Verksamheten för samhällets informations- och cybersäkerhet
Enheten för operativ cybersäkerhet och it-incidenthantering, CERT-SE

Exempel på it-incidenter

Typexempel inklusive bedömning

Innehållsförteckning

1. Inledning

Från och med april 2016 är statliga myndigheter skyldiga att rapportera it-incidenter som allvarligt kan påverka säkerheten i myndighetens informationshantering. Syftet med regleringen är att stödja samhällets informationssäkerhet och bland annat förbättra lägesbilden samt öka förutsättningar att avvärja och begränsa konsekvenserna av allvarligare typer av it-incidenter. I MSB:s föreskrifter om obligatorisk it-incidentrapportering för statliga myndigheter (MSBFS 2016:2) tydliggörs när, hur och vilka kategorier av it-incidenter som ska rapporteras.

Varje myndighet ska göra sin egen bedömning av vilka it-incidenter som är så allvarliga att de ska rapporteras och vilka it-incidenter som inte uppfyller kriterierna för att vara rapporteringspliktiga. En sådan bedömning är dock inte alltid enkel att göra.

Flera myndigheter har uttryckt en önskan om stöd vad gäller bedömningen av it-incidenter. Det kommer dock att ta en tid innan de första myndighetsgemensamma lärdomarna och erfarenheterna kommer att kunna sammanställas. MSB har dock valt att redan från början tillhandahålla stöd och bistå genom att tillhandahålla en förteckning över ett antal typexempel på it-incidenter som MSB bedömer vara rapporteringspliktiga respektive inte rapporteringspliktiga.

I föreskrifterna MSBFS 2016:2 om obligatorisk it-incidentrapportering för statliga myndigheter anges tio kategorier inom vilka it-incidenter kan rapporteras. Exemplen nedan presenteras inom ramen för dessa kategorier. Det bör noteras att exemplen som beskrivs endast är typexempel och att de inte ska ses som en uttömmande beskrivning eller begränsning av de olika kategorierna. Exemplen ska inte heller ses som bindande råd i någon juridisk mening utan varje myndighet har, som ovan nämnts, ansvar för att göra sin egen bedömning.

2. Kategorier

De kategorier som anges i föreskrifterna MSBFS 2016:2 används som indelning av exemplen på it-incidenter:

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 föreskrifterna kan en inrapporterande myndighet ange en eller flera kategorier för att beskriva en it-incident. Det är möjligt, och sannolikt, att inrapporterande myndighet kategoriserar en it-incident enligt en viss kategori, men att exempeltexten även stämmer överens med en annan kategori. Detta kommer att uppstå pga. att it-incidenter kan betraktas på många olika sätt, beroende på ett antal olika faktorer. En myndighet väljer kanske att främst se en it-incident som en störning i driftmiljö samtidigt som it-incidenten medför informationsförlust. I dessa fall är det lämpligt att ange båda kategorierna vid rapportering.

2.1 Störning i mjuk- eller hårdvara

En störning i mjuk- eller hårdvara innefattar fel i system, komponenter eller programvara. Det inkluderar felaktigheter i sk firmware. Hit hör också oväntad funktionalitet i ett system (t ex att ett system skickar information till annat ställe än det är avsett att göra). Även systemkrascher räknas hit, oavsett om systemkraschen gäller en applikation eller ett operativsystem.

En felaktighet (bugg) gör att en nattlig uppdatering går fel. Flera servrar som hanterar verksamhetssystem är otillgängliga under påföljande dag.

Exempel a)

De verksamhetssystem som är otillgängliga under påföljande dag är ekonomisystem och påverkar inte de tjänster som myndigheten erbjuder till medborgare och organisationer, utan är huvudsakligen en intern olägenhet. Ingen informationsförlust görs.
Bedömning: rapporteras inte

Exempel b)

De verksamhetssystem som är otillgängliga hanterar e-tjänster där medborgare dagligen hämtar eller lämnar information. Myndigheten får flera klagomål om tjänstens otillgänglighet.
Bedömning: ska rapporteras

Exempel c)

Den drabbade myndigheten anser sig ha hittat ett allvarligt fel i uppdateringen (mjukvarupaket) och vill sprida informationen till andra myndigheter som kan tänkas drabbas av samma olägenhet i samma programvara.
Bedömning: ska rapporteras

Ett hårdvarufel i ett lagringsnät (SAN, NAS e dyl) drabbar myndigheten. Flera databaser kraschar. Hårdvaran tar två timmar att reparera, men databaserna beräknas ta flera arbetsdagar att återbygga och få tillgängliga igen.

