Version 1.0

Stöd för ifyllande av incidentrapporteringsformulären för samhällsviktiga respektive digitala tjänster

Vägledningen är ett s.k. ”levande dokument”. Det uppdateras kontinuerligt med ny information utifrån vilka frågor MSB får. Kontrollera alltid att ni använder den senaste versionen på www.msb.se/nis.

Innehållsförteckning

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

Samhällsviktiga tjänsters sektorstillhörighet och vidarebefordran av incidentrapporter

Begreppet ”Samhällsviktiga tjänster” avser, enligt i NIS-direktivet och den svenska lagen (Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster), tjänster inom sju sektorer. I Sverige har varje sektor en särskild tillsynsmyndighet som också har föreskriftsrätt (med undantag för sektorn Hälso- och sjukvård där Inspektionen för vård och omsorg har ansvar för tillsyn och Socialstyrelsen har mandat att utfärda föreskrifter). När en leverantör av en samhällsviktig tjänst rapporterar om en incident till MSB så vidarebefordrar MSB den rapporten till den ansvariga tillsynsmyndigheten (och myndigheten med mandat att utfärda föreskrifter) enligt det följande schemat:

Rapport om incident hos samhällsviktig tjänst i sektorn	**Vidarebefordras till**
Bankverksamhet	Finansinspektionen
Digital infrastruktur	Post- och telestyrelsen
Dricksvattenförsörjning	Livsmedelsverket
Energiförsörjning	Statens energimyndighet
Finansmarknadsinfrastruktur	Finansinspektionen
Hälso- och sjukvård	Inspektionen för vård och omsorg (IVO) och Socialstyrelsen
Transporter	Transportstyrelsen

Typer av samhällsviktiga tjänster

Energi	**Transport**
Systemansvarstjänst för transmission av el (TSO)	Flygplatstjänst
Elöverföring i regionnät	Flygkontrolltjänster
Eldistribution (DSO)	Infrastrukturförvaltning och-/eller trafikledning av järnväg
Elproduktion	Järnvägsföretag
Elhandel	Hamnar
Import, export, produktion, raffinering, bearbetning eller försäljning av flytande drivmedel och bränslen	Sjötrafikinformationstjänst
	Vägmyndighet
	Intelligenta transportsystem
Drivmedelslager och depåer för flytande drivmedel och bränslen	**Bankverksamhet**
	Bankverksamhet
Överföringstjänst i ledningar mm, för flytande drivmedel och bränslen	**Finansmarknadsinfrastruktur**
Systemansvarstjänst för transmission av naturgas (TSO)	Handelsplatser
	Centrala motparter
Systemansvarstjänst för distributionssystem för naturgas (DSO)	**Leverans och distribution av dricksvatten**
	Leverans och distribution av dricksvatten
Handel och leverans av naturgas	**Digital infrastruktur**
Kondensering av naturgas samt hantering av LNG	Administration och förvaltning av toppdomän
	DNS-tjänster

Hälso- och sjukvård
Primärvård
Prehospital akutsjukvård
Specialiserad somatisk vård
Specialiserad psykiatrisk vård
Kommunal hälso- och sjukvård
Tandvård

Typer av digitala tjänster

Digitala marknadsplatser	Molntjänster	Sökmotorer

Kriterier för betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten

Se Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9), kap. 3-9. Vid användning av incidentrapporteringsformuläret för samhällsviktiga tjänster i samband med en incident går det bra att kopiera och klistra in den eller de relevanta kriterierna.

