Anvisningar för NIS 2-incidentanmälan

Innehåll

1 Inledning

Syftet med detta dokument är att med hjälp av ett exempelfall ge organisationer råd om hur man gör incidentanmälningar enligt cybersäkerhetslagen, och när det gäller den offentliga förvaltningen hur man gör anmälningar enligt informationshanteringslagen och hur man fyller i de tillhörande anmälningsblanketterna.

Namn, adresser och andra specificerande uppgifter som förekommer i detta dokument har skapats som exempel och de situationer som beskrivs i dem är inte avsedda att vara direkt användbara för en NIS2-aktör. Exemplen i bilderna och texterna i detta dokument åskådliggör därmed endast eventuella scenarier som eventuellt kan förekomma i incidentanmälningar enligt cybersäkerhetslagen och informationshanteringslagen.

Enligt artikel 23 i NIS2-direktivet ska organisationer som omfattas av direktivet underrätta den behöriga tillsynsmyndigheten om betydande incidenter i de tjänster som de tillhandahåller. Anmälningsskyldigheten har tre nivåer och består av en första anmälan, en uppföljande anmälan och en slutrapport. Vid långvariga incidenter eller på begäran av myndigheten ska organisationerna dessutom lämna en delrapport om incidenten.

Skyldigheten att anmäla en betydande incident till tillsynsmyndigheten och vad anmälningarna ska innehålla regleras i 11–13 § i cybersäkerhetslagen. Bestämmelser om frivillig underrättelse finns dessutom i 15 §. I fråga om organisationer inom den offentliga förvaltningen föreskrivs om anmälningsskyldigheten och innehållet i anmälningarna i 18 d § i informationshanteringslagen. Bestämmelser om frivillig underrättelse finns dessutom i 18 f § i informationshanteringslagen.

Enligt 11 § 2 mom. i cybersäkerhetslagen avses med en betydande incident en incident som har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller betydande ekonomiska förluster för den berörda aktören, samt en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. En betydande incident har fastställts för myndigheterna i 2 § 24 punkten i informationshanteringslagen. Dessutom tillämpas kommissionens genomförandeförordning 2024/2690 för vissa organisationer. Förordningen innehåller kompletterande bestämmelser, bland annat om definitionen av en betydande incident.

Den första anmälan ska lämnas in inom 24 timmar från det att den betydande incidenten upptäcktes och den uppföljande anmälan inom 72 timmar från upptäckten av den betydande incidenten. En delrapport ska lämnas på begäran av tillsynsmyndigheten eller vid en långvarig incident senast en månad efter det att den uppföljande anmälan har lämnats in. Slutrapporten om en incident ska ges inom en månad från det att den uppföljande anmälan lämnades eller, om det är fråga om en långvarig incident, inom en månad från det att hanteringen av incidenten avslutades. Den frivilliga underrättelsen gäller andra än betydande incidenter samt cyberhot och tillbud. Vid en frivillig underrättelse lämnas ingen separat uppföljande anmälan eller slutrapport.

I denna anvisning behandlas endast anmälningar som görs i enlighet med cybersäkerhetslagen. Övrig reglering kan ålägga vissa aktörer att dessutom anmäla incidenterna även på andra sätt. Dessa anvisningar är inte juridiskt bindande och i eventuella oklara situationer har lagstiftningen alltid företräde i förhållande till det som konstateras i denna anvisning.

2 NIS2-applikation för anmälningar

I det här avsnittet går vi igenom fem olika typer av anmälningar. De första fyra typerna av anmälningar beskrivs i kronologisk ordning och till sist beskrivs den frivilliga underrättelsen som en separat helhet.

Observera att fält som förekommer upprepade gånger på blanketterna, till exempel kontaktuppgifter, eventuella brottsanmälningar eller anmälningar till andra myndigheter (dataombudsmannens byrå) samt CSIRT-tilläggsblanketter endast beskrivs en gång vid sidan av den första anmälan. Dessa poster upprepas flera gånger på blanketterna, så ni kan vid behov återgå till anvisningarna för dessa återkommande fält i avsnitt 2.1.

2.1 Första anmälan

Den första anmälan om en betydande incident inleds genom att fylla i uppgifter om organisationens sektor i fälten enligt Bild 1.

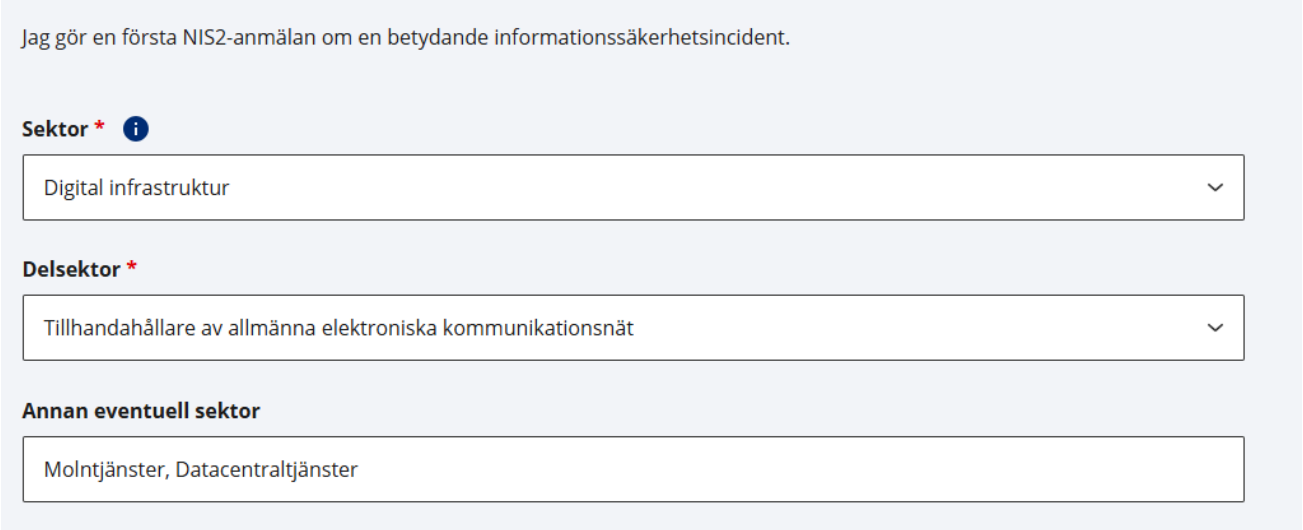

Bild 1 Fält för sektor

Vid valet av organisationens sektor används den huvudsakliga sektorn som omfattas av NIS2-regleringen. Detta val kan till exempel göras genom att jämföra omsättningarnas storlek för organisationens olika sektorer och välja den största av dem.

I punkten "annan eventuell sektor" kan ni lägga till de sektorer där er organisation är verksam utöver den ovan nämnda "huvudsakliga sektorn". Som ett praktiskt exempel kan en organisation vars huvudsakliga sektor är televerksamhet lägga till exempelvis datacentraltjänster för andra sektorer, om ovan nämnda företag erbjuder sådana tjänster separat till sina kundföretag.

När ni har fyllt i uppgifterna om er organisations sektorer kan ni fylla i fälten för de allmänna uppgifterna om incidenten, som beskrivs på bild 2.

Bild 2 Allmän information

I beskrivningsfältet för händelsen antecknas en allmän beskrivning av händelsen i ljuset av den information som finns tillgänglig när anmälan görs, en bedömning av dess eventuella konsekvenser samt en eventuell beskrivning av händelseförloppet för incidenten. När den första anmälan görs är det också möjligt att ovan nämnda uppgifter ännu inte har kunnat preciseras, varvid ni kan fylla i beskrivningsfältet enligt uppgifterna vid tidpunkten för anmälan.