Exempel a)

Hårdvarukraschen orsakas av en ren olyckshändelse. Inga data förloras, men myndighetens databaser beräknas inte kunna nås på en arbetsvecka vilket påverkar myndighetens verksamhet på ett sätt som inte kan ses som lindrigt. Det påverkar även andra myndigheters verksamhet pga beroende till databaserna.
Bedömning: ska rapporteras

Exempel b)

Hårdvarukraschen orsakas av ett handhavandefel (någon spillde en kopp kaffe på fel ställe), men inget data förloras. Myndighetens databaser beräknas inte kunna nås på flera dagar, men informationen i databaserna är inte kritisk för myndighetens verksamhet och inte heller för andra som använder den, även om det är omständligt att klara sig utan verksamhetsstödet.
Bedömning: rapporteras inte

2.2 Störning i driftmiljö

En störning i en driftmiljö kan exempelvis bestå av haveri i ett tekniskt system eller en komponent i infrastrukturen. Det kan också vara förlust av tillgänglighet i system. Hit räknas också störningar i system med säkerhetsfunktioner, t ex säkerhetskopiering, loggningssystem o dyl.

En molntjänst som myndigheten använder sig av upphör att fungera. Ett antal verksamhetssystem blir otillgängliga under flera dagar.

Exempel a)

Molntjänsten används uteslutande för interna stödsystem som inte innehåller kritiska verksamhetsdata. Myndighetens verksamhetsarbete fortgår som normalt, men medarbetare kan inte rapportera in tid och ekonomiavdelningens arbete kan inte göras under tiden tjänsten är otillgänglig. Störningen märks inte för medborgare, men den märks tydligt för de handläggare som behöver stöd med att boka eller hantera nödvändiga resor för verksamheten. Viss privatekonomisk påverkan förekommer, då reseräkningar inte kommer in i tid för lönekörningar och utbetalning av utlägg blir förskjuten en månad till medarbetare.
Bedömning: rapporteras inte

Exempel b)

Molntjänsten används för olika verksamhetssystem och tjänstebortfallet sker vid en intensiv period för myndigheten och får därför allvarlig påverkan på myndighetens verksamhet.
Bedömning: ska rapporteras

Telefoniväxeln hos en statlig myndighet upphör att fungera under en vardagsförmiddag.

Det kan vara svårt att bedöma om telefoni-incidenter ska räknas som it-incident eller inte. Moderna telefoniväxlar är ofta IP-baserade, men det kan vara värdefullt att verifiera om det är en IP-baserad telefoniväxel som myndigheten använder eller inte. Om informationen inte finns tillgänglig bör telefoniväxeln bedömas som att den är IP-baserad.

Exempel a)

Myndigheten är otillgänglig via telefon en hel förmiddag och inga manuella rutiner för den trasiga telefonifunktionen finns. Flera medborgare kan inte nå sina myndighetshandläggare via telefonväxeln, utan måste ringa på

mobiltelefonnummer där så är möjligt. Myndigheten har inte en IP-baserad telefoniväxel.
Bedömning: rapporteras inte

Exempel b)

Myndigheten är otillgänglig via telefon en hel förmiddag. Manuella rutiner kopplar om inkommande samtal till en automatisk talsvarsfunktion där de hänvisas till information på webbplatsen för myndigheten samt att använda mobiltelefonnummer där så är möjligt. Myndigheten har en IP-baserad telefoniväxel.
Bedömning: rapporteras inte

Exempel c)

Myndigheten är otillgänglig via telefon under hela förmiddagen, utan möjlighet att informera inkommande samtal om att ett systemfel just nu förekommer. Det är osäkert vad felet består i och när det kommer att kunna avhjälpas. Myndigheten har en IP-baserad telefoniväxel.
Bedömning: ska rapporteras

Kontorsnätet på en myndighet slutar fungera en sen eftermiddag. Felet verkar bero på en trasig komponent i infrastrukturen (router eller switch).

Exempel a)

Interna system som e-post, intranät och lagringsareor för dokument kan inte kommas åt på myndigheten. Handläggare kan fortfarande arbeta på sina lokala datorer och telefoni är inte påverkad. Ingen extern störning förekommer. Ingen information förloras.
Bedömning: rapporteras inte

Exempel b)

Alla interna system är nere och handläggare kan inte logga in på sina lokala datorer, eftersom de servrar som hanterar inloggning på nätet är otillgängliga. Telefoni är inte påverkad. Ingen extern störning förekommer, men handläggare är oroliga för att de inte kan svara på e-post som förväntat. Ingen information förloras.
Bedömning: rapporteras inte

Exempel c)

Alla interna system är nere och handläggare kan inte logga in på sina lokala datorer, eftersom de servrar som hanterar inloggning på nätet är otillgängliga.