Energi
3 kap. 1 § p. 1a - El - Störningen har pågått i minst två timmar och har påverkat minst 2 000 kunder.
3 kap. 1 § p. 1b - El - Störningen har pågått i minst två timmar och har påverkat minst 50 % av kunderna.
3 kap. 1 § p. 2 - El - Störningen har påverkat styrning och övervakning av transmissionsnät, regionnät eller elproduktion.
3 kap. 2 § p. 1 - Gas - Störningen innebär risk för en händelse som resulterar i en avsevärd försämring av försörjningssituationen för gas.
3 kap. 2 § p. 2 - Gas - Störningen kan leda till avbrott i gasförsörjningen.
3 kap. 2 § p. 3 - Gas - Störningen har påverkat styrning och övervakning inom ramen för systemansvarstjänst.
3 kap. 3 § p. 1 - Olja - Störningen har pågått i minst 12 timmar.
3 kap. 3 § p. 2 - Olja - Störningen påverkar styrning och övervakning av ledning, överföring och distributionsnätverk under minst två timmar.
Transport
4 kap. 1 § p. 1a - Störningen har pågått i minst en timme och kan antas ha påverkat minst 1000 användare.
4 kap. 1 § p. 1b - Störningen har pågått i minst en timme och kan antas ha påverkat ett sammanhängande geografiskt område om minst 10 000 km2.
4 kap. 1 § p. 2 - Störningen har pågått i minst två timmar.
Bankverksamhet
5 kap. 1 § p. 1a - Störningen innebär att transaktioner inte kan eller sannolikt inte kommer att kunna initieras eller behandlas för minst 25 % av leverantörens normala antal transaktioner.
5 kap. 1 § p. 1b - Störningen innebär att transaktioner inte kan eller sannolikt inte kommer att kunna initieras eller behandlas för minst 25 % av leverantörens användare.
5 kap. 1 § p. 2 - Störningen pågår sammanlagt minst tre timmar under en 24-timmars period.

Finansmarknadsinfrastruktur
6 kap. 1 § p. 1 - Störningen innebär avvikelse från sådan konnektivitet som avses i art. 11 punkt 5 Kommissionens delegerade förordning (EU) 2017/584 av den 14 juli 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU avseende tekniska tillsynsstandarder som specificerar organisatoriska krav för handelsplatser.
6 kap. 1 § p. 2 - Störningen påverkar väsentliga tjänster hos systemviktiga finansiella infrastrukturföretag och har pågått i minst en timme.
6 kap. 1 § p. 3 - Störningen har pågått i minst två timmar.
Hälso- och sjukvård
7 kap. 1 § p. 1 - Störningen innebär att anmälningsskyldighet inträder enligt 3 kap. 5 § första stycket patientsäkerhetslagen (2010:659).
7 kap. 1 § p. 2 - Störningen har påverkat tillhandahållandet av ambulans och ambulanssjukvård enligt 7 kap. 6 § hälso- och sjukvårdslagen (2017:30).
7 kap. 1 § p. 3 - Störningen innebär att sådan hälso- och sjukvård som baseras på system som insamlar, bearbetar, lagrar eller distribuerar och presenterar information inte kan tillhandahållas i minst två timmar.
7 kap. 1 § p. 4 - Störningen har pågått i minst sex timmar.
Leverans och distribution av dricksvatten
8 kap. 1 § p. 1a - Störningen har pågått i minst två timmar och kan antas ha påverkat minst 2 000 personer.
8 kap. 1 § p. 1b - Störningen har pågått i minst två timmar och har påverkat akutsjukhus.
8 kap. 1 § p. 2 - Störningen har påverkat styrning och övervakning av tjänsten.
Digital infrastruktur
9 kap. 1 § p. 1 - Störningen innebär att toppdomänens namnservertjänst har en tillgänglighet på mindre än 100 procent.
9 kap. 1 § p. 2 - Störningen innebär förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data i samband med tillhandahållande av en toppdomäns namnservertjänst och har berört fler än 2 500 domännamn.
9 kap. 1 § p. 3 - Störningen innebär att en rekursiv namnservertjänst har en tillgänglighet på mindre än 100 procent under en sammanhängande period som överstiger en timme.
9 kap. 1 § p. 4 - Störningen innebär förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data i samband med tillhandahållande av en rekursiv namnservertjänst som har berört fler än 10 000 användare.
9 kap. 1 § p. 5 - Störningen innebär att en auktoritativ namnservertjänst har en tillgänglighet på mindre än 100 procent under en sammanhängande period som överstiger två timmar.
9 kap. 1 § p. 6 - Störningen innebär förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data i samband med tillhandahållande av en auktoritativ namnservertjänst som har berört fler än 2 500 domännamn.