I det ovan nämnda fältet kan ni också beskriva konsekvensens omfattning i er organisations verksamhet. I referensfallet beskrivs ett fall där hela organisationens servermiljö har krypterats till följd av en incident, men där man inte har identifierat någon påverkan på till exempel säkerhetskopior av tjänstens data.

Följaktligen kan det medföljande fältet även användas för att begränsa konsekvensbedömningen för fallet, om ni har konstaterat att incidenten exempelvis endast påverkar en enskild tjänst i er organisation. I fråga om den nämnda tjänsten kan ni också beskriva om det är fråga om en affärskritisk tjänst och/eller ett affärskritiskt system eller om det till exempel är fråga om ett system som används för att upprätthålla intern dokumentation.

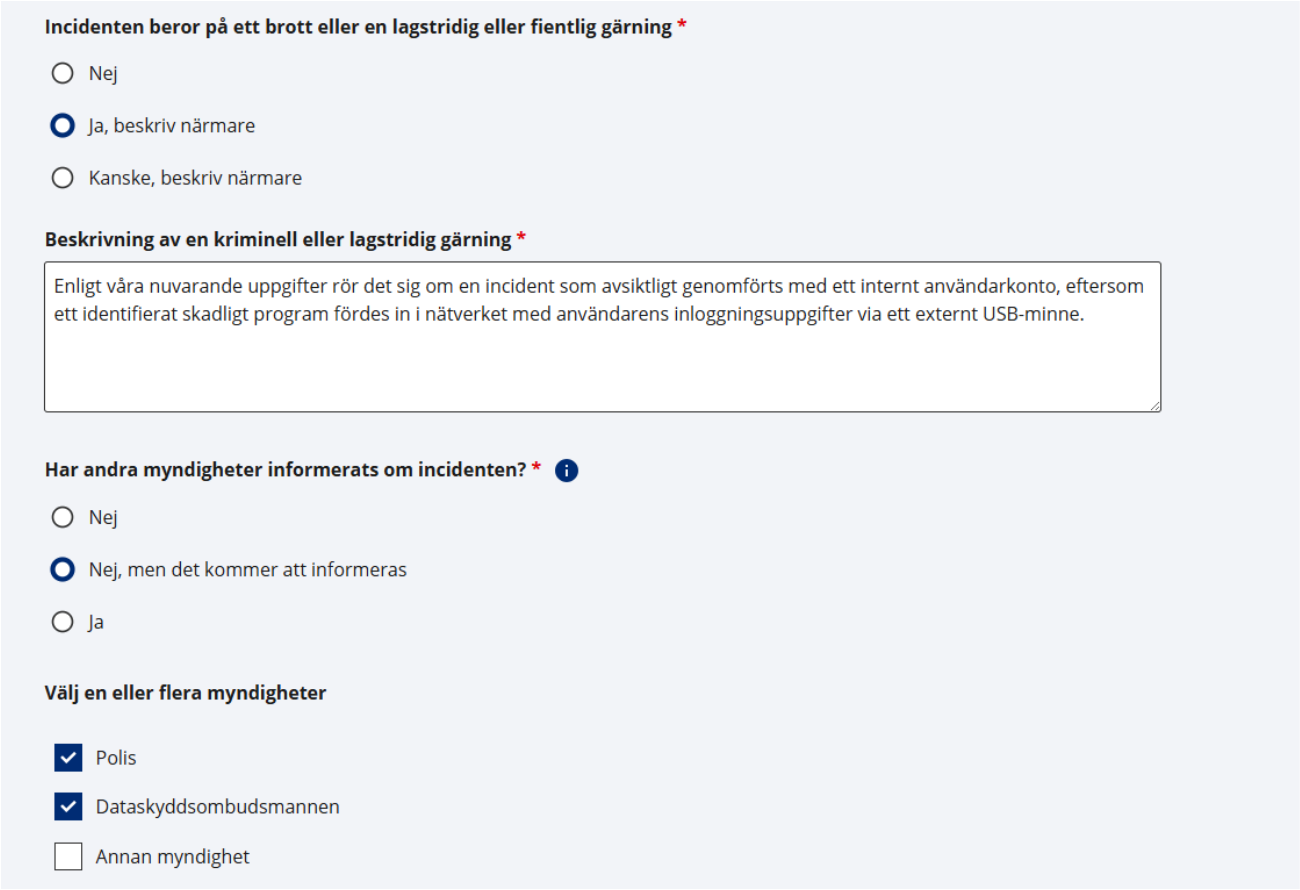

Bild 3 Anmälningar till andra myndigheter som kommer att informeras om incidenten.

Om grundorsaken till exempelfallet är ett så kallat internt hot bör man beakta de fält i blanketten som gäller möjligheten till brott, lagstridig eller fientlig gärning.

Med tanke på tidsgränsen för den första anmälan (24 timmar) ska man dock beakta att det kanske inte nödvändigtvis är möjligt att fylla i de ovan nämnda fälten. I en situation där er organisation misstänker en eventuell fientlig gärning kan ni också välja punkten "Kanske" och komplettera ert svar till exempel i den uppföljande anmälan eller slutrapporten, när er interna och/eller externa utredning har kunnat precisera hur incidenten uppstod, till exempel vad gäller en intern aktör och gärningens avsiktlighet.

I fältet för beskrivning av ett brott eller en lagstridig eller fientlig gärning kan ni beskriva händelseförloppet i ljuset av den information som finns tillgänglig i nuläget. På grund av tidsgränsen för den första anmälan är det dock möjligt att händelseförloppet ännu inte är helt klarlagt. Om ni önskar kan ni också beskriva hur incidenten uppstod på en övergripande nivå och precisera er beskrivning senare i anmälningsprocessen, till exempel i form av en uppföljande anmälan och/eller en delrapport.

I ett fall där även personuppgifternas informationssäkerhet har äventyrats, till exempel till följd av en filstöld, ska man även beakta personuppgiftsansvariges anmälningsskyldighet enligt den allmänna dataskyddsförordningen (s.k. GDPR-anmälan) till dataombudsmannens byrå. Anmälningsskyldigheten gäller en personuppgiftsincident som innebär "en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats."

En personuppgiftsincident ska anmälas till dataombudsmannens byrå utan obefogat dröjsmål och i mån av möjlighet inom 72 timmar från det att den personuppgiftsansvarige blivit medveten om personuppgiftsincidenten.

Vid val av myndigheter som ärendet kommer att anmälas till och/eller där en anmälan redan har gjorts, kan ni även välja punkten "Annan myndighet". Syftet med detta alternativ är till exempel att möjliggöra informationsflödet mellan olika myndigheter vid incidenter där aktörer, på grund av ett omfattande verksamhetsområde, har två eller flera tillsynsmyndigheter. I referensfallet på bild 2 har polisen (på grund av möjligheten till lagstridig gärning) och dataombudsmannens byrå (på grund av den eventuella personuppgiftsincidenten) valts som andra myndigheter.

Observera att annan myndighet i detta sammanhang inte avser CSIRT-enheten vid Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom, som även är känd under sitt tidigare namn CERT-enheten. CSIRT-enheten får en kopia av de uppgifter som har getts till tillsynsmyndigheten efter att denna blankett har fyllts i. Uppgifterna som skickas till enbart CSIRT-enheten har en separat undermeny på blanketten för första anmälan och den behandlar vi senare i detta dokument.

