Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2017-03-14	2016-6304-7	

Årsrapport It-incidentrapportering 2016

Innehållsförteckning

1. Inledning 3

2. Sammanfattning 3

3. Allmänt om rapporteringen 4

4. It-incidentrapporteringen under året 4

4.1 Incidentkategorier 5

4.2 Störningar i verksamhetskritiska tjänster 6

4.3 Vissa incidenter och brister 7

Bilaga med sekretessbelagda uppgifter:
Vissa särskilda företeelser avseende it-incidentrapporteringen

1. Inledning

Från och med den 1 april 2016 ska myndigheter under regeringen, med vissa undantag, till stöd för arbetet med samhällets informationssäkerhet 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. De tre myndigheterna har under 2016 haft en löpande samverkan för att skapa goda förutsättningar för rapporteringen till regeringen. Uppgifter från Säkerhetspolisen och Försvarsmakten har inhämtats.

2. Sammanfattning

En knapp tredjedel av de rapporteringsskyldiga myndigheterna har under 2016 rapporterat en eller flera it-incidenter till MSB. Huruvida detta är ett rimligt utfall är svårt att ta ställning till efter ett knappt år av rapportering. Bedömningen är dock att det som rapporterats inte ligger i paritet med faktiska antalet allvarliga it-incidenter. Detta är ett av MSB förväntat utfall. MSB arbetar 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.

De vanligaste incidentkategorierna är *störning i driftmiljö* och *angrepp*. Den vanligaste konsekvensen av de rapporterade incidenterna är *hindrande av tillgång till information*.

Ett flertal kryptotrojaner har rapporterats under året. Bland de som har drabbats av infektioner i 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. Under året har det även rapporterats ett flertal så kallade vd-bedrägerier. I de fall det har funnits goda betalningsrutiner på plats, och dessa har följts, så har bedrägeriförsöken inte varit framgångsrika.

För att systemet med it-incidentrapportering ska kunna ge en samlad bild av de allvarliga it-incidenter som drabbar myndigheter behövs en större volym rapporter från fler myndigheter.

3. Allmänt om rapporteringen

Obligatorisk it-incidentrapportering har pågått sedan den 1 april 2016. Denna rapport omfattar rapportering avseende incidenter från detta datum till och med den 31 december 2016. MSB har under året utvecklat sina interna processer och rutiner för att ta emot rapporteringen. Det pågår ett arbete med att etablera formerna för att återföra kunskap från rapporteringen, primärt till de rapporteringsskyldiga myndigheterna.

4. It-incidentrapporteringen under året

Av 244 rapporteringsskyldiga myndigheter har 77 myndigheter lämnat it-incidentrapporter till MSB under 2016. Åtta myndigheter har rapporterat fem eller fler incidenter. Den myndighet som rapporterat flest har rapporterat 20 incidenter. Trettionio myndigheter har endast rapporterat en incident. Huvuddelen av dessa incidenter var av begränsad/okänd eller ej angiven betydelse för verksamhetsviktiga tjänster.

Säkerhetspolisen har under 2016 fått in tre it-incidentrapporter enligt 10 a § säkerhetsskyddsförordningen. Försvarsmakten har inga uppgifter avseende rapporterade incidenter att lämna då de under 2016 inte fått in några formella rapporter enligt 10 a § säkerhetsskyddsförordningen.

Sammanlagt har det under 2016 inkommit 214 incidentrapporter. Av dessa har 12 incidenter polisanmälts. Rapportflödet har varit relativt jämnt med runt 25 rapporter i månaden, bortsett från sommarmånaderna juli och augusti där antalet gick ner. Nedgången kan sannolikt till del förklaras av att färre användare är aktiva i systemen och att det sker mindre drift- och utvecklingsåtgärder i it-miljöer under sommaren.

Antalet rapporterande myndigheter bedöms under 2016 varit 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 Myndigheten för samhällsskydd och beredskaps 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. Myndigheterna sätter en hög tröskel för vad de anser vara en allvarlig it-incident. Oavsett orsak medför detta att det finns begränsningar i vilka övergripande slutsattser som kan dras av hur drabbade myndigheter är av it-incidenter efter detta första knappa år av rapportering.