Kriterier för avsevärd inverkan på tillhandahållandet av den digitala tjänsten

Se artikel 3 och 4 i Kommissionens genomförandeförordning (EU) 2018/151.

Namn på den störda samhällsviktiga tjänsten

Det är viktigt att namnge den störda tjänsten så att det framgår vad det är för något som har drabbats av en störning. Namnet som anges bör vara sådant att det förmedlar relevanta detaljer om vad det är för tjänst som har drabbats av en störning. Exempel på sådana detaljer kan vara:

- Om det är en specifik undertyp av en viss typ av samhällsviktig tjänst (exempelvis är ”biomedicinsk analysverksamhet” en specifik undertyp av den samhällsviktiga tjänsten ”primärvård” och ”radarbevakning av luftrummet i anslutning till en flygplats” en specifik undertyp av den samhällsviktiga tjänsten ”flygkontrolltjänst”)
- Om det är en samhällsviktig tjänst som leverantören tillhandahåller på en viss plats i landet (”biomedicinsk analysverksamhet vid labb i Västra götalandsregionen” och ”radarbevakning av luftrummet i anslutning till Arlanda” skulle kunna vara exempel på samhällsviktig tjänster som leverantörer tillhandahåller på specifika platser)

Om den störda samhällsviktiga tjänsten är biomedicinsk analysverksamhet och störningen uppträder på alla labb som leverantören av den samhällsviktiga tjänsten driver i en viss region skulle ett bra namn på den störda samhällsviktiga tjänsten kunna vara:

- *Biomedicinsk verksamhet vid [företaget X:s] labb i [region A].*

Om den störda samhällsviktiga tjänsten är en flygkontrolltjänst och störningen uppträder på två av de fem flygplatser där leverantören av den samhällsviktiga tjänsten bedriver verksamhet skulle ett bra namn på den störda samhällsviktiga tjänsten kunna vara:

- *[Företaget X:s] radarbevakning av luftrummet vid [flygplats A] och [flygplats B].*

Rapportering som leverantör eller på uppdrag av leverantör

Leverantörer av samhällsviktiga respektive digitala tjänster har möjlighet att uppdra åt en annan organisation att rapportera incidenter åt dem. Om en leverantör av en samhällsviktig eller digital tjänst har lämnat rapporteringen till en annan organisation så behöver det anges *både* vilken organisation det är som sköter rapporteringen *och* vilken organisation rapporteringen handlar om.

Om incidenten har inträffat i en tjänst som tillhandahålls av en extern aktör

En leverantör av en samhällsviktig eller digital tjänst kan vara beroende av eller använda sig av tjänster från andra organisationer. Om något inträffar hos en organisation som leverantören är beroende av (om det exempelvis blir elavbrott, en fiberkabel går av, eller om externt tillhandahållen webhosting går ner) och det leder till att leverantörens informationssystem eller nätverk inte fungerar som de ska (och det i sin tur resulterar i en störning med betydande inverkan på kontinuiteten i tjänsten/avsevärd inverkan på

tillhandahållandet av tjänsten) så har incidenten inträffat i en tjänst som tillhandahålls av en extern aktör.

När det sker ska fråga 7 besvaras med ett ”Ja” och de tillhörande fritextfälten fyllas i, såsom i det följande fiktiva exemplet:

Namnet på organisationen som tillhandahåller tjänsten
Alla sorters IT-tjänster AB
Organisationsnummer
128918709-9012
Namn på den externa aktörens tjänst
ASIT Complete Web
Beskrivning av tjänsten och vad er organisation använder tjänsten till
Komplett webhosting med frontend- och backendfunktioner. Inkluderar också molntjänst där stora delar av vår organisations data lagras. Vi använder tjänsten för att kunna tillhandahålla vårt tjänsteutbud över nätet. Kunder loggar in i vår webbportal för att därigenom kunna justera vilka tjänster de använder sig av. Informationen som genereras när kunder gör val lagras i den tillhörande molntjänsten.