Vid incidentfall vars konsekvenser sträcker sig utanför Finlands gränser ska följande fält fyllas i. I fältet Beskrivning av konsekvenser kan ni till exempel räkna upp de medlemsländer i Europeiska unionen som påverkas av incidenten samt berätta närmare om incidentens konsekvenser inom Europeiska unionen. Om incidenten kan ha gränsöverskridande konsekvenser, men detta ännu inte är helt klarlagt vid tidpunkten för första anmälan, kan ni också i detta fält beskriva eventuella konsekvenser och sannolikheten för att de inträffar.

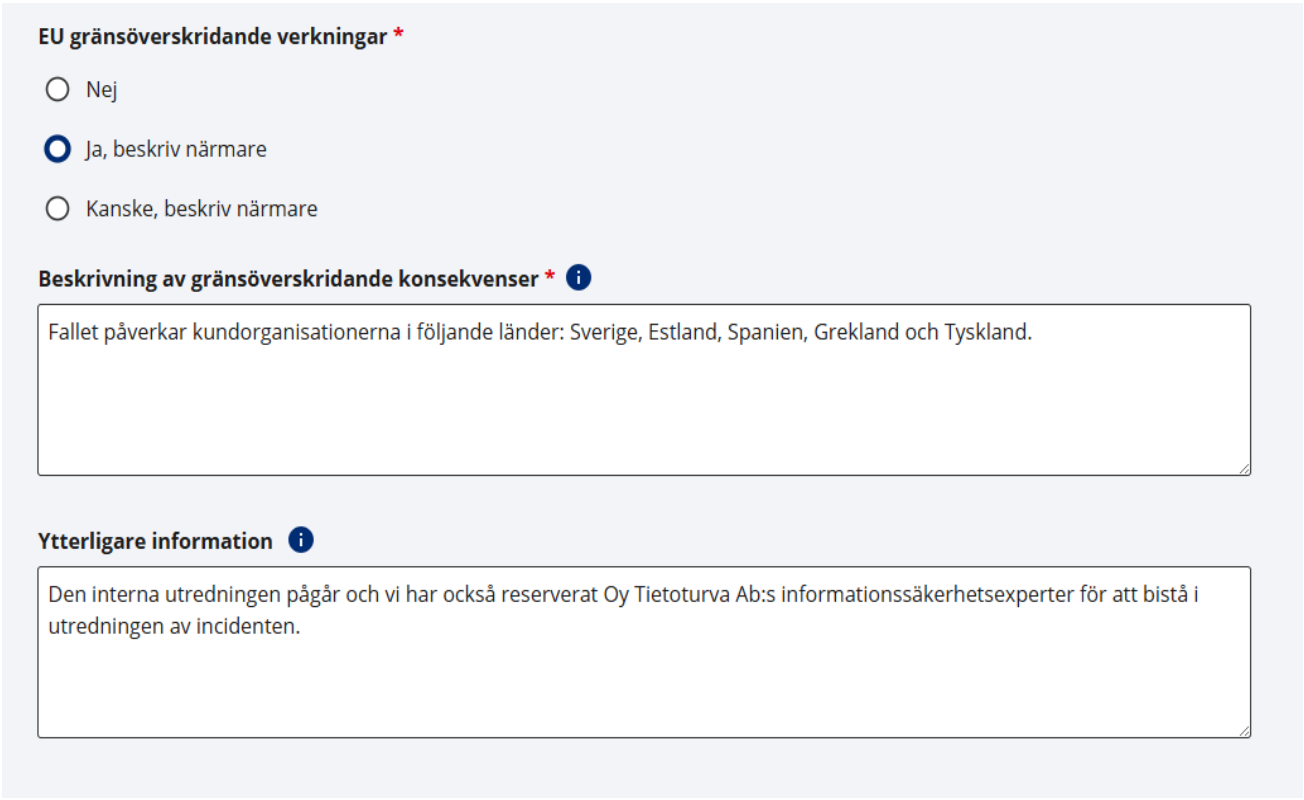

Bild 4 Gränsöverskridande konsekvenser och tilläggsuppgifter

Därefter kan ni fylla i anmälarens kontaktuppgifter, antingen på organisationens vägnar eller som privatperson, såsom i exemplet på Bild 5. Kom ihåg när ni fyller i anmälarens kontaktuppgifter att den behöriga tillsynsmyndigheten kan kontakta de e-postadresser som angetts för begäran om tilläggsuppgifter och för fortsatt utredning av (anmält) ärende/händelse.

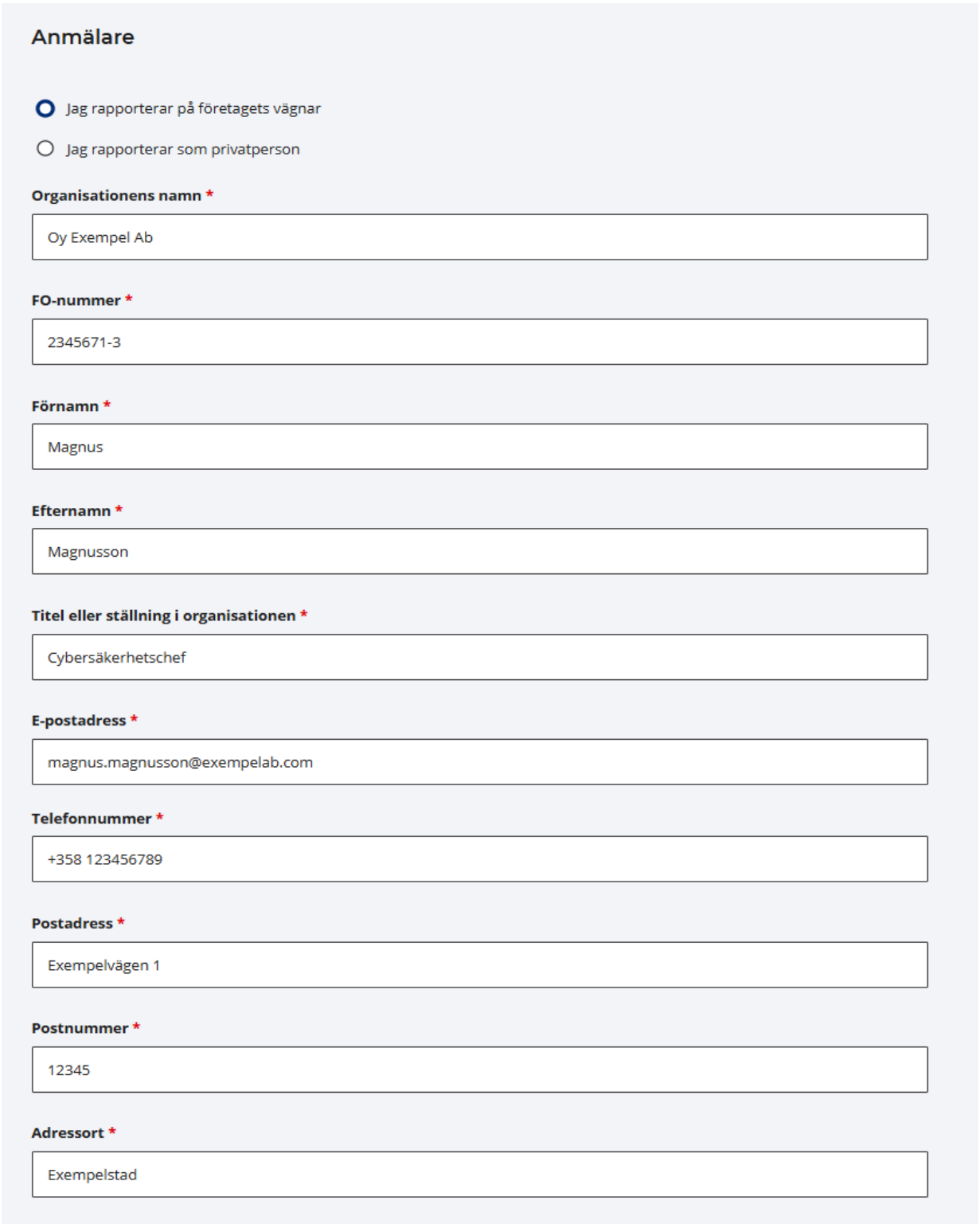

Bild 5 Anmälarens kontaktuppgifter

Ovanstående uppgifter förmedlas till den myndighet som övervakar er organisation, vilken till exempel för sektorn Digital infrastruktur är Transport- och kommunikationsverket.