Telefoni är inte påverkad. Pga att felet upprepas och nätet störts ut ett upprepat antal gånger under de kommande dagarna påverkas myndighetens verksamhet allt mer genom att förseningar i handläggning av ärenden uppkommer. Vid felsökning hos tjänsteleverantören hittar man inte problemet utan felsökning fortsätter.
Bedömning: ska rapporteras

2.3 Informationsförlust eller informationsläckage

Tillgänglighetsförluster kan vara permanenta eller temporära. Exempelvis är en informationsförlust orsakad av brand i serverhall ofta permanent, medan systemfel eller en omfattande överbelastningsattack kan leda till temporär tillgänglighetsförlust. Kategorin förlust av tillgänglighet till, eller läckage av information i myndighetens informationssystem, kan inkludera felaktig avyttring av teknisk utrustning som innehåller information som inte ska vara allmänt tillgänglig, eller otillåtet offentliggörande av sådan information. Informationsläckage innebär att myndighetens information inte gått förlorad men att någon på obehörigt sätt skaffat sig tillgång till den.

Vid informationsläckage kan det vara svårt att bedöma hur stor spridning informationen fått eller om läckaget inneburit att aktören som skaffat sig tillgång till informationen behållit den för eget bruk. Osäkerhet kring hur stor spridning informationen fått bör beaktas vid bedömningen av hur allvarlig incidenten är.

Personuppgifter kommer på avvägar och publiceras på internet, inklusive sekretessmarkerade uppgifter.

Exempel a)

Personuppgifter i ringa mängd har läckt ut via en skadlig kod som finns på en intern server. Bland de uppgifter som har läckt ut innehåller några få sekretessmarkerade uppgifter. Informationen hittas nu på flera forum på internet.
Bedömning: ska rapporteras

Exempel b)

En stor mängd personuppgifter har läckt ut, men det är okänt hur läckaget gick till. Informationen hittas nu på flera forum på internet. Informationen innehåller enstaka sekretessmarkerade uppgifter.
Bedömning: ska rapporteras

Exempel c)

En begränsad mängd personuppgifter har läckt ut via e-post som en handläggare har skickat där fel fil inkluderades av misstag. Informationen har väldigt liten spridning och endast enstaka sekretessmarkerade uppgifter finns med.
Bedömning: rapporteras inte

Myndigheten upptäcker att personuppgifter är oavsiktligt tillgängliga via speciellt utformade anrop på myndighetens webbplats.

Exempel a)

En it-tekniker på myndigheten upptäcker av en händelse att det går att använda felaktiga anrop till en extern webbtjänst som myndigheten har. Anropen går att anpassa så att personuppgifter kan tas fram om man vet hur och vad man letar efter. Efter kontroll av loggar och driftinformation kan myndigheten inte se att någon information har läckt ut, men bedömer att detta inte kan garanteras.
Bedömning: ska rapporteras

Exempel b)

En extern konsult informerar myndigheten om att det, enligt information på ett populärt internetforum, går att hämta personuppgifter via deras webbtjänst, även utan abonnemang och rättigheter. Vid kontroll kan myndigheten konstatera att ett antal försök att komma åt personuppgifter har gjorts och det kan också konstateras att vid ett tiotal tillfällen har personuppgifter kunnat hämtas ut (en och en) felaktigt.
Bedömning: ska rapporteras

2.4 Informationsförvanskning eller hindrad tillgång till information

Förvanskning av information kan leda till att informationen helt eller delvis har blivit korrumperad eller att det inte går att säkerställa dess riktighet.

Hindrad tillgång till information kan exempelvis innebära att informationen eller ett system där informationen finns inte kan användas på avsett sätt.

Myndigheten upptäcker, via loggar, att ett vilande konto plötsligt används för fjärraccess.

Exempel a)

Myndighetskontot har omfattande tillgång till myndighetens uppgifter inom ett eller flera verksamhetssystem, men det går inte att fastställa om någon information har förändrats eller läckt ut. Man kan konstatera att inloggning har skett ett antal gånger.
Bedömning: ska rapporteras

Exempel b)

Myndighetskontot har endast tillgång till en övningsdator som använts med externa parter och därtill tillhörande tjänster, huvudsakligen åtkomst till en övningswebbplats samt övnings-e-post. Ingen övrig access finns. Ingen ytterligare inloggning har skett, men man kan konstatera att kontot har använts för inloggning ett antal gånger.
Bedömning: rapporteras inte

Ett rootkit upptäcks i en dator på det interna myndighetsnätet.