När leverantören uppmärksammades på incidenten

I formulären får leverantörerna redogöra för när de blev uppmärksammade på incidenten. Formuleringen om att leverantören blev ”uppmärksammad på”, snarare än ”upptäckte” incidenten är medveten vald. En incident kan i vissa fall först upptäckas av personer eller system utanför den egna organisationen, och det kan också hända att leverantören blir varse incidenten genom att utomstående meddelar leverantören att något verkar vara fel. Det som efterfrågas är alltså när leverantören på egen hand upptäckte incidenten, eller när information inkom till leverantören om att incident har eller kan ha inträffat.

Gränsöverskridande konsekvenser av incidenten

Förmågan att upptäcka och effektivt hantera gränsöverskridande konsekvenser betonas särskilt i NIS-direktivet. Exempel på gränsöverskridande konsekvenser av en *incident* kan vara att skadlig kod tar sig in i leverantörens eller andra organisationers informationssystem eller nätverk i andra länder, eller att information som vanligen skickas från informationssystem i ett land till informationssystem i ett annat land inte kan skickas, eller måste skickas på annat sätt.

VIKTIGT! MSB kan komma att använda informationen om vilka länder som påverkas av gränsöverskridande konsekvenser för att kontakta våra motparter inom NIS-samarbetet och informera dem. MSB tar inte en kontakt med utomstående utan att först informera rapportören.

Funktioner och kapacitet i samhällsviktiga respektive digitala tjänster

Avser fråga 14 och 15 i formuläret för samhällsviktiga tjänster, och fråga 13 och 14 i formuläret för digitala tjänster.

Samhällsviktiga tjänster kan bestå av en uppsättning delar eller *funktioner* som tillsammans utgör tjänsten. Exempelvis kan hälso- och sjukvård omfatta journalhantering, röntgen, biomedicinsk analys, etc. Vid en störning i den samhällsviktiga tjänsten kan det vara så att vissa funktioner drabbas, medan andra fortsätter att fungera. Funktioner som drabbas kan antingen sluta fungera helt och hållet, eller få en minskad *kapacitet* i förhållande till hur de normalt fungerar. Det kan i sin tur innebära att den samhällsviktiga tjänsten i sin helhet får en minskad kapacitet.

Ibland finns det dessutom alternativa sätt att bedriva verksamhet inom de olika funktionerna. Exempelvis kan en störning som innebär att patientjournaler inte är tillgängliga hanteras genom att information om patienter samlas in och delas på annat sätt.

Frågan: Bedömer ni att den samhällsviktiga/digitala tjänsten kan/kunde tillhandahållas medan störningen pågår/pågick?

Svara ”Ja, med full funktionalitet” om:

Alla de delar eller funktioner som utgör den samhällsviktiga eller digitala tjänsten kan bedriva verksamhet eller kan användas (även om verksamheten bedrivs på alternativa sätt, och även om det bara är med en lägre kapacitet än i normalfallet) och tjänsten därmed, i sin helhet, kan bedrivas.

Exempel: En incident har inneburit att journaler, biomedicinska analysresultat och annat som hämtas inom nätverket på ett sjukhus (temporärt) går att hämta, men med en lång fördröjning. Då går vården kanske att bedriva, men under tiden som störningen pågår så kanske inte lika många patienter kan behandlas som under normalläget, och alternativa arbetssätt kanske måste tillämpas inom akutsjukvården exempelvis. I det här fallet har den samhällsviktiga tjänsten inte förlorat i funktionalitet, men däremot har dess *kapacitet* minskat.

Svara ”Ja, med viss begränsning i funktionalitet” om:

Några av de delar eller funktioner som utgör den samhällsviktiga eller digitala tjänsten inte kan bedriva verksamhet eller inte kan användas, och det resulterar i att den samhällsviktiga tjänsten kan tillhandahållas med *vissa* begränsningar.

Exempel: En incident har inneburit att det (temporärt) inte går att komma åt journaler. Då går vården kanske att bedriva (om än med lägre kapacitet) om informationen går att inhämta och dela på andra sätt, men vissa patienter som behöver intensivvård kanske måste flyttas till andra vårdgivare.

Svara ”Ja, med stor begränsning i funktionalitet” om:

Flera av de delar eller funktioner som utgör den samhällsviktiga eller digitala tjänsten inte kan bedriva verksamhet eller inte kan användas, och det resulterar i att den samhällsviktiga tjänsten kan tillhandahållas med *stora* begränsningar.