Om ni i anslutning till ett ärende vill skicka information till Cybersäkerhetscentrets CSIRT-enhet och/eller dela ytterligare information med CSIRT-enheten, kan ni under posten för adressort välja alternativet "Jag behöver stöd av Cybersäkerhetscentrets CSIRT-enhet eller jag vill frivilligt ge dem ytterligare information", vilket öppnar en tilläggsblankett.

Observera att de uppgifter som anges i fälten under denna knapp endast förmedlas till Cybersäkerhetscentrets CSIRT-enhet vid Transport- och kommunikationsverket Traficom. Dessa uppgifter förmedlas inte till tillsynsmyndigheterna. Enligt 25 § i cybersäkerhetslagen får information som på frivillig basis lämnats ut till CSIRT-enheten för skötseln av uppgifter enligt denna lag inte utan samtycke av den som lämnat ut informationen användas i brottsutredningar eller vid administrativt eller annat beslutsfattande som gäller den som lämnat ut informationen.

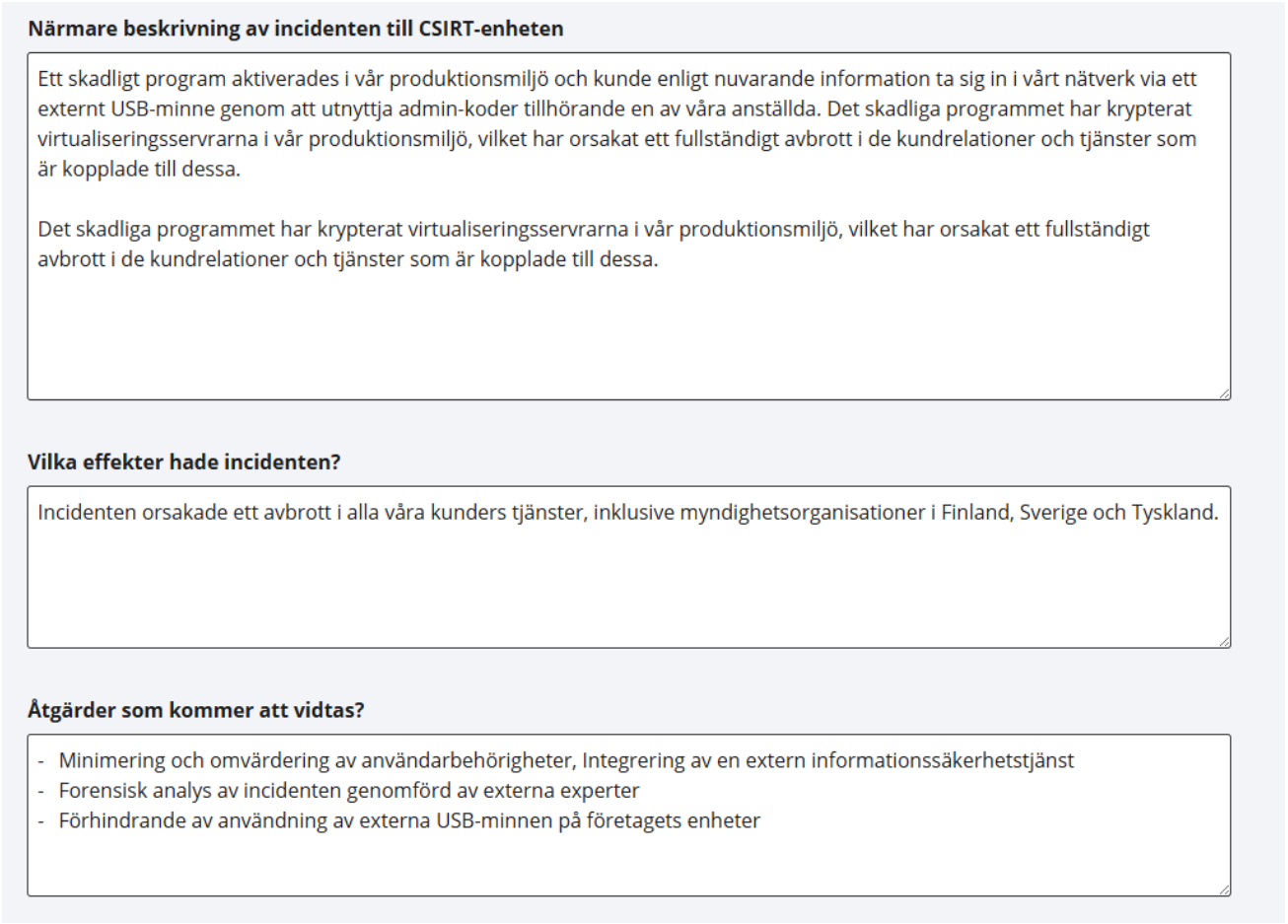

Bild 6 CSIRT-tilläggsblankett

Bild 6 beskriver ett exempel på en tilläggsanmälan till CSIRT-enheten enligt referensfallet, där man på ett allmänt plan har beskrivit händelseförloppet för incidenten, de första åtgärderna som vidtogs samt identifieringsuppgifter relaterade till incidenten. Utöver de identifieringsuppgifter som räknas upp i beskrivningen för fältet kan ni till exempel ange en s.k. Hash-identifierare och/eller en s.k. angreppsindikator, det vill säga

en IOC-indikator (Indicator of Compromise), samt annan teknisk identifieringsinformation kopplad till incidenten.

Angreppsindikatorerna, dvs. IOC-indikatorerna, är tekniska identifierare eller mätbara tekniska observationer som kan användas för att avgöra om en cyberattack är möjlig, pågår just nu eller har inträffat redan tidigare.

De vanligaste angreppsindikatorerna är olika logguppgifter som produceras av nätverk-, enhet-, fil- och beteendebaserade system. I referensfallet kunde eventuella IOC-poster till exempel utgöras av loggdata över tidpunkten då utpressningsprogrammet aktiverades.

Bild 7 MSSP-tilläggsuppgifter

Om er organisation använder en extern leverantör av informationssäkerhetstjänster för att utreda en incident och/eller på kontinuerlig basis kan ni lägga till deras kontaktuppgifter i fälten enligt Bild 7 om ni vill att Cybersäkerhetscentrets CSIRT-enhet kan kontakta leverantören i frågor som gäller incidenten.

Bild 8 CSIRT-tilläggsblankett, avsnittet om brottsanmälan d.v.s. polisanmälans.

Under Brottsanmälan kan ni komplettera uppgifterna om en eventuell brottsanmälan om ni har gjort en sådan innan den första anmälan fylldes i. Vid behov kan ni också välja alternativet "Kommer att göras" och komplettera i senare anmälningar, till exempel i samband med en uppföljande anmälan om en brottsanmälan som görs senare.