Enligt 4 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter ska varje myndighet rapportera en it-incident senast 24 timmar efter det att myndigheten upptäckt den rapporteringspliktiga incidenten. I de allmänna råden till de nämnda

föreskrifterna framgår att myndigheten anses ha upptäckt it-incidenten när information om den hanteras i utpekad intern process för hantering av it-incidenter eller när säkerhetsansvarig eller motsvarande fått kännedom om incidenten. Vid genomgång av rapporterna visar det sig att runt 20 procent av incidenterna rapporterats mer än fem dagar efter att de upptäckts, vissa incidenter har rapporterats först efter en månad. Tiden från upptäckt till rapport kan variera beroende på rutiner, vilken dag i veckan den upptäcks eller när det går att fastställa att det är en allvarlig incident. Vad som är en rimlig rapporteringstid varierar från fall till fall. Det går att överväga om kortare ledtider för rapporteringen på sikt kan innebära att incidentrapporteringen blir mer användbar.

4.1 Incidentkategorier

Vid rapportering av en it-incident går det att ange flera incidentkategorier för varje rapport. Till exempel kan en störning i driftmiljön orsakas av ett angrepp och således kan både kategorin för störning i driftsmiljön och kategorin för angrepp anges vid rapportering.

Rapporterade incidenter har av den mottagande myndigheten bedömts huvudsakligen tillhöra en kategori. Enligt denna bedömning har rapporterna varit fördelade mellan de incidentkategorier som framgår av 3 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2) enligt nedanstående tabell.

Incidentkategori	**Antal (stycken)**
Störning i mjuk- eller hårdvara	38
Störning i driftmiljö	66
Informationsförlust eller informationsläckage	11
Informationsförvanskning	0
Hindrad tillgång till information	5
Säkerhetsbrist i en produkt	2
Angrepp	66
Handhavandefel	17
Oönskade eller oplanerade störningar i kritisk infrastruktur	9
Annan plötslig oförutsedd händelse som lett till skada	0
Totalt	214

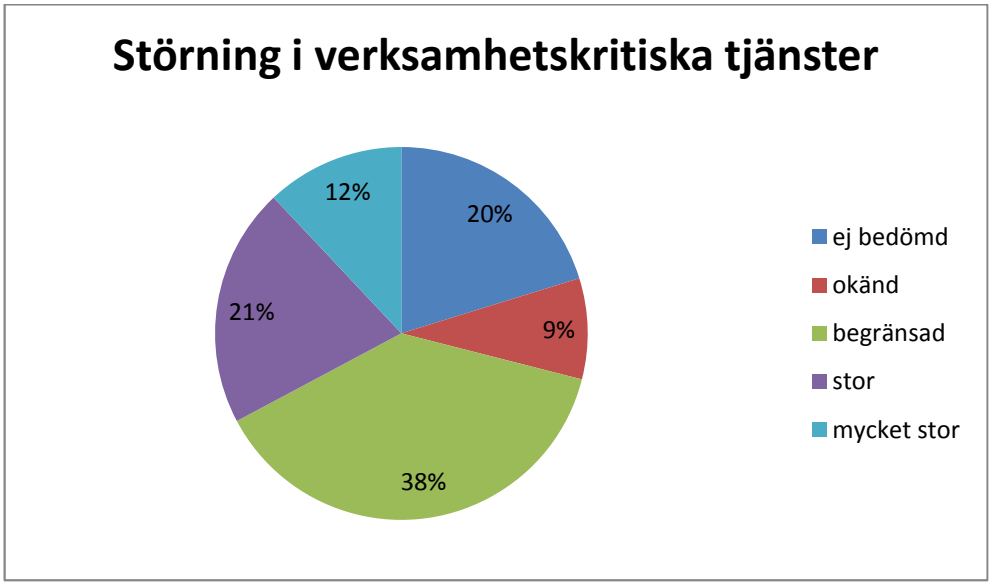
De mest vanligt förekommande typerna av incidenter är *störning i driftmiljö* och *angrepp* följt av *störning i mjuk- eller hårdvara*. Att incidenter i driftmiljön dominerar är i linje med tidigare erfarenheter. Möjligen kan noteras att andelen incidenter kategoriserade som angrepp, vilka omfattar påverkan av en extern aktör, sannolikt är relativt hög beroende på de incidenter som rapporteras måste ha uppnått en viss allvarlighetsgrad.