Exempel: En incident har inneburit att det (temporärt) inte går att komma åt vare sig journaler, röntgenbilder eller biomedicinska analysresultat. I det fallet kanske vård kan bedrivas i en mycket begränsad utsträckning.

Svara ”Nej” om:

Det inte går att bedriva verksamhet inom eller använda sådana delar av eller funktioner inom den samhällsviktiga eller digitala tjänsten som är nödvändiga för att den överhuvudtaget ska kunna tillhandahållas.

Var i Sverige användare av tjänsten påverkas negativt av störningen

MSB använder sig av NUTS-systemet för att geografiskt lokalisera störningar. Systemet är framtaget av Eurostat (det europeiska statistikorganet) och används i Sverige av bl.a. Statistiska centralbyrån. För att se en karta över hur områdesindelningen ser ut, klicka här.

Frågan besvaras genom att rapportören successivt arbetar sig nedåt i en trädstruktur. Det är alltid **enbart** det eller de svar som anges längst ned i strukturen som räknas. Vill man exempelvis ange att man är säker på att användare av den samhällsviktiga tjänsten påverkas i hela Hallands län och är osäker men tror att användare också påverkas i Växjö kommun så svarar man:

I kolumnen för säkra bedömningar: ☒ Delar av landet → ☒ Västsverige → ☒ Hallands län
I kolumnen för osäkra bedömningar: ☒ Delar av landet → ☒ Småland med öarna → ☒ Kronobergs län → Skriv "Växjö kommun" i fritextfältet.

Om man istället bara vore säker på att vissa kommuner i Halland (exempelvis Laholm, Halmstad, Hylte och Falkenberg) påverkas av störningen, samtidigt som man är mer osäker på de övriga kommunerna, så skulle det korrekta sättet att svara på vara:

I kolumnen för säkra bedömningar: ☒ Delar av landet → ☒ Västsverige → ☒ Hallands län → Skriv "Laholms kommun, Halmstads kommun, Hylte kommun, Falkenberg kommun" i fritextfältet.
I kolumnen för osäkra bedömningar: ☒ Delar av landet → ☒ Småland med öarna & ☒ Västsverige → ☒ Kronobergs län & ☒ Hallands län → Skriv "Kungsbacka kommun, Varberg kommun, Växjö kommun" i fritextfältet.

VIKTIGT! Svaret ”Okänt” ska inte kombineras med något annat svar.

Gränsöverskridande konsekvenser av störningen

Förmågan att upptäcka och effektivt hantera gränsöverskridande konsekvenser betonas särskilt i NIS-direktivet. Exempel på gränsöverskridande konsekvenser av en *störning* kan vara att el som produceras i Sverige för konsumtion i Danmark kanske inte kommer att kunna levereras då produktionen ligger nere under en störning.

VIKTIGT! MSB kan komma att använda informationen om vilka länder som påverkas av gränsöverskridande konsekvenser för att kontakta våra motparter inom NIS-samarbetet och informera dem. MSB tar inte en kontakt med utomstående utan att först informera rapportören.

Påverkan på samhällets skyddsvärden

Det svenska krisberedskapssystemet är strukturerat kring värnandet av ett antal samhälleliga skyddsvärden. Inom NIS-sammanhang är i synnerhet de tre utpekade skyddsvärdena av särskild vikt. Påverkan på skyddsvärden är viktigt för att kunna avgöra allvarlighetsgraden hos en störning i en samhällsviktig tjänst.

Det kan vara så att det är enklare att ha en uppfattning om påverkan på vissa av de efterfrågade skyddsvärdena än andra. Exempelvis kan leverantörer av samhällsviktiga tjänster inom hälsa och sjukvård ha enklare att svara på om människors hälsa påverkas negativt av störningen, men ha svårare att bedöma påverkan på användarnas ekonomi. I ett sådant fall kan det vara lämpligt att välja något av ja-svaren för Människors hälsa, och sedan Kan ej bedöma om påverkan på Användarnas ekonomi.