Exempel a)

En dator på myndighetens kontorsnät uppför sig underligt och när it-avdelningen får i uppgift att åtgärda den konstateras att den har någon typ av skadlig kod installerad. Vid närmare kontroll visar det sig vara ett s.k. root-kit. Man hittar inga indikationer på att root-kitet har gjort något alls, vare sig i den lokala datorn eller i övrig infrastruktur på myndigheten.
Bedömning: ska rapporteras

Exempel b)

En server på myndighet skickar ut oväntad trafik, vilket ses i bland annat andra servrars loggar. När it-avdelningen får i uppgift att åtgärda den konstateras att

den har någon typ av skadlig kod installerad. Vid närmare kontroll visar det sig vara ett s.k. root-kit. Det finns indikationer på att detta har använts för att försöka ta sig in på både lokala konton på servern, men också på andra konton och servrar på nätverket. En utredning startas upp för att kunna bedöma vad som egentligen har hänt.
Bedömning: ska rapporteras

Inloggningssidan till myndighetens webbportal för andra myndigheter blockeras genom en överbelastningsattack.

Överbelastningsattacker ska alltid rapporteras om de medför någon typ av märkbar störning på myndighetens infrastruktur eller tjänster. Om överbelastningsattacken däremot avstyrs av t ex ett DDoS-skydd från internetleverantören på ett sådant sätt att en märkbar störning aldrig uppstår, så ska attacken inte rapporteras annat än om den har ett repeterande mönster, t ex tre eller fler gånger på ett dygn eller repetitivt en viss vardag i veckan alternativt en viss dag i månaden.

Exempel a)

Under eftermiddagen en tisdag drabbas myndigheten av en överbelastningsattack (DDoS) som gör att myndighetens webbportal för tjänster som erbjuds andra myndigheter svarar endast sporadiskt. Webbportalen är svår att nå under knappt en timme, innan överbelastningsattacken slutar och funktionaliteten återställs utan ytterligare åtgärder från myndighetens sida.
Bedömning: ska rapporteras

Exempel b)

Under eftermiddagen en tisdag drabbas myndigheten av en omfattande överbelastningsattack (DDoS) som gör att myndighetens webbportal för tjänster som erbjuds andra myndigheter inte går att nå på över två timmar, innan överbelastningsattacken ebbar av och normal funktionalitet återställs utan ytterligare åtgärder från myndighetens sida. En timme senare återkommer attacken med förnyad kraft och slår återigen ut webbportalen i nästan två timmar till och under efterföljande dygn kommer ytterligare en attack med samma resultat.
Bedömning: ska rapporteras

2.5 Säkerhetsbrist i en produkt

Kategorin kan exempelvis innefatta it-incidenter orsakade av säkerhetsluckor eller annan sårbarhet i tekniskt hjälpmedel som används av myndigheten.

En extern part från okänt ställe nyttjar, med hjälp av ett färdigt verktyg, en sårbarhet som är okänd för myndigheten eller som inte har hunnit åtgärdas i myndighetens utrustning.

Exempel a)

En it-tekniker upptäcker att någon, via internet, har tagit sig in på en dator som myndigheten använder som gäst- och surfdator i sin reception. Datorn har inte hunnit uppdateras korrekt med patchar och det verkar som att detta har utnyttjats för att kunna ta sig in på datorn. Endast en skrivare och tillgång till internet finns på den dator som har angripits.
Bedömning: rapporteras inte

Exempel b)

En it-tekniker upptäcker att någon, via internet, har tagit sig in på en extern brandvägg som hör till myndigheten. Konfigurationen i brandväggen verkar vara förändrad och myndigheten känner att de inte vågar lite på skyddsfunktionen innan brandväggen har gåtts igenom och verifierats av egen personal.
Bedömning: ska rapporteras

Exempel c)

En kommunikatör på myndigheten hittar information på internet som indikerar att en wifi-anslutningspunkt hos myndigheten saknar lösenord och kan användas fritt av vem som helst som är inom räckhåll för anslutningspunkten. Incidenten rapporteras till it-driften, som konstaterar att det är korrekt, någon har kommit åt och ändrat inställningarna för wifi-anslutningspunkten. Inga loggar verkar finnas för anslutningen.
Bedömning: ska rapporteras

2.6 Angrepp

Det kan ofta vara svårt att i ett initialt skede avgöra varifrån ett angrepp kommer eller om det faktiskt rör sig om ett angrepp. Till den här kategorin räknas exempelvis överbelastningsattacker, införande av skadlig kod, intrång i informationssystem (s.k. hackning), olovligt nyttjande eller annat missbruk av lösenord, olovlig åtkomst till information genom skadliga program och obehörig användning av informationssystem.

Som angrepp räknas även angrepp som möjliggjorts eller genomförts av egen personal eller personer som på motsvarande sätt har en anknytning till den drabbade myndigheten, exempelvis inhyrd personal.