I nedre kanten av bild 8 kan ni också välja om ni vill att CSIRT-enheten kontaktar er i fråga om incidenten samt ge ert eventuella samtycke till konfidentiell kommunikation med andra myndigheter. I denna anvisning vill vi betona att man vid ovan nämnda konfidentiella kommunikation inte förmedlar information till tillsynsmyndigheten i enlighet med 25 § i cybersäkerhetslagen.

Bild 9 CSIRT-kontaktuppgifter

I slutet av CSIRT-tilläggsblanketten kan ni också lägga till kontaktuppgifter som CSIRT-enheten kan använda för att kontakta er angående utredningen av incidenten. Dessa kontaktuppgifter kan till exempel vara kontaktuppgifter till företagets SOC-säkerhets-operationscenter eller en teknisk expert/experter.

När ni har fyllt i de fält som behövs för den första anmälan kan ni gå till förhands-granskningen genom att klicka på Fortsätt. I förhandsgranskningsläget kan ni säker-ställa att ni noggrant har fyllt i de fält som är relevanta för er incident.

Efter förhandsgranskningen kan ni fylla i CAPTCHA-förfrågan längst ner på sidan och klicka på knappen Skicka, varefter anmälan skickas till tillsynsmyndigheten för den NIS2-sektor ni har valt. Ni kan även skriva ut uppgifterna i er incidentanmälan i PDF-format från blankettens tredje sida efter att ni skickat in anmälan.

För den NIS2-incidentanmälan ni lämnat in skickas även en automatisk mottagningsbe-kräftelse till den e-postadress ni uppgett, med vilken ni kan försäkra er om att anmälan har anlänt till tillsynsmyndigheten.

2.2 Uppföljande anmälan

Efter den första anmälan ska en uppföljande anmälan göras inom 72 timmar från det att den betydande incidenten upptäcktes. Det huvudsakliga syftet med den uppföljande anmälan är att precisera uppgifterna i den första anmälan till exempel om händelsens grundorsak, noggrannare konsekvenser och allvarlighetsgrad.

När ni fyller i den uppföljande anmälan behöver ni det unika ärendenumret i formatet ”123456” som ni fick i mottagningsbekräftelsen för den första anmälan. Ni hittar det ovan nämnda ärendenumret i det e-postmeddelande med e-postrubriken ”Mottagningsbekräftelse” som skickades till anmälarens e-postadress i samband med den första anmälan.

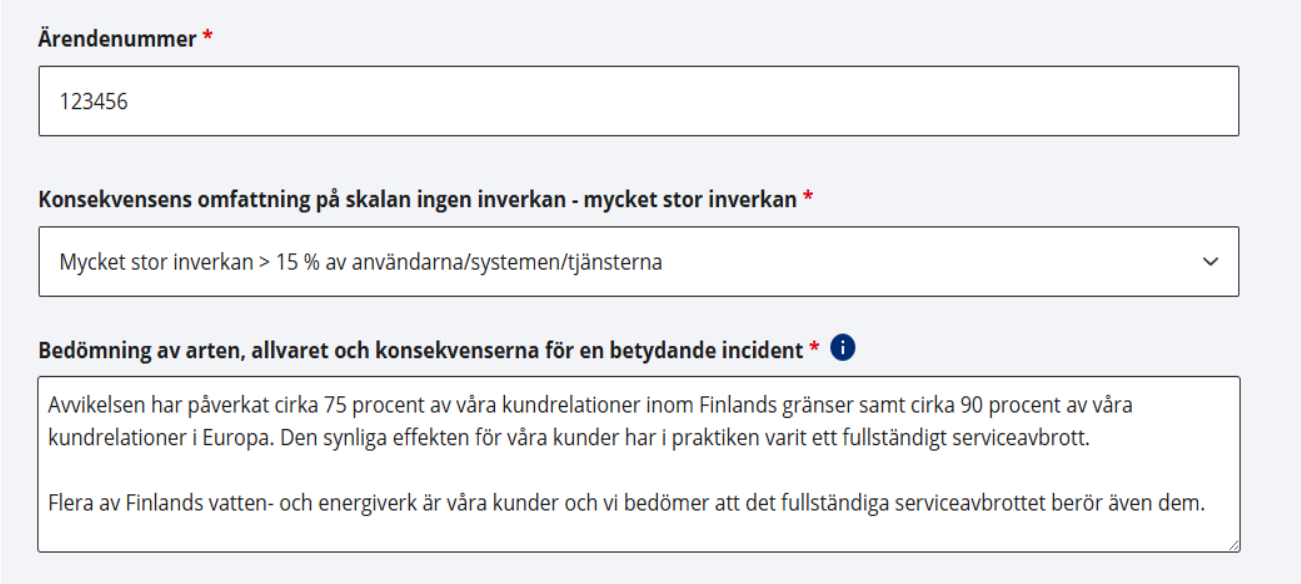

Bild 10 Basuppgifter för den uppföljande anmälan

När ni väljer ett lämpligt alternativ för omfattningen av konsekvensen är det bra att beakta att detta avsnitt utgår från principen om så kallad övergripande konsekvens. Välj således i den aktuella punkten det alternativ som beskriver incidentens inverkan på ett övergripande sätt, oberoende av om konsekvensen är ett fullständigt serviceavbrott eller till exempel en fördröjning i tjänstens funktion till exempel på grund av en DDoS-överbelastningsattack.

Som exempel kan nämnas ett fall där 10 procent av företagets tjänster är utsatta för ett fullständigt avbrott och 20 procent av tjänsterna drabbas av en betydande fördröjning, men där servicen fortfarande fungerar för ett begränsat antal användare. I detta fall bör man välja alternativet "Mycket omfattande konsekvens", eftersom de betydande konsekvenserna överskrider den gräns på 15 procent som anges i alternativen. På ett allmänt plan kan man säga att om tjänsten utsätts för en betydande konsekvens på grund av en incident ska detta beaktas när denna punkt fylls i.

När ni bedömer incidentens art, allvarlighetsgrad och konsekvens kan ni komplettera de första uppgifterna som lämnades i den första anmälan, till exempel genom att precisera avgränsningen av konsekvenserna per tjänst. Ni kan även ange preliminära uppskattningar av hur många användare som påverkas samt hur tjänsterna fungerar för

dessa användare (exempel: fullständigt eller partiellt avbrott, hos alla användare eller endast hos vissa användare).