Typer av incidenter

I lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster definieras en incident som ”en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem”. Således kan händelser som räknas som incidenter dels uppstå *i* nätverk eller informationssystem, och dels *utanför* dem, i vad vi här kallar för deras ”kringmiljö”. Det avgörande för att händelsen i nätverket eller systemet, eller i kringmiljön, ska räknas som en *incident* är att händelsen har medfört en ”faktisk negativ inverkan på säkerheten i nätverk och informationssystem”, d.v.s. att händelsen har haft minst en konsekvens som negativt har påverkat säkerheten i nätverk eller informationssystem.

Frågorna är uppdelade så att den som rapporterar först får beskriva händelsen som inträffat, och därefter får beskriva den eller de konsekvenser som händelsen har medfört som innebär att säkerheten i informationssystem eller nätverk har påverkats negativt, d.v.s. det som gör att händelsen enligt lagens definition är en incident.

Genom att välja ”Incident i system eller nätverk” kommer man vidare till en fråga om vad det är för slags incident som har inträffat i systemet/n eller nätverket/n. Genom att välja ”Incident i kringmiljö” kommer man vidare till en fråga om vad det för slags incident som har inträffat i kringmiljön (svarsalternativen ger också ledning om hur begreppet ”kringmiljö” här ska förstås).

Det är också viktigt att notera att modellen skiljer på incidenten i sig, och orsaken eller orsakerna till att incidenten inträffade. Exempelvis kan en webbsida gå ner i samband med att den mottar stora mängder trafik. Det kan ske genom att webbsidan får många anrop, och anropen kan dels komma från enheter som på helt legitima grunder försöker ansluta till sidan, såväl som från enheter som används för att slå ut den. Om det vid närmare efterforskningar visar sig att stora delar av mängden anrop skickades i antagonistiskt (illvilligt) syfte kan vi sluta oss till att ett angrepp *orsakade* incidenten. Angreppet är därför incidentens orsak, inte incidenten i sig.

Incidenter i kringmiljön

En incident i kringmiljön är när det händer något i kringmiljön och det leder till minst en negativ konsekvens för informationssystem eller nätverk, eller informationen i informationssystem eller nätverk.

Incident i värmehållning eller kylning	När det blir för varmt eller för kallt (exempelvis vid avbrott i fjärrkyla)
Incident i klimat	När det blir för fuktigt eller för torrt (exempelvis vid kraftig kondensbildning)
Incident i lokal	När det sker något i en lokal där informationssystem eller nätverk är fysiskt placerade (exempelvis brand eller översvämning)
Incident i korrekt tid-, takt- eller positionsförsörjning	När det inte kommer in förväntad sådan försörjning, eller om det kommer in felaktig sådan försörjning (exempelvis felaktiga tidsuppgifter)
Incident i energitillförsel	När det inte kommer in sådan tillförsel, eller om det kommer in felaktig sådan tillförsel (exempelvis vid elavbrott, eller spänningsfall)
Incident i förbindelse	När förbindelser avbryts, eller störs (exempelvis när en fiberkabel går sönder vid underhållsarbete)

Antagonistiskt syfte

När incidentens orsak ska anges i Skede 2 i formulären för samhällsviktiga respektive digitala tjänster så kan den som rapporterar ange att incidenten orsakades av en mänsklig handling. Om det anges får den som rapporterar sedan svara på om handlingen utfördes i antagonistiskt (illvilligt) syfte. Det finns åtminstone fyra typer av antagonistiskt syfte som en angripare kan ha:

1. Förhindra förmedling av nytta (för den som utsätts eller via den som utsätts)
2. Orsaka skada (för den som utsätts eller andra via den som utsätts)
3. Förhindra förmedling av skada (för den som angriper eller andra)
4. Orsaka vinning (för den som angriper eller andra)

Kategorierna kan ibland överlappa varandra. Exempelvis kan en överbelastningsattack utföras i syfte att ta ner en webbsida för att förhindra användarna av sidan från att komma åt den (punkt 1 ovan), samtidigt som den utförs i syfte att skada ägaren av webbsidan (punkt 2 ovan). Ett annat exempel är att spionera på en organisation i syfte att få tag i insiderinformation för att kunna sälja aktieinnehav vid en tidpunkt när det har ett högt värde (punkt 4 ovan) och innan insiderinformation som pekar på vikande resultat redovisas för omvärlden och gör att aktiekursen sjunker (punkt 3 ovan).