Myndighetens webbplats blir oåtkomlig under 3 timmar på grund av en riktad överbelastningsattack.

Överbelastningsattacker ska alltid rapporteras om de medför någon typ av märkbar störning på myndighetens infrastruktur eller tjänster. Om överbelastningsattacken däremot avstyrs av t ex ett DDoS-skydd från internetleverantören på ett sådant sätt att en märkbar störning aldrig uppstår, så ska attacken inte rapporteras annat än om den har ett repeterande mönster, t ex tre eller fler gånger på ett dygn eller repetitivt en viss vardag i veckan alternativt en viss dag i månaden.

Exempel a)

Överbelastningsattacken pågår i 1 timme, men endast myndighetens allmänna informationsplats på webben påverkas. E-post levereras långsamt, men kommer fram.
Bedömning: ska rapporteras

Exempel b)

Överbelastningsattacken pågår i 3 timmar och slår ut i princip allt som myndigheten har mot internet, webbplats, e-postservrar, DNS-funktionalitet m m. på grund av detta kommer ingen e-post in under drygt 3 timmar och handläggare på myndigheten blir försenade i sitt arbete eftersom attacken omöjliggör för handläggare att hämta information från andra webbplatser på nätet.
Bedömning: ska rapporteras

Via e-post inkommer ett dokument med länk och uppmaning att slå på makron i Microsoft Word, skadlig kod finns inbäddad i dokumentets makron.

Exempel a)

Handläggare på myndigheten får e-post som innehåller en faktura. Inkluderat i detta är ett dokument som heter ”faktura.xdoc”. När dokumentet öppnas av en handläggare uppmanas denne att slå på makron i Microsoft Word för att kunna läsa innehållet i dokumentet. Samtidigt varnar handläggarens antivirus-system att något är skadligt i dokumentet.

Handläggaren låter antivirussystemet hantera dokumentet och slår inte på makron, utan avslutar och tar bort e-postmeddelandet.
Bedömning: rapporteras inte

Exempel b)

Ett stort antal chefer på myndigheten får e-post som uppmanar dem att följa länken och ladda hem information om ett intressant kursupplägg för team-building för personalen. Länken verkar underlig med ett konstigt domännamn och om man följer den laddas en pdf-fil ner. Flera av cheferna vidarebefordrar e-posten till it-avdelningen som konstaterar att det verkar röra sig om något som är speciellt riktat mot myndighetenschefer.
Bedömning: ska rapporteras

Exempel c)

En handläggare på myndigheten får e-post som till synes kommer från en annan myndighet som man löpande har kommunikation med. Inkluderat i e-posten är ett dokument som ser legitimt ut. När dokumentet öppnas av handläggaren så händer inget konstigt, utan det innehåller relevant information. Samtidigt genereras en varning hos myndighetens säkerhetsövervakning att en icke godkänd VPN-tunnel öppnas mot en okänd IP-adress utanför myndigheten.
Bedömning: ska rapporteras

Repeterade misslyckade inloggningsförsök sker mot admin-konton på myndigheten.

Exempel a)

Vid en rutinkontroll på loggar upptäcks några misslyckade inloggningsförsök mot ett admin-konto på myndighetens nätverk (Microsoft AD). Inloggningsförsöken görs inom en mycket kort tidsram och återkommer inte senare.
Bedömning: rapporteras inte

Exempel b)

Vid en rutinkontroll av loggar på myndigheten upptäcks sporadiska misslyckade inloggningsförsök mot ett admin-konto utsträckt under en period på några veckor mot myndighetens nätverk (Microsoft AD). Inloggningsförsöken kommer igen med några försök i princip dagligen och kan inte härledas till automatiska funktioner som gör något, utan verkar göras av någon som försöker komma åt admin-kontot, men inte har rätt information och behörighet.
Bedömning: ska rapporteras

Exempel c)

En person på myndighetens systemövervakningsavdelning upptäcker pågående, repeterade försök att komma åt inloggning i databaser på myndighetens nätverk. Inloggningsförsöken görs mot standard-kontonamn för funktionerna och de är repeterade och misslyckade. När kontroll görs mot tidigare loggar märks att den här typen av inloggningsförsök har pågått under en viss tid.
Bedömning: ska rapporteras

En anställd på myndigheten kopierar databas med inloggningsuppgifter och lägger ut denna på en publik sajt.