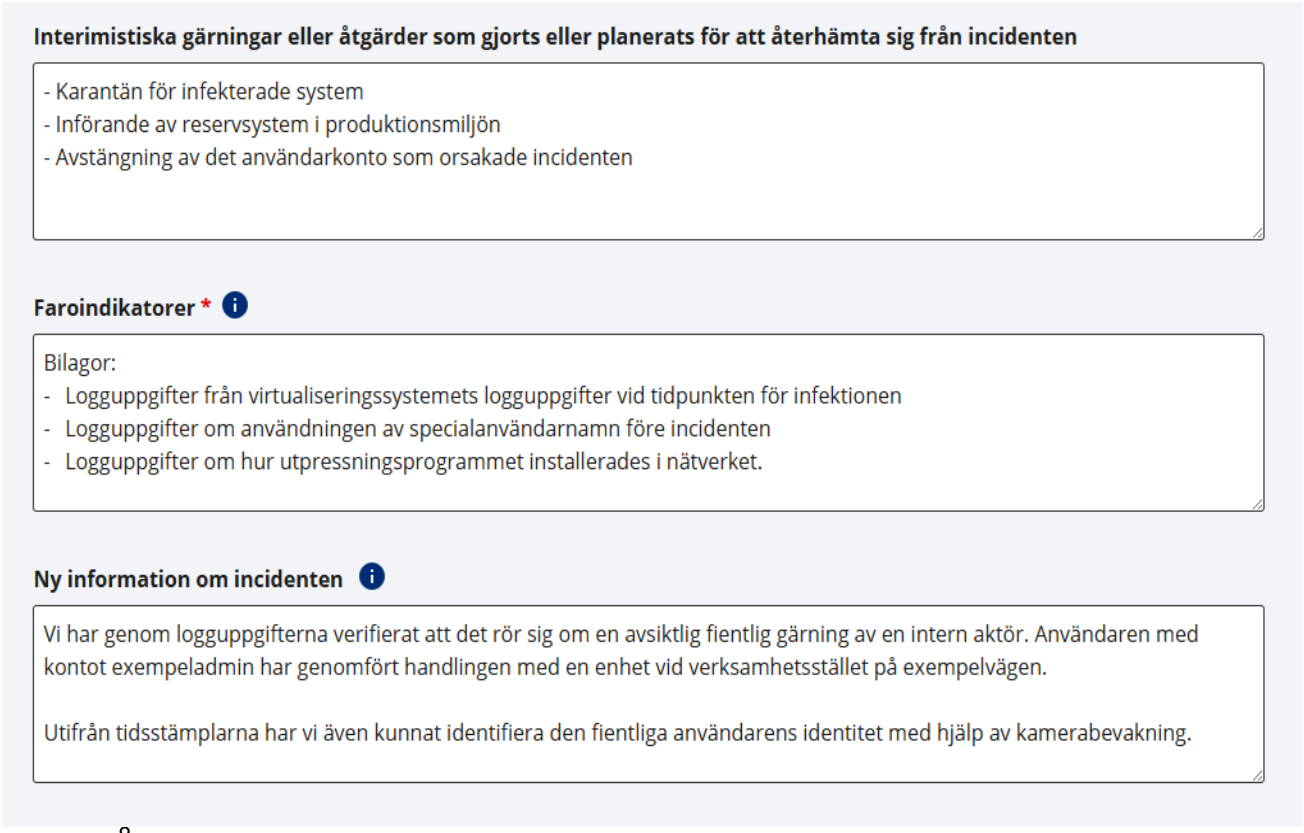

Bild 11 Åtgärder, IOC-poster och nya uppgifter

I rutan för de tillfälliga åtgärder som beskrivs på bild 11 ovan kan ni till exempel beskriva tillfälliga åtgärder som har vidtagits för att begränsa incidentens konsekvenser. Sådana åtgärder kan till exempel vara ibruktagande av säkerhetskopior, begränsning av användarrättigheter, utnyttjande av reservsystem samt andra tillfälliga och snabbt genomförbara åtgärder av tillfällig karaktär.

Tekniska identifieringsuppgifter relaterade till informationssäkerhetsincidenten (IOC, eng. Indicators of Compromise) kan anges i fältet för tekniska angreppsindikatorer, om sådana IOC-poster finns tillgängliga.

När man gör den uppföljande anmälan är det vanligt att händelseförloppet har preciserats sedan den första anmälan. I fältet för nya uppgifter kan ni precisera de uppgifter ni angett i den första anmälan samt ge ytterligare information. I fråga om referensfallet kan den nya informationen till exempel vara en verifierad attackvektor eller verifiering av en intern aktör.

I detta fält kan ni också nämna åtgärder genom vilka ni har strävat efter att säkerställa att den nuvarande incidenten inte kan upprepas i framtiden. I referensfallet skulle ett bra exempel vara en åtgärd där användningen av externa USB-minnen på företagets enheter helt förbjuds utan ett separat godkännande.

2.3 Delrapport

Syftet med delrapporten är att ge en mellanuppdatering om hur utredningen av incidenten framskrider efter den uppföljande incidentanmälan. I delrapporten kan ni beskriva hur hanteringen av incidenten har framskridit för er organisations del efter den första anmälan och den uppföljande anmälan, samt vilken status ärendet har i nuläget. Ange också vilka aktörer som deltagit i hanteringen av incidenten (myndigheter, företag som tillhandahåller informationssäkerhetstjänster osv.).

Delrapporten kan utnyttjas till exempel i långvariga fall där återhämtningen från en incident tar betydligt längre tid än vad som specificeras för anmälningsgränserna i cybersäkerhetslagen. I referensfallet skulle det vara möjligt för företaget att lämna in en delrapport till tillsynsmyndigheten när tidtabellen för återhämtning från incidenten har preciserats.

Delrapporten kan också utnyttjas i fall där det i utredningen av en incident har framkommit omständigheter som har en avgörande betydelse för utredningen av fallet. I referensfallet har det blivit betydelsefullt att konsekvenserna för organisationens kundrelationer kunde minimeras snabbare än väntat, eftersom organisationens reservsystem kunde återställa organisationens tjänster till full funktion innan produktionsmiljön åter var i drift.

Ärendenummer *

123456

Framåtskridande och statusuppdatering av behandlingen av incidenten *

Utredningen av incidenten har avslutats, den straffrättsliga processen framskrider på behörigt sätt.

Återhämtningen från incidenten löper enligt god modell, den uppskattade fullständiga återhämtningstiden är cirka 1 vecka, reservsystemen genomför underhållet av produktionsmiljön under tiden för incidenten. Incidentens inverkan på kunderna upphörde cirka kl. 04.30 när reservsystemen aktiverades i produktionen.

I undersökningen deltog Oy Tietoturva Ab, Polisen, Cybersäkerhetscentret.

Ytterligare information

Grundorsakerna till incidenten har identifierats och användningen av dem har förhindrats i framtiden genom tekniska åtgärder. Vi har även preciserat våra processer för att begränsa användarbehörigheter i samband med uppsägningar, i syfte att förhindra att de omständigheter som ledde till incidenten upprepas i vår organisation.

Bild 12 Delrapport

2.4 Slutrapport

Slutrapporten ska fyllas i inom en månad (1 mån.) efter att den uppföljande anmälan har lämnats in eller, om det är fråga om en långvarig incident, inom en månad (1 mån.) efter att hanteringen av incidenten har avslutats. Syftet med denna typ av anmälan är att fungera som en slutlig rapport till tillsynsmyndigheten, där informationen om incidenten redovisas så att säga i sin helhet.

Bild 13 Varaktighet & Antal personer

I det andra fältet i slutrapporten ombeds ni att bedöma hur informationssäkerhetsincidenten har påverkat användare inom respektive sektor som omfattas av tillsyn enligt cybersäkerhetslagen. När denna konsekvensbedömning görs ska man dock beakta att det inte nödvändigtvis är möjligt att bedöma konsekvensernas fullständiga effekter. Således kan ni i det ovan nämnda fältet lämna en avrundad uppskattning av incidentens konsekvenser, där noggrannheten bestäms utifrån den tillgängliga informationen samt incidentens allvarlighets- och konsekvensgrad.

När ni bedömer konsekvensens varaktighet i det tredje fältet kan ni till exempel använda tidslinjen som presenteras på bild 13 för att beskriva incidentens varaktighet.

I det ovan nämnda fältet kan ni också beskriva separata tidsperioder, om incidentens konsekvenser till exempel har begränsats till tre separata tidsperioder till följd av incidenten. Att beskriva separata verkningstider av en konsekvens är särskilt ändamålsenligt till exempel i anmälningar om incidenter till följd av DDoS-attacker, där det är vanligt att incidentens konsekvens inte är kontinuerlig utan går i vågor beroende på DDoS-attackens volym.

Fältet "Detaljerad information om incidenten och dess konsekvenser" kan fyllas i enligt den bifogade anvisningen samt genom att följa exemplet på bild 14.