Hanteringsåtgärder

Alla leverantörer av samhällsviktiga omfattas av föreskriftskrav på ett systematiskt informationssäkerhetsarbete. Leverantörer av digitala tjänster omfattas av säkerhetskrav i Kommissionens genomförandeförordning (EU) 2018/151. I det ingår att ha en incidenthanteringsprocess med vissa standardinslag (såsom att felsöka, eskalera incidenten för att skaffa mer resurser, informera ledningen, etc.). Sådana standardinslag behöver inte rapporteras. Åtgärder som genomförs *utöver* de standardinslagen ska däremot rapporteras.

Exempel på sådana särskilda hanteringsåtgärder kana vara att ta in konsultstöd för att hantera incidenten, att genomföra en särskild kommunikationsinsats för att informera kunder eller allmänheten om incidenten eller störningen eller att genomföra större omstarter eller ominstallationer av infrastruktur.

Exempel på hur frågorna i Skede 2 kan besvaras utifrån en fiktiv incident

Exempel: En webbsida går ner i samband med att den mottar stora mängder trafik

Typ av incident

I vad har incidenten inträffat?

Svar: Incident i system eller nätverk

Vilken typ av system eller nätverk är det?

Svar: Övrigt system eller nätverk

Vilken typ, eller vilka typer, av incident är det?

Svar: Överbelastningsincident

Beskriv incidenten utförligt:

Här beskriver rapportören incidenten med egna ord i fritext.

Incidentens konsekvenser

Beroende på vad det innebär att webbsidans server har överbelastats (om det är det som har hänt) kan följande svar vara de rätta att ange om incidentens konsekvenser:

Har incidenten påverkat era systems eller nätverks…

Tillgänglighet?	**Riktighet?**	**Konfidentialitet?**
Tillgång för behöriga kan inte upprättas, Avbrott har uppstått i behörigas befintliga tillgång, Information kan inte tas emot från behöriga användare,	Riktigheten har inte påverkats negativt	Konfidentialiteten har inte påverkats negativt

Information från behöriga användare kan inte behandlas, Information från behöriga användare kan inte skickas, Uppgifter utförs inte på behörigas begäran, Systemet eller nätverket utför inte uppgifter det konfigurerat att utföra, Systemet eller nätverket kan inte konfigureras på behörigas begäran		

Har incidenten negativt påverkat er information?

Svar: Ja, information som är viktig för användare av våra tjänster

Har incidenten påverkat er informations…

Tillgänglighet?	**Riktighet**?	**Konfidentialitet**?
Tillgång för behöriga kan inte upprättas till information, Avbrott har uppstått i behörigas befintliga tillgång till information	Riktigheten hos information har inte påverkats negativt	Konfidentialiteten hos information har inte påverkats negativt

Beskriv incidentens konsekvenser:

Här beskriver rapportören incidentens konsekvenser med egna ord i fritext.

Orsakerna till incidenten

Om rapportören genom efterforskningar har kunnat fastställa att stora delar av trafiken som skickats till webbsidan har skickats i antagonistiskt (illvilligt) syfte från ett antal olika enheter skulle följande svar kunna vara de rätta att ange om incidentens orsaker:

Vad bedömer ni att incidenten orsakades av?

Svar: Mänsklig handling

Vem bedömer ni orsakade incidenten?

Svar: Utomstående

Bedömer ni att syftet var antagonistiskt?

Svar: Ja

Har ni polisanmält incidenten?

Svar: Ja

Vad för slags angrepp var det som orsakade incidenten?

Svar: DDoS

Huruvida information om det inträffade har eller kommer att rapporteras till någon annan myndighet

I början av Skede 3 i incidentrapporteringsformulären för samhällsviktiga respektive digitala tjänster har den som rapporterar möjlighet att ange om det inträffade har eller kommer att rapporteras till någon annan myndighet. Syftet med frågan, som är frivillig att besvara, är att upprätta en bild över vilka incidentrapporteringskrav som överlappar med incidentrapportering enligt NIS-regleringen.