Exempel a)

En anställd på myndigheten kopierar några få poster ur en databas. Informationen är inloggningsuppgifter till en webbtjänst som är online. Informationen läggs upp på en publik sajt där många kan ta del av den.
Bedömning: ska rapporteras

Exempel b)

En anställd på myndigheten kopierar hela egna avdelningens telefonlista, inklusive inloggningsinformation och lägger upp den på Dropbox för enkel åtkomst hemifrån för egen användning.
Bedömning: ska rapporteras

Exempel c)

En anställt på myndigheten kopierar en hel användardatabas, inklusive namn, e-postadress och krypterade lösenord, och lägger ut den som en ”databasdump” på en publik sajt på nätet.
Bedömning: ska rapporteras

En anställd på myndigheten raderar eller förändrar information i ett av myndighetens verksamhetssystem.

Exempel a)

En anställd på myndigheten raderar information i ett av myndighetens verksamhetssystem av rent misstag och utan någon som helst misstanke om att den anställde medvetet försökt förstöra något finns. Informationen kan återställas med backuprutiner.
Bedömning: rapporteras inte

Exempel b)

En anställd på myndigheten förändrar medvetet väsentlig information i ett verksamhetssystem innan hen slutar. Konsekvenserna av detta är att när detta upptäcks så uppstår en osäkerhet i riktigheten i de ärenden som myndigheten har handlagt sedan den anställde slutade. Bedömning: ska rapporteras

Myndighetens twitterkonto eller facebook-konto har hackats och används för att sprida desinformation.

Exempel a)

En sen fredag upptäcker en kommunikatör på myndigheten att deras twitterkonto publicerat felaktig information och konstiga bilder med länkar till okända webbsidor. Ingen på kommunikationsenheten har gjort detta och när de försöker logga in på twitterkontot så fungerar deras normala lösenord inte.
Bedömning: ska rapporteras

Exempel b)

Myndigheten upptäcker att det finns en facebook-sida som har samma namn som myndigheten, så när som på en liten felskrivning i namnet i form av två omkastade bokstäver. Den felaktiga sidan används för att sprida desinformation och oönskade inlägg med politisk karaktär.
Bedömning: ska rapporteras

Datorer hos myndigheten drabbas av ransomware (utpressningstrojan), som krypterar filer och gör dessa omöjliga att använda. För att låsa upp filerna avkrävs myndigheten en lösensumma.

Samtliga fall av ransomware (utpressningstrojan) där myndigheten riskerar att förlora data ska rapporteras.

Exempel a)

Fem datorer hos handläggare på myndigheten drabbas av en utpressningstrojan/ ransomware som krypterar alla filer på datorn och sedan begär en lösensumma. Den skadliga koden begränsas till dessa fem datorer som samtliga har aktuella backuper. Inga data försvinner, men återläsningstiden för backuperna och ominstallation av datorerna är totalt ungefär 2 arbetsdagar.
Bedömning: rapporteras inte

Exempel b)

Fem datorer hos handläggare på olika enheter på myndigheten drabbas av en utpressningstrojan/ ransomware som krypterar alla filer på datorn och sedan begär en lösensumma. Förutom att kryptera de lokala datorerna krypteras även nätverksanslutna diskenheter, några usb-minnen som satt i datorerna samt en externt ansluten lokal hårddisk som användes för att säkerhetskopiera stora bildfiler. Data försvinner eftersom det inte går att återställa allt som krypterades.
Bedömning: ska rapporteras

Domännamnet till myndigheten kapas och trafiken styrs till en falsk sida som liknar myndighetens.

Samtliga fall av domäner som kapas, registreras som ett snarlikt myndighetsnamn eller likande och som sprider falsk information i en myndighets namn ska rapporteras.

2.7 Handhavandefel

Kategorin omfattar exempelvis it-incidenter som orsakas av internt felaktigt bruk eller felaktig implementering av tekniskt system eller komponent.

Konsulter installerar en ftp-server i ett DMZ av brandväggen för att underlätta sitt arbete. Interna dokument samt mp3-filer blir tillgängliga från internet.

Exempel a)

Enligt myndighetens it-policy tillåts uppsättning av temporära tjänster i myndighetens testmiljö. Ftp-servern som sattes upp är i en dedikerad testmiljö och den är korrekt rapporterad och godkänd av driftansvarig för miljön. De interna dokument som ligger på ftp-servern är arbetsmaterial för dokumentationen till ett pågående projekt. Inloggning till ftp-servern skyddas av användarkonto och lösenord. Brandväggsöppningen som gör ftp-servern tillgänglig från internet är inte godkänd. Det är okänt om andra än konsulterna kommit åt informationen på ftp-servern.
Bedömning: rapporteras inte

Exempel b)

Myndighetens it-policy har ingen information om huruvida servrar med filtjänster är godkända eller inte på DMZ mot internet. It-avdelningen har inte godkänt ftp-servern, utan den är uppsatt helt utan kännedom från personal på myndigheten.
Bedömning: ska rapporteras

En bärbar dator med personuppgiftsregister glöms kvar på bussen och försvinner.