Beskriv noggrant vad som har hänt. Ange eventuella fel, störningar eller oväntade händelser. Bedöm hur betydande eller kritisk incidenten är med tanke på verksamheten. Ni kan använda skalan (t.ex. liten, måttlig, allvarlig) eller beskriva allvarlighetsgraden

verbalt. Beskriv vilka konsekvenser incidenten har haft eller kan ha. Fundera till exempel på hur incidenten har påverkat verksamheten, produkterna, tjänsterna eller säkerheten. Om incidenten har ekonomiska eller tidsmässiga konsekvenser, nämn även dessa.

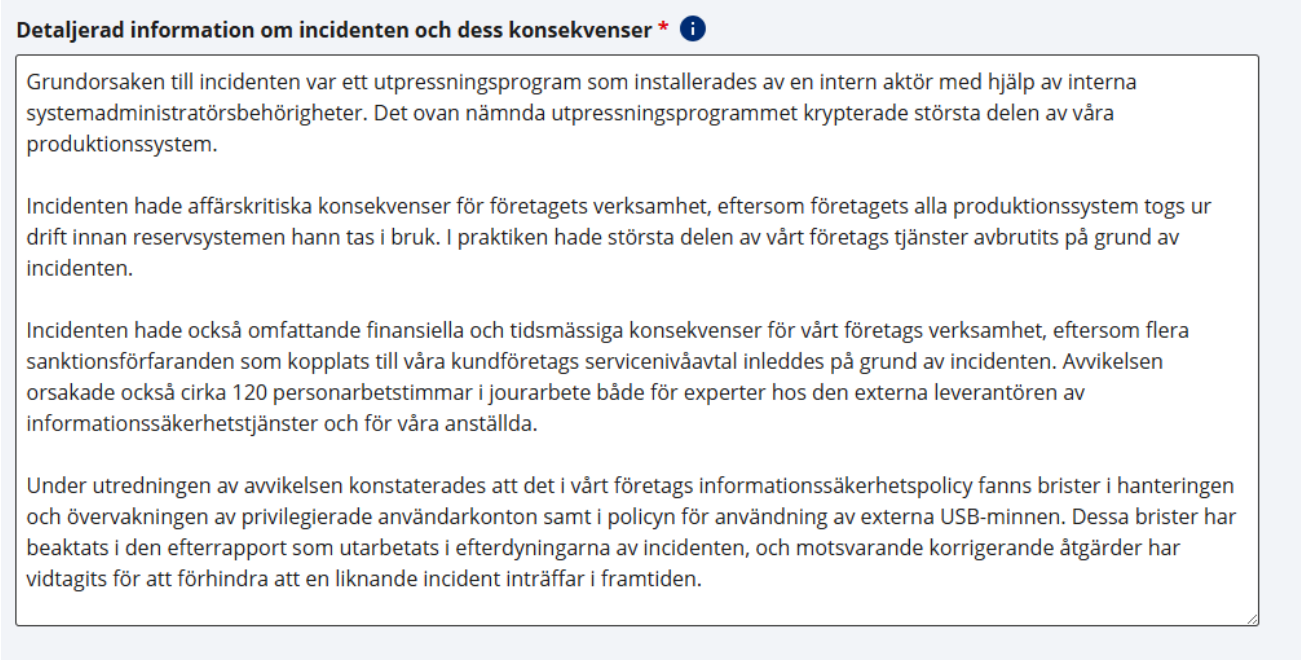

Bild 14 Detaljerad information om incidenten och dess konsekvenser

När ni fyller i kategorifälten enligt Bild 15 ska ni välja alla fält som beskriver de omständigheter som förekommit i samband med incidenten. I referensfallet skulle den huvudsakliga grupperingen passa under alternativet ”Avsiktliga interna gärningar”, men på grund av fallets karaktär har även alternativet fysisk skadevållande/utnyttjande/stöld valts, eftersom ett eventuellt utpressningsprogram kan ha haft som syfte att rikta ett utpressningskrav mot den organisation som varit föremål för incidenten.

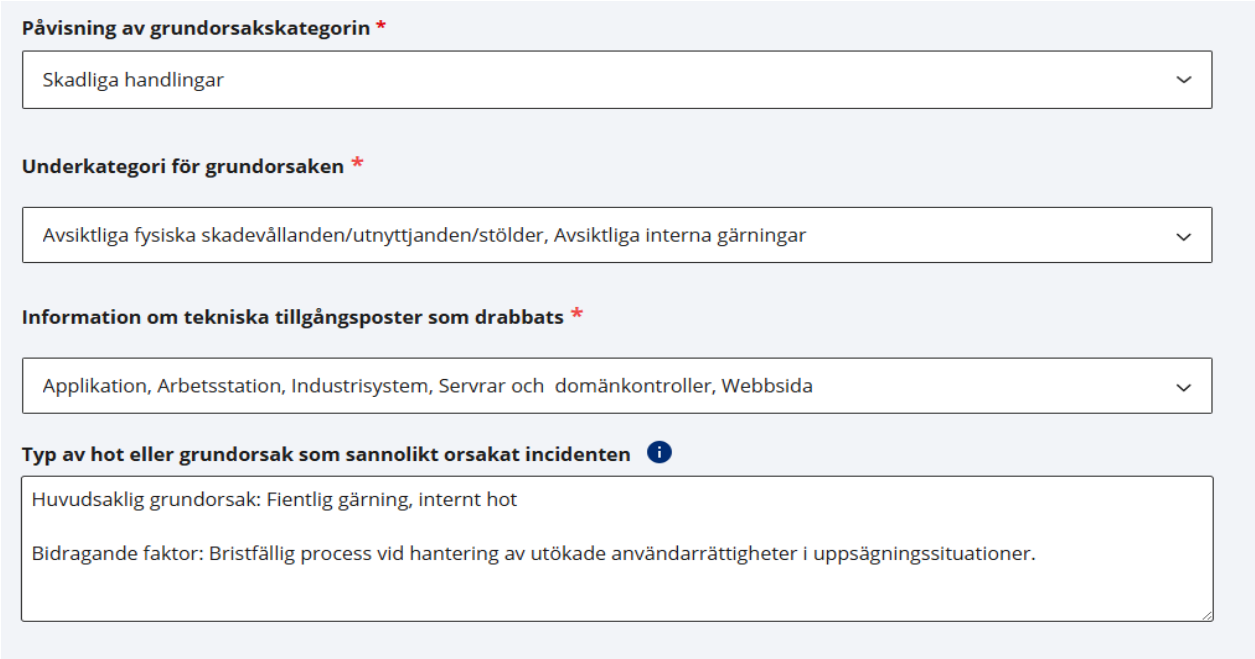

Bild 15 Kategorisering av incidentens grundorsaker och konsekvenser.

När ni väljer de tekniska tillgångsposter som påverkas av konsekvensen, välj de system som påverkades avsevärt på grund av incidenten.
I referensfallet där konsekvensen var omfattande bör det beaktas att den huvudsakliga konsekvensen riktades mot den först valda kategorin, det vill säga alternativet ”Servrar och domänkontroller”.

Beskriv vad som sannolikt orsakade incidenten. Om incidenten berodde på flera hot eller grundorsaker, välj den huvudsakliga orsaken och ange även andra eventuella faktorer. Ni kan fylla i ovan nämnda fält till exempel enligt följande:

- *'Huvudsaklig orsak: Mänskligt misstag, tilläggsfaktor: Bristfällig process.'*

Om ni i samband med utredningen har genomfört en mer omfattande analys av grundorsaken till incidenten, kan beskrivningen innehålla noggrannare detaljer om de grundorsaker som lett till incidenten samt om de relaterade processerna.

