och säkerhetskopierad information att förloras vid exempelvis en brand.

4 kap 26 § Säkerhetsloggning

Säkerhetsloggning innebär att händelser som t.ex. visar åtkomst, försök till åtkomst, behörighetsförändringar, autentiseringar osv registreras och sparas. Även om säkerhetsloggar också kan lagras lokalt behöver de även loggas i en central och skyddad tjänst för att säkerställa möjligheten att göra en effektiv analys av loggarna. Central och skyddad lagring av loggning försvårar för en angripare att radera eller modifiera loggposter för att dölja ett angrepp. Att spara loggar i en central fil kan göras på många sätt. Till säkerhetsloggning hör även arbetet med att analysera de loggar som genererats och på det sättet bygga förmåga att både se en normalbild och större avvikelser. Det finns både open source-lösningar och kommersiella lösningar som stöd för logganalysarbetet. Lösningarna kan installeras på en separat server vilket ger en merkostnad för hårdvara eller på en server som redan används för andra funktioner. Kostnader tillkommer för utbildning av driftpersonal samt, för kommersiella lösningar, även periodiska licenskostnader. Storleken på den administrativa kostnaden för analysarbetet är beroende på hur omfattande analys som myndigheten väljer att göra. Konsekvensen av avsaknad av funktionen innebär risk för att händelser av betydelse för säkerhetsarbetet inte upptäcks eller inte kan analyseras.

4 kap 31 § Skydd mot skadlig kod

Skydd mot skadlig kod, ofta kallad antivirusskydd (AV) består oftast av en klientprogramvara som installeras på klienter och servrar och som scannar alla filer efter misstänkta mönster som tyder på att en kod kan vara skadlig för systemet. Kontroll av skadlig kod kan också ske i s.k. proxys där nätverkstrafiken passerar in i nätverket. Hittas skadlig kod så behöver detta rapporteras, vilket ofta sker genom att AV-klienten kommunicerar med en AV-server som i sin tur larmar en administratör. Att ha skydd mot skadlig kod är att betrakta som grundläggande i en it-miljö. Kostnaderna består i periodiska licenskostnader och utbildning av driftpersonal. Det finns ett flertal leverantörer att välja bland. Avsaknad av skydd innebär att skadlig kod kan spridas i nätverket och infektera enheter.

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

Föreskrifterna om it-säkerhet för statliga myndigheters 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

Ange vem som kan kontaktas vid eventuella frågor

Kontaktperson vid frågor om konsekvensutredningen och de nya föreskrifterna om it-säkerhet för statliga myndigheter Helena Andersson som 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.