Myndigheten för samhällsskydd och beredskap

Årsrapport it-incidentrapportering

2017

Årsrapport it-incidentrapportering

2017

Årsrapport it-incidentrapportering 2017

Myndigheten för samhällsskydd och beredskap (MSB)

Publikationsnummer: MSB1198 - April 2018
ISBN: 978-91-7383-822-1

Innehåll

Inledning

1. Inledning

Från och med den 1 april 2016 ska myndigheter under regeringen, med vissa undantag, till stöd för arbetet med samhällets informations- och cybersäkerhet och i enlighet med 20 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap rapportera vissa it-incidenter till Myndigheten för samhällsskydd och beredskap (MSB).

Enligt 10 a § säkerhetsskyddsförordningen (1996:633) ska myndigheter under vissa omständigheter anmäla en it-incident till den myndighet som enligt 39 § nämnda förordning utövar tillsyn över säkerhetsskyddet. De myndigheter som utövar denna tillsyn är Säkerhetspolisen och Försvarsmakten.

MSB ska enligt 11 a § förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap efter att ha inhämtat uppgifter från Säkerhetspolisen och Försvarsmakten angående de incidenter som rapporterats enligt 10 a § säkerhetsskyddsförordningen lämna en årlig rapport till regeringen avseende it-incidentrapporteringen. Uppgifter från Säkerhetspolisen och Försvarsmakten har inhämtats.

Det övergripande syftet med rapporteringen är att ge MSB bättre förutsättningar att stödja arbetet med, samt stärka, samhällets informations- och cybersäkerhet. MSB arbetar kontinuerligt med att tillvarata den information som inkommer för att på bästa sätt bedriva såväl ett operativt som ett proaktivt arbete gällande statliga myndigheters informations- och cybersäkerhet.

Denna rapport omfattar rapportering avseende incidenter under kalenderåret 2017.

Sammanfattning

2. Sammanfattning

En knapp tredjedel av de rapporteringsskyldiga myndigheterna har under 2017 rapporterat en eller flera allvarliga it-incidenter till MSB. Den låga rapporteringsgraden gör att det inte med säkerhet går att presentera en tydlig bild av de it-incidenter som sker på myndigheterna. Därför stöder inte underlaget fullt ut samhällets informations- och cybersäkerhet på det sätt som är tänkt. 2017 är det första hela kalenderår som denna rapportering har varit igång, detta gör att det är svårt att i detta skede jämföra antalet inkomna rapporter med föregående års rapportering, baserat på antal inkomna rapporter 2016 (april till och med december) är det månatliga genomsnittet likvärdigt[1]. MSB arbetar dock för att öka rapporteringsbenägenheten men bedömer att det kommer att ta ett par år innan systemet fungerar fullt ut. Vissa observationer kan dock lyftas fram.

Den vanligaste typen av incidenter som rapporterats är angrepp följt av störning i mjuk- eller hårdvara. Den vanligaste konsekvensen av de rapporterade incidenterna är hindrande av tillgång till information.

Ett flertal kryptotrojaner rapporterades under början av året. Vid dessa infektioner av it-system har de myndigheter som haft en god ordning på sin it-verksamhet fått mindre störningar än de som inte haft lika bra kontroll över sin it-verksamhet. Detta illustrerar vikten av ett systematiskt informationssäkerhetsarbete, något som är föreskrivit för myndigheter i MSB:s föreskrifter (2016:1). För att underlätta ett systematiskt informationssäkerhetsarbete finns MSB:s metodstöd att tillgå på informationssäkerhet.se.

Ytterligare iakttagelser från årets incidentrapporter är vikten av tydlig kravställning och uppföljning gentemot externt upphandlade leverantörer av tjänster. Denna typ av problematik talar för ytterligare insatser då tjänster upphandlas, detta gäller såväl upphandling av hela system och stora nätverkslösningar som enskilda tjänster av konsulter. Från och med den 1 april 2018 ställs krav på samverkan med Säkerhetspolisen och Försvarsmakten vid utkontraktering av säkerhetskänslig verksamhet, vidare ska Säkerhetspolisen och/eller Försvarsmakten kunna, i de fall de anser upphandlingen inte möter de säkerhetskrav som ställs, besluta att aktuell myndighet inte får fullfölja upphandlingen[2].