Exempel a)

Den bärbara datorn har diskkryptering aktiverad. Datorns innehåll är skyddat, även om någon försöker starta upp datorn och komma åt informationen. Inga data kan läcka ut.
Bedömning: rapporteras inte

Exempel b)

Den bärbara datorn har inte diskkryptering aktiverad och skyddas enbart av användarnamn och lösenord. Datorns innehåll kan teoretiskt kommas åt av en tekniskt kompetent person. Dataläckage befaras.

Bedömning: ska rapporteras

Stora mängder känslig information skickas på felaktigt sätt okrypterat via e-post eller på annat sätt över internet.

Exempel a)

En myndighet arbetar med en stor utredning om hur krisberedskapen inom myndighetens ansvarsområde ska förbättras och där delar av arbetsmaterialet bedöms omfattas av offentlighets och sekretesslagen. En handläggare skickar arbetsmaterialet, okrypterat, till sitt privata e-postkonto för att kunna arbeta vidare med det på ett enkelt sätt under helgen, för att hinna klart med sin del i tid.
Bedömning: ska rapporteras

Exempel b)

En it-tekniker på myndigheten letar efter felaktigheter i konfigurationsfiler till ett routerkluster. För att få assistans och andras åsikter visar it-teknikern konfigurationsfilen som en textmassa på en chat-sajt där många nätverkstekniker brukar vara och prata.
Bedömning: ska rapporteras

2.8 Oönskad eller oplanerad störning i kritisk infrastruktur

Funktionen hos myndighetens informationssystem är ofta starkt beroende av tillgång till extern försörjning av el och kommunikationstjänster, men även interna system för att trygga funktionen i kritisk infrastruktur. Till kategorin bör därför räknas it-incidenter som orsakas av exempelvis elektriskt fel, vattenskada eller störning i funktioner för avbrottsfri kraftförsörjning, kylning eller ventilation.

Översvämning drabbar myndighetens datahall, som ligger intill ett vattendrag.

Exempel a)

En tidig vårmorgon går ett fuktlarm från myndighetens datahall. När ansvariga tekniker kommer till datahallen konstaterar de att det är vatten under datagolvet i hallen och arbete inleds omgående för att sanera och hantera med hjälp av den firma som ansvarar för underhåll av hallen. Under tiden fortsätter driften att fungera utan störningar.
Bedömning: rapporteras inte

Exempel b)

En tidig vårmorgon går ett fuktlarm från myndighetens datahall. När ansvariga tekniker kommer till datahallen konstatera de att det är vatten över hela golvet, även på golvet i racken som har servrar och annat monterat. Ett antal lågt hängande elfördelningsdosor är också i farozonen för vattnet som fortsätter att stiga. Pga detta väljer de ansvariga att nödstoppa hallen för att åtgärda vattnet på golvet utan att riskera kortslutning och annat. Myndighetens verksamhet påverkas påtagligt under ett antal dagar.
Bedömning: ska rapporteras

Kommunikationsavbrott mot identifieringstjänst gör att myndighetens inloggningar slutar fungera.

Exempel a)

Myndigheten använder Microsoft AD för att logga in till sitt nätverk. Inloggningarna till de lokala datorerna och till serverfunktioner slutar fungera när ett kommunikationsavbrott - en trasig router - gör att klienter och servrar inte når AD-servern för att verifiera inloggningar. Problemet fortgår under knappt en timme. Endast interna störningar uppstår.
Bedömning: rapporteras inte

Exempel b)

Myndighetens externa webbportal använder elektroniska identiteter för att medborgare ska kunna logga in på webbportalen och titta på samt förändra sin information. Pga ett okänt kommunikationsfel fungerar inte inloggningen och det är svårt att bedöma när den kommer att börja fungera igen. Flertalet privatpersoner börjar höra av sig och frågar om när felet är åtgärdat.
Bedömning: ska rapporteras

Ett blixtnedslag skapar en spik i kraftförsörjningen till myndighetens serverhall och orsakar drifthaveri för myndighetens e-tjänst under sex timmar.