Vid en undersökning av vilka kategorier som angetts i rapporterna är den vanligaste förekommande incidentkategorin störning i driftmiljö, vilket har angivits i cirka 45 procent av rapporterna. Den näst vanligaste incidentkategorin är angrepp vilket har angivits i 39 procent av rapporterna. Detta följs av *hindrad tillgång till information*, *handhavandefel* och *störning i mjukvara*, alla tre anges i ungefär 20 procent av rapporterna. Det är noterbart att *handhavandefel* är relativt frekvent förekommande. Det tyder på att kompetenshöjande åtgärder kan ge positiv effekt på informationssäkerheten.

Hindrad tillgång till information är den vanligaste angivna konsekvensorienterade kategorin. Ungefär hälften av de incidenter som involverat hindrad tillgång till information har även kategoriserats som angrepp eller handhavandefel. Att hindrad tillgång till information är en vanligt förekommande kategori är i linje med övrig erfarenhet på området. Informationssäkerhetsaspekten tillgänglighet är en central aspekt vilken kan störas på många olika sätt.

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.



I cirka 30 procent av fallen har det inte gjorts någon bedömning eller så har störningens omfattning varit okänd. I 33 procent av fallen har incidenten bedömts skapa stor eller mycket stor störning i en verksamhetskritisk tjänst.

I cirka 40 procent av fallen med stora eller mycket stora störningar i verksamhetskritiska tjänster har det handlat om hindrande av tillgång till information. Ungefär 70 procent av fallen har inneburit störningar i driftsmiljön. I cirka 10 procent 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 tillgänglighetsattacker. I de fall där störningen inte angivits, eller angivits som okänd, omfattar 40 procent någon form av angrepp. Detta ligger i linje med att det är incidenter som beror på den egna organisationen eller tekniska problem som skapar de största informationssäkerhetsproblemen.

4.3 Vissa incidenter och brister

I ett fåtal fall har det rapporterats om läckage av personuppgifter. I huvuddelen av dessa skedde läckaget efter angrepp från utomstående.

Huvuddelen av de incidenter i vilka det har rapporterats informationsförlust har involverat kryptotrojaner. Kryptotrojaner fungerar på så sätt att en användare luras att starta en programvara vilken krypterar hela eller delar av användarens lagringsmedium. Krypteringen går vanligtvis att låsa upp om den som råkat ut för låsningen betalar en lösensumma till den som kontrollerar krypteringsprogrammet. Under året har ett flertal incidenter innehållit någon form av kryptotrojaner. Av dessa har cirka 40 procent lett till informationsförlust. Det är tydligt att graden av informationsförlust, och därmed den skadliga konsekvensen av en kryptotrojan, är direkt kopplad till myndigheternas rutiner för säkerhetskopiering. Viktiga aspekter är 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 av rapporterande myndighet bedömts skapa begränsade störningar i verksamhetskritiska tjänster. Antalet incidenter med kryptotrojaner ökade mot slutet av året vilket sannolikt förklaras av att det under den tiden pågick en stor kampanj riktad mot svenska aktörer vilken använde sig av mejl som utgav sig komma från PostNord.

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

Från incidentrapporteringen framkommer en bild av att det finns brister i loggningen av it-system. I ett antal incidenter har det framkommit att myndigheter inte har någon dedikerad loggserver, något som är en viktig komponent för att kunna upprätthålla en fungerande övervakning av it-system och för att i efterhand ha möjlighet att klargöra vad som hänt i systemet.

Ett antal rapporter visar på att orsaken till incidenten ligger utanför myndighetens kontroll. Incidenterna har istället sin upprinnelse i fel hos någon tjänsteleverantör. Inte sällan rör det sig om att kommunikationer och därmed verksamhetens ledningssystem slås ut. Denna sårbarhet är viktig att uppmärksamma då den är utom myndigheternas och statens kontroll. Även om

det finns kontrakt är dessa i sig inte tillräckliga för att säkerställa funktionalitet. Då verksamhetssystem använder sig av elektroniska kommunikationer vilka upphandlas från en kommersiell aktör har myndigheterna inte möjlighet att ha full kontroll över systemens funktionalitet.