För att systemet med it-incidentrapportering ska kunna ge en samlad bild av de allvarliga it-incidenter som drabbar myndigheter behövs en större mängd rapporter från fler myndigheter, då MSB antar att de allvarliga it-incidenter som rapporteras endast utgör en delmängd av det faktiska antalet allvarliga it-incidenter hos svenska myndigheter per år.[3]

1. Det rapporterades 214 allvarliga it-incidenter under nio månader 2016, vilket ger en genomsnittssiffra på 23,8 rapporter per månad, si ffran för 2017 är 281 rapporter vilket genererar en genomsnittssiffra rörande antal rapporter per månad på 23,4.
2. http://www.regeringen.se/4a7e9b/contentassets/952cbf9c95bf4978bd8b51ba1d70333b/pm-utkontraktering-och-overlatelse-av-sakerhetskanslig-verksamhet.pdf
3. Som en jämförelse kan nämnas att det i Estland under kalenderåret 2016 rapporterade 2248 (https://www.ria.ee/public/Kubertur-valisus/RIA_CSA_2017.PDF) it-incidenter. Det är vanskligt att jämföra olika länders it-incidentrapportering då den kan grunda sig i olika föreskrifter och regleringar gällande vad som utgör en it-incident. Baserat på den kunskap som MSB har inom ämnet antas dock att antalet inrapporterade it-incidenter är lågt i förhållande till antalet myndigheter och deras it-beroende.

Allmänt om rapporteringen

3. Allmänt om rapporteringen

Obligatorisk it-incidentrapportering har pågått sedan den 1 april 2016. MSB har under året vidareutvecklat interna processer och rutiner för att ta emot rapporteringen. Det pågår ett arbete med att utveckla formerna för att återföra kunskap från rapporteringen, primärt till de rapporteringsskyldiga myndigheterna, men också till andra samhällsaktörer. Den rapportering som sker enligt 20 § förordning (2015:1052) kommer under 2018 att rapporteras parallellt med den rapportering som sker i enlighet med NIS-direktivets införlivande i svensk lagstiftning, planerat att träda i kraft under 2018. Detta innebär att vissa myndigheter, de som levererar en eller flera samhällsviktiga tjänster, även kommer att träffas av krav att rapportera it-incidenter enligt NIS-direktivet. I och med införandet av NIS-direktivet kommer föreskrifterna för det statliga obligatoriet behöva revideras för att bättre uppfylla det övergripande syftet att stärka samhällets informations- och cybersäkerhet, denna revidering bör genomföras med resultaten från den rapportering som skett. Det finns även en tydlig vinst med att harmonisera rapporteringen för att inte belasta rapporterande aktörer för hårt.

It-incidentrapport-eringen under året

4. It-incidentrapporteringen under året

Av 244 rapporteringsskyldiga myndigheter har 79 myndigheter lämnat it-incidentrapporter till MSB under 2017. 17 myndigheter har rapporterat fem eller fler incidenter. Den myndighet som rapporterat flest har rapporterat 35 incidenter. 30 myndigheter har endast rapporterat en incident, huvuddelen av de incidenterna var av begränsad/okänd eller ej angiven betydelse för verksamhetsviktiga tjänster.

Säkerhetspolisen har lämnat uppgifter till MSB avseende incidentrapportering enligt 10 a § säkerhetsskyddsförordningen för 2017 uppgifterna redovisas i bilaga 1. Försvarsmakten har under 2017 inte fått in några rapporter enligt 10 a § säkerhetsskyddsförordningen.

Sammanlagt har det under 2017 inkommit rapporter om 281 incidenter till MSB. Av dessa har 16 myndigheter angett att de har polisanmält incidenten, denna siffra ska läsas i ljuset av att 78 incidenter har klassats som någon form av angrepp. Rapportflödet har varit ojämnt fördelat över året, flest rapporter inkom under oktober och november med knappt 40 per månad. Under sommarmånaderna samt januari var frekvensen betydligt lägre, knappt 20 rapporter per månad. Nedgången under sommaren kan sannolikt till del förklaras av att färre användare är aktiva i systemen. Vidare har två inkomna incidentrapporter efter granskning visat sig vara sådana som inte är rapporteringspliktiga.