Exempel a)

Strömspiken i kraftförsörjningen slår ut ett serverkluster som inte skyddas av UPS-er på fredag eftermiddag. Elaggregaten till serverklustret förstörs och måste ersättas av reservdelar. Det serverkluster som berörs omfattar några av de e-tjänster som ska fungera dygnet runt (H24/365). Det externa service-avtalet är skrivet på ett sådant sätt att stöd inte kan ges under helgen utan först nästkommande vardag.
Bedömning: ska rapporteras

Exempel b)

Strömspiken i kraftförsörjningen slår ut ett UPS-par och orsakar en mindre brand i en myndighetens datahall. Branden släcks snabbt av släckningssystemet. I samband med detta behöver sanering i datahallen göras och bland annat en serverrack i datahallen behöver stängas av tills el-kopplingen är verifierad för användning igen. Under tiden väljer ansvariga

tekniker att aktivera de standby-servrar som finns för e-tjänsten, men trots detta är e-tjänsten otillgänglig i flera timmar.
Bedömning: ska rapporteras

Luftkonditioneringsanläggningen i myndighetens serverhall går sönder och orsakar driftstörningar i två timmar.

Exempel a)

En lördagmorgon går ett driftlarm om värme från myndighetens datahall. När larmet kontrolleras konstateras att luftkonditioneringen i serverhallen har slutat fungera och måste repareras. Under tiden ökar temperaturen gradvis i serverhallen och ansvariga tekniker väljer att, med godkännande från it-avdelningen, stänga ner flera servrar som genererar värme. Servrarna väljs noggrant för att störa driften så lite som möjligt. Efter två timmar är allt uppe i normal drift igen. Mycket små interna störningar uppstår.
Bedömning: rapporteras inte

Exempel b)

En vardagseftermiddag går ett driftlarm om värme från myndighetens datahall. När larmet kontrolleras konstateras att luftkonditioneringen i serverhallen har slutat fungera och måste repareras. Under tiden ökar temperaturen gradvis i serverhallen och ansvariga tekniker väljer att, med godkännande från it-avdelningen, stänga ner flera servrar som genererar värme. Servrarna väljs noggrant för att störa driften så lite som möjligt. Efter två timmar är allt uppe i normal drift igen. Men som en följd av avbrottet uppstår en mängd störningar vilket inkluderar myndighetens externa e-postsystem och vissa interna verksamhetssystem som påverkar myndighetens ärendehantering.
Bedömning: ska rapporteras

Den enda bredbandsförbindelsen till myndigheten blir avgrävd och skapar totalt bortfall av internet och fast telefoni för myndigheten och dess tjänster.

Exempel a)

Vid myndighetens kontor pågår grävningsarbete för nya fiberanslutningar för bredband. Under grävningsarbetet grävs den befintliga kopplingen av och myndighetens koppling till internet samt telefoni slutar fungera helt. Endast mobiltelefoner fungerar in till myndigheten. Ingen reservplats finns för

webbsidan och myndigheten har inget bra sätt att förmedla information om händelsen samt alternativa kontaktvägar.
Bedömning: ska rapporteras

Exempel b)

Vid myndighetens kontor pågår grävningsarbete och under arbetet grävs den befintliga kopplingen av och myndighetens koppling till internet samt telefoni slutar fungera helt. Endast mobiltelefoner fungerar in till myndigheten. Myndigheten har en reservplats för sin webbsida hos en internetleverantör och väldigt fort dirigeras sidan om till reservplatsen, vilket minimerar störningarna för medborgare och andra. På sin webbsida och på sin facebook-sida publicerar myndigheten information om händelsen och anger alternativa kontaktvägar för att nå myndigheten under störningstiden.
Bedömning: rapporteras inte

Kabelbrand i tunnel skapar avbrott i myndighetens privata direktförbindelser.

Exempel a)

En större kabelbrand i en tunnel påverkar myndighetens internetkopplingar. Myndighetens e-tjänster ligger hos service-leverantörer och påverkas inte, men handläggarens möjlighet att arbeta på resande fot eller hemifrån (via VPN, privata direktförbindelser) försvinner. Handläggare måste istället arbeta från kontoret som enda möjlighet under de dagar det tar att åtgärda kabelbranden.
Bedömning: rapporteras inte

2.9 Annan plötslig oförutsedd händelse som leder till skada

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

Exempel a)

Beställda reservdelar till myndighetens infrastruktur är restnoterade från leverantören och nödvändig leverans försenas. Inga incidenter händer under leveranstiden, men it-avdelningen flaggade detta till ledningen som en risk.
Bedömning: rapporteras inte

Exempel b)

Beställda reservdelar till myndighetens infrastruktur är restnoterade från leverantören och nödvändig leverans försenas. Under leveranstiden är delar av kritisk infrastruktur inte redundant och pga detta så uppstår också en driftstörning när en del av den icke-redundanta infrastrukturen inte klarar av att hantera nödvändig trafik på nätverket och behöver startas om för att fungera. Efter omstart uppstår samma problem igen och ny omstart måste göras.
Bedömning: ska rapporteras