För att besvara frågan anges *Har rapporterats* eller *Ska rapporteras* under Status, myndighetens namn under Rapporteringen sker till, regelverkets namn under Regelverk och diarienumret som rapporten registrerats under om statusen är Har rapporterats. Om statusen är Ska rapporteras så anges bara ett ”-”.

Hot och sårbarheter

Hot definieras i modellen för incidentrapporteringen som:

> Något som orsakar eller bidrar till att orsaka att:
> 1. En incident inträffar
> 2. Konsekvenserna av en incident förvärras

Två specialfall pekas också ut:

> Något som orsakar eller bidrar till att orsaka att:
> 3. Störningar inträffar när incidenter inträffar
> 4. Konsekvenserna av störningar förvärras

Hoten kan vara av olika typer. De kan vara av antagonistisk art i form av människor som agerar i illvilligt syfte – antingen genom att med sitt handlande orsaka en incident (punkt 1 ovan), eller att vid en incident agera på ett sätt som förvärrar incidenten (punkt 2 ovan). Hoten kan också vara av annan art, exempelvis naturliga hot såsom solstormar (punkt 1 och 2 ovan) eller tekniska hot där teknologi antingen orsakar att incident uppstår, eller förvärrar den efter det att den uppstått.

Se exemplet nedan för en beskrivning av hur man kan tänka på hot och sårbarheter utifrån definitionerna i modellen.

Sårbarheter definieras i modellen för incidentrapporteringen som:

> Avsaknad av något som skulle kunna:
> 5. Förhindra eller bidra till att förhindra att en incident inträffar
> 6. Förhindra eller mildra eller bidra till att förhindra eller mildra konsekvenserna av incidenter

Även här pekas specialfall ut:

> Avsaknad av något som skulle kunna:

7. Förhindra eller bidra till att förhindra att en störning inträffar när en incident inträffar
8. Förhindra eller mildra eller bidra till att förhindra eller mildra konsekvenserna av störningar

Även sårbarheterna kan vara av olika art. De kan vara personliga i form av individuell kunskapsbrist, exempelvis när kunskaper om hur man ska förhålla sig till misstänkt phishing saknas (punkt 5 ovan), organisatoriska i form av brist på ledning, styrning eller struktur (punkt 5 eller 6 ovan), tekniska i form av avsaknad av korrekt konfigurerade brandväggar (oftast punkt 5, men ibland även punkt 6 ovan) eller bristfällig nätverkssegmentering (främst punkt 6 ovan), fysiska i form av avsaknad av brandskydd eller klimatanläggning (främst punkt 5 ovan).

Exempel på hur en incident kan beskrivas och analyseras med hot och sårbarheter

Exempelincident: Rörläckage uppstår i en serverhall och vatten rinner in i rummet. Fem av åtta servrar slutar att fungera.

Servrarna i hallen står uppställda två och två på höjden, på ställningar, 1 m ovanför golvet.

När rörläckaget upptäcks har vattennivån stigit till 1,05m ovanför golvet och når därför till de fyra servrarna som står närmast golvet på ställningarna. När incidenten har hanterats och en utvärdering ska göras kan följande konstateras:

Hot – Något som orsakar eller bidrar till att orsaka att:	
En incident inträffar	**Konsekvenserna av en incident förvärras**
Vattenrör finns i väggen intill serverrummet	Det fanns en propp i golvbrunnen som förhindrade avrinning och hade kunnat innebära att vattennivån steg även till de övre servrarna
Vattnet i röret är varmt och ångar varför fara för servrarna uppstår direkt när vattnet kommer in i serverhallen	Det fanns lådor på golvet vilket gjorde att vattennivån steg fortare än den annars skulle ha gjort
Sårbarheter – Avsaknad av något som skulle kunna:	
Förhindra eller bidra till att förhindra att en incident inträffar	**Förhindra eller mildra eller bidra till att förhindra eller mildra konsekvenserna av incidenter**
Avsaknad av vattensensor som skulle kunna varna om att vatten förekommer i serverhallen	Avsaknad av vattensensor som skulle kunna varna om