Antalet rapporterande myndigheter har under 2017 varit fortsatt lågt. Det kan finnas olika anledningar till att myndigheter inte har rapporterat någon incident. Myndigheterna har kanske inte varit med om någon it-incident, it-driften kan vara upphandlad innan ikraftträdandet av MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter på ett sätt som inte omfattar incidentrapportering från leverantören, något som enligt 9 § 2 st. nämnda föreskrift undantar it-incidentrapportering. Ytterligare en förklaring kan vara att myndigheterna sätter en hög tröskel för vad de anser vara en allvarlig it-incident, något som gör att incidenter som bör rapporteras inte gör det beroende på olika tolkningar av begreppet allvarlig. Oavsett orsak medför denna låga rapporteringsgrad att det inte skapas någon heltäckande bild av de incidenter som myndigheter råkar ut för och att rapporteringen inte på ett önskvärt sätt bidrar till att höja nivån på samhällets informations- och cybersäkerhet. Bilagt återfinns en förteckning över de myndigheter som inkommit med en eller flera it-incidentrapporter.

För att ge en bättre bild av it-incidenterna som sker hos myndigheterna och därigenom kunna stärka samhällets informations- och cybersäkerhet krävs ett bättre underlag och därmed måste rapporteringsbenägenheten hos myndigheter öka.

4.1 Incidenttyper

De inrapporterade it-incidenterna har efter en sammanvägd bedömning av MSB placerats i en av 10 incidenttyper. Enligt denna bedömning har rapporterna varit fördelade mellan de incidenttyper som framgår av 3 § MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2) enligt nedanstående tabell.

Incidenttyp	Antal (stycken)
Angrepp	78
Störning i mjuk- eller hårdvara	60
Handhavandefel	50
Störning i driftmiljö	45
Oönskade eller oplanerade störningar i kritisk infrastruktur	18
Säkerhetsbrist i en produkt	12
Annan plötslig oförutsedd händelse som lett till skada*	9
Informationsförvanskning	4
Informationsförlust eller informationsläckage	3
Hindrad tillgång till information	2
Totalt	**281**

** Till kategorin kan räknas it-incidenter som orsakats av annan händelse än de som omfattas av kategorierna som nämnts ovan men som av rapporterande myndighet inte bedöms kunna sorteras in i någon av dessa kategorier.*

De mest vanligt förekommande typerna av incidenter är angrepp, följt av störning i mjuk- eller hårdvara. Att incidenter i driftmiljön är vanligt förekommande är i linje med tidigare erfarenheter. Möjligen kan noteras att den relativt höga andelen incidenter kategoriserade som angrepp, vilka omfattar påverkan av en extern aktör, sannolikt beror på att rapporterade incidenter måste ha uppnått en viss allvarlighetsgrad. Det faktum att myndigheterna själva bedömer allvarlighetsgraden i de incidenter som upptäcks gör att incidenter som involverar en extern aktör riskerar att värderas som mer allvarliga än incidenter som härrör inifrån den egna organisationen, detta trots att incidenter med sitt ursprung i exempelvis handhavandefel hos egen personal kan vara lika allvarliga, eller mer allvarliga än incidenter som beror på en extern aktör. Incidenttyperna hindrad tillgång till information, informationsförlust, informationsläckage och informationsförvanskning förekommer i liten utsträckning vid en sammanvägd bedömning. Detta beror på att det oftast är konsekvenser av incidenter av exempelvis typen angrepp eller handhavandefel.

Den vanligaste incidenttypen 2017 var angrepp, vilket utgör cirka 28 % av incidenterna. I angreppskategorin är det skadlig kod, utpressningstrojaner, samt bedrägerier, som dominerar incidenterna inom kategorin. 64 % av de incidenter som beror på angrepp har angett att konsekvensen, det vill säga störningen i verksamhetskritiska tjänster, varit begränsad.