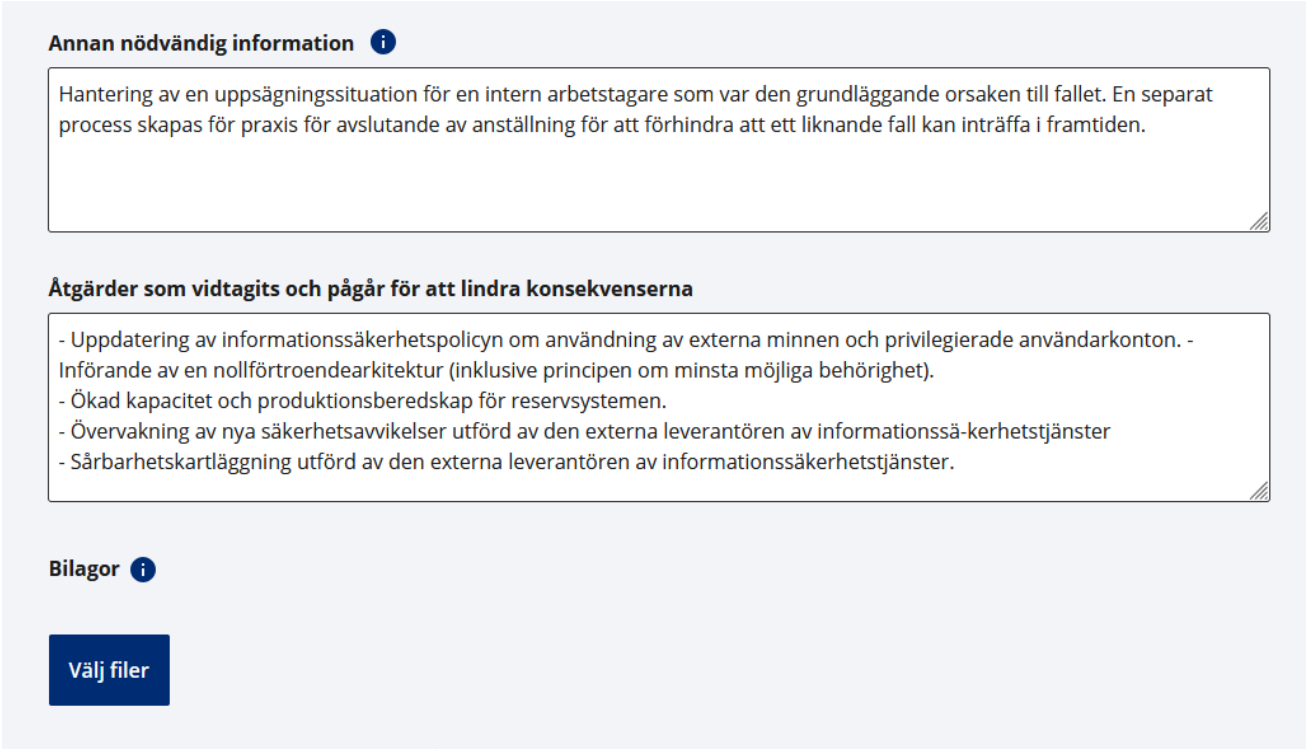

Bild 16 Övriga uppgifter och åtgärder

I fältet för annan nödvändig information kan ni skriva alla sådana uppgifter som inte passade i tidigare fält, men som ändå är viktiga för hanteringen av incidenten. Detta kan omfatta till exempel specialsituationer, bakgrundsuppgifter eller tilläggsobservationer som förtydligar incidentens omfattning eller orsaker.

I fältet "Åtgärder som vidtagits och pågår för att lindra konsekvenserna” kan ni beskriva nuläget för de åtgärder som ert företag vidtagit samt åtgärdernas kontinuitet i framtiden. Enligt bild 16 kan ni också berätta i detta fält om ni har fortsatt verksamheten till exempel med den externa leverantören av informationssäkerhetstjänster även efter incidenten.

Bifoga dokument, rapporter, bilder eller andra filer som stöder eller kompletterar beskrivningen av incidenten. Säkerställ att bilagorna är i godtagbara filformat (t.ex. PDF, DOCX, XLSX, JPG, PNG). Namnge filerna tydligt och beskrivande så att deras innehåll är lätt att förstå.

Beakta eventuella begränsningar av filstorlek. Om er fil är stor ska ni överväga att förminska den eller dela den i flera delar så att bilagorna kan laddas ner utan problem. Som bilaga till slutrapporten kan ni också lägga till interna rapporter, analyser av grundorsaken samt övriga dokument angående incidenten.

2.5 Frivillig underrättelse till tillsynsmyndigheten

I detta avsnitt kan ni göra en frivillig underrättelse till tillsynsmyndigheten om andra störningar än betydande incidenter. Uppgifterna förmedlas också till CSIRT-enheten vid Traficoms Cybersäkerhetscenter. Om ni däremot vill göra en anmälan endast till CSIRT-enheten hittar ni blanketten för den frivilliga underrättelsen också direkt på Cybersäkerhetscentrets ingångssida.

Vem som helst kan göra frivilliga underrättelser om incidenter, hot och tillbud. En frivillig underrättelse kan göras av till exempel en aktör i enlighet med cybersäkerhetslagen, ett småföretag som verkar inom en sektor som är viktig för samhället eller en privatperson.

Med hjälp av dessa underrättelser får Cybersäkerhetscentret värdefull information om fenomen och utvecklingstrender i den nationella cybermiljön, och vi uppmuntrar er därför att även göra frivilliga underrättelser med låg tröskel.

Den frivilliga underrättelsen är indelad i tre separata kategorier.

2.5.1 Incident

Syftet med en frivillig incidentanmälan är att anmäla en icke-betydande incident till tillsynsmyndigheten.

I cybersäkerhetslagen definieras en incident enligt följande:

"*Incident* är en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem,"

En icke-betydande incident avser en incident vars inverkan på företagets verksamhet är liten. Exempel på sådana situationer är till exempel att man via ett försök till nätfiske (eng. phishing) lyckas fånga upp en enskild arbetstagares användarnamn och lösenord för ett icke-privilegierat användarkonto.

2.5.2 Cyberhot

Ni kan också meddela tillsynsmyndigheten om cyberhot som har framkommit i ert företags verksamhet, till exempel nya sårbarheter i programvara som framkommit i en utredning om informationssäkerhet.

I cybersäkerhetslagen definieras ett cyberhot enligt följande:

”Cyberhot är en omständighet, händelse eller handling som när den förverkligas kan skada, störa eller på annat negativt sätt påverka kommunikationsnät eller informationssystem, användare av dessa system och andra personer,”

Ett praktiskt exempel på ett cyberhot kan också vara en omfattande kampanj för nätfiske riktad mot företagets e-postadresser, där angriparna dock inte lyckats få kontroll över några användaruppgifter.

2.5.3 Tillbud

Ett tillbud är avsett för situationer där en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som av någon slumpmässig orsak inte uppstod.

Sådana situationer är till exempel lyckade angrepp genom nätfiskeförsök (eng. phishing) mot arbetstagarens lösenord, men ändå så att användarnamn som fåtts under kontroll på detta sätt inte har kunnat utnyttjas till exempel på grund av att man använder multifaktorsautentisering (eng. 2FA/MFA)

Eventuella utvecklingsidéer, önskemål om tillägg och annan respons om denna anvisning kan skickas per e-post till "nis.valvonta.ktk@traficom.fi".

Vänligen inkludera följande identifierare i e-postmeddelandets ämnesråd: [NISLO]