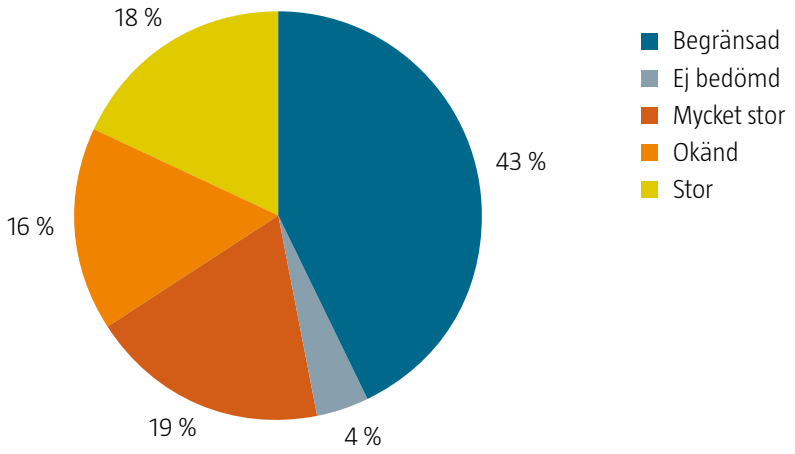
Näst vanligaste incidenttypen är störning i mjuk- eller hårdvara, vilket utgör 21 % av incidenterna. Av dessa har 66 % bedömts resultera i stora, eller mycket stora störningar i verksamhetskritiska tjänster.

Handhavandefel utgör knappt 20 % av de rapporterade incidenterna. Det är noterbart att handhavandefel är relativt frekvent förekommande.

4.2 Störningar i verksamhetskritiska tjänster

I rapporteringen anger myndigheterna om incidenten orsakat någon störning i verksamhetskritiska tjänster. Fördelning av denna bedömning har gjorts enligt nedanstående diagram.

Störning i verksamhetskritiska tjänster



I 20 % av fallen har det inte gjorts någon bedömning eller så har störningens omfattning varit okänd. I 37 % av fallen har incidenten bedömts skapa stor eller mycket stor störning i en verksamhetskritisk tjänst, i hela 80 % av dessa har rapportörerna angett hindrad tillgång till information som en konsekvens av it-incidenten.

I cirka 10 % av de incidenter som har orsakat stor eller mycket stor störning har det angivits att de till del består av någon form av angrepp. Av dessa har merparten i huvudsak varit införsel av skadlig kod, och/eller hindrad tillgång till information. I de fall där störningen ej bedömts, eller angivits som okänd, omfattar 34 % någon form av angrepp.

4.3 Vissa incidenter, brister och iakttagelser

4.3.1 Läckage av personuppgifter

I ett fåtal fall har det rapporterats om läckage av personuppgifter, 12 av 281. Andelen av dessa fall som är klassificerade som angrepp är låg, 2 av 12, den dominerande faktorn bakom läckage av personuppgifter är handhavandefel, 6 av 12 incidenter. Här är det tydligt att kompetenshöjande insatser skulle förbättra informationssäkerheten och skyddet av personuppgifter.

4.3.2 Kryptotrojaner

Kryptotrojaner var fortsatt aktuella under de första två månaderna 2017. Kryptotrojaner fungerar på så sätt att en användare luras att starta en programvara vilken krypterar hela eller delar av användarens lagrings-medium. Krypteringen går vanligtvis att låsa upp om den som råkat ut för låsningen betalar en lösensumma till den som kontrollerar krypterings-programmet, MSB avråder från att under några som helst omständigheter

betala lösensummor för att återfå krypterad information. Under året har ett flertal incidenter innehållit någon form av kryptotrojaner. Av dessa har cirka 45 % lett till informationsförlust. Det är tydligt att graden av informationsförlust, och därmed den negativa konsekvensen av en kryptotrojan är direkt kopplad till myndigheternas rutiner för säkerhetskopiering. Hur ofta säkerhetskopior tas, liksom att den som sköter systemen har rutiner för att hantera de kopior som tas. Huvuddelen av incidenterna med kryptotrojaner har bedömts skapa begränsad störning i verksamhetskritiska tjänster. Alla incidenter med kryptotrojaner ägde rum under årets två första månader och kan sättas i relation till den våg av kryptotrojaner som noterades under senhösten/vintern 2016.

4.3.3 VD/GD-bedrägeri

Ett annat sätt att försöka få ut pengar av en myndighet är att göra så kallade VD/GD-bedrägerier. Dessa bedrägerier genomförs på så sätt att någon via mejl utger sig för att vara en chef som behöver få en snabb utbetalning genomförd. Det förekommer att bedragarna kapar ett e-postkonto för att genomföra dessa bedrägerier. Det har rapporterats elva försök till så kallade vd-bedrägerier under året. Utifrån de rapporterade incidenterna framgår att om det finns rutiner för hur myndigheten genomför legitima utbetalningar, och om dessa följs, minskar risken för att bedrägerierna lyckas.

4.3.4 Överbelastningsattacker

En kategori som uppmärksammats mycket i media är överbelastningsattacker. Från incidentrapporteringen går det att se att cirka 6 %, eller 17 incidenter klassats som attacker genom överbelastning. Antalet incidenter som leder till hindrad tillgång till information är betydligt högre, men i de fallen har det inte föranletts av något angrepp, snarare handhavandefel och/eller störning i mjuk eller hårdvara. Stora ihållande överbelastningar och överbelastningsattacker får ofta stora och påtagliga konsekvenser och uppmärksammas därför i media, baserat på inkomna incidentrapporter är dock antalet överbelastningar som kan härledas till en antagonistisk aktör relativt lågt.

4.3.5 Utkontraktering

Ett antal rapporter visar på att orsaken till incidenten ligger utanför myndighetens kontroll. Dessa incidenter har istället sin upprinnelse i fel hos någon tjänsteleverantör. Incidenterna är av olika karaktär, men cirka hälften av de rapporterade incidenterna som har sitt ursprung hos en extern part kategoriseras av MSB som endera handhavandefel eller angrepp. Andelen incidenter hos externa leverantörer som beror på handhavandefel visar på svårigheten att säkerställa ett metodiskt informationssäkerhetsarbete hos externa leverantörer. I det inkomna materialet går att se hur myndigheter aktivt försöker arbeta för att deras leverantörer ska jobba på ett bättre sätt gällande informationssäkerhet. Denna sårbarhet är viktig att uppmärksamma då den är utom myndigheternas och statens kontroll, även om det finns avtal är dessa i sig inte tillräckliga för att säkerställa funktionalitet. Då verksamhetssystem använder sig av elektroniska kommunikationer vilka köps av en kommersiell aktör förlorar myndigheterna möjligheten att ha full kontroll över systemens funktionalitet. De incidenter som beror på dåligt upphandlade leverantörer antas minskas då Säkerhetspolisens och Försvarsmaktens mandat att ingripa vid upphandlingar som rör skyddsvärda verksamheter stärks den 1 april 2018.

4.3.6 Problem med e-post

Ett antal incidenter involverar e-post hantering och beskriver hur myndigheter efter att anställdas e-post konton hackats och levererat stora mängder spam har blivit svartlistade och fått stora problem med att skicka mail. Denna typ av händelse kan få stora konsekvenser om en myndighet inte kan kontakta och interagera med enskilda via e-post. Detta belyser vikten av att ha en god säkerhetskultur då dessa incidenter uppstått när anställda loggat in via hemdatorer som varit infekterade med skadlig kod som stulit användar- och inloggningsuppgifter.

4.3.7 Hindrad tillgång till information

Av 281 inrapporterade incidenter har 149 (53 %) lett till hindrad tillgång till information[4]. Att hindrad tillgång till information är en vanligt förekommande konsekvens är i linje med övrig erfarenhet på området. Informationssäkerhetsaspekten tillgänglighet är central och kan störas på många olika sätt. Förlorad tillgänglighet är även en noterbar och mätbar effekt för användare. Detta gör att relativt korta avbrott i tillgänglighet noteras, och uppmärksammas. Det kan kontrasteras mot exempelvis informationsförvanskning eller informationsförlust vilket i vissa fall inte upptäcks alls, eller upptäcks långt efter incidenten är ett faktum. Det bör även noteras att syftet med att hindra tillgång till information är just att skapa avbrott som faktiskt märks. I de fall en antagonistisk aktör syftar till att förvanska, stjäla eller på annat sätt kompromettera information ingår det att göra det obemärkt. Denna skillnad speglas även i inkomna incidentrapporter, avbrott, oavsett uppsåt, uppmärksammas och noteras, och rapporteras därmed, i högre grad än incidenter där en antagonistisk aktör medvetet ansträngt sig för att inte lämna spår eller ge sig tillkänna.

4. Detta ska inte förväxlas med noteringen att två incidenter av typen ’hindrad tillgång till information’ redovisats i tabell 1. Den redovisningen avser MSB:s sammanvägda bedömning av de enskilda incidenterna.

Åtgärder för att stärka samhällets informations- och cybersäkerhet

5. Åtgärder för att stärka samhällets informations- och cybersäkerhet

Baserat på de inkomna it-incidentrapporterna går det att göra ett antal observationer avseende områden som kan behöva stärkas för att förbättra myndigheters informations- och cybersäkerhet. Dessa åtgärder baseras till del av de åtgärdsförslag som MSB kommer att redovisa i den kommande Nationella risk och förmågebedömningen (NRFB) som redovisas till regeringen i slutet av april 2018.

Sammanfattningsvis ser MSB stor förbättringspotential hos de myndigheter som omfattas av it-incidentrapporteringen.

Det är samtliga myndigheters ansvar att rapportera de allvarliga it-incidenter som sker i myndigheternas it-miljöer, detta för att syftet med rapporteringen ska kunna uppfyllas. MSB strävar efter att på bästa sätt stödja myndigheterna i deras arbete. Den underrapportering som MSB upplever försvårar arbetet med att stärka samhällets informations- och cybersäkerhet.

Många av de incidenter som rapporteras till MSB är möjliga att med relativt enkla medel förebygga. MSB ämnar att genom dessa råd och de övriga stöd myndigheten tillhandahåller underlätta för statliga myndigheter att bedriva ett systematiskt och effektivt informations- och cybersäkerhetsarbete för att i förlängningen stärka samhällets informations- och cybersäkerhet.

5.1 Systematiskt informationssäkerhetsarbete

Flera av incidenterna pekar på behovet av ett systematiskt arbete med informations- och cybersäkerhet. MSB:s erbjuder ett metodstöd för systematiskt informationssäkerhetsarbete[5] vilket är avsett att underlätta ett sådant arbete. Med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap tillhandahåller MSB föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

5.2 Utbildning/kompetensförsörjning

Viktiga observationer från det begränsade materialet är att det tycks finnas ett fortsatt behov av att höja kompetensnivån avseende information- och cybersäkerhet för flera yrkeskategorier. Detta illustreras av den relativt stora andel incidenter som härrör från någon typ av handhavandefel. Detta ger vid handen att kompetensförsörjningen avseende informations- och cybersäkerhet behöver stärkas. Detta kan ske genom till exempel kompetenshöjande åtgärder, så som internutbildningar, höjning av säkerhetskultur samt att betona informations- och cybersäkerhetskompetens vid framtagande vid rekrytering av personal. MSB erbjuder en snabb och enkel grundutbildning i informationssäkerhet, DISA[6], vilken finns tillgänglig via msb.se.

5. Metodstödet finns tillgängligt för nedladdning via informationssakerhet.se
6. https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/DISA--utbildning-informationssakerhet/

5.3 Utkontraktering/upphandling

Det förekommer ett antal incidenter där problemen ligger hos leverantören av en utkontrakterad tjänst. En bättre kravställning, samt en bättre uppföljning på dessa krav skulle bidra till en ökning av informationssäkerheten i dessa fall. För att stödja aktörer har MSB tagit fram en vägledning med bäring på informationssäkerhet vid upphandling[7], vägledningen revideras och en ny version planerar att släppas under andra kvartalet 2018.

5.4 Ytterligare åtgärder

I kommande rapport NRFB 2018 pekar MSB på ytterligare åtgärder för att stärka samhällets informations- och cybersäkerhet. Två utav de åtgärderna som föreslås är etablerandet av tekniska sensorsystem, samt mandatet att få utöva tillsyn med stöd i de föreskrifter för systematiskt informationssäkerhetsarbete som MSB tillhandahåller. De tekniska sensorsystemen ska användas för att stödja vissa offentliga och enskilda verksamhetsutövare inom samhällsviktig verksamhet, genom att på deras begäran tillhandahålla sensorsystem. Den tilltänkta tillsynen bör utformas på ett sådant sätt att den stödjer aktörerna i deras arbete att åstadkomma ett systematiskt informationssäkerhetsarbete.

7. https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Vagledning--informationssakerhet-i-upphandling/

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1198 - april 2018 ISBN 978-91-7383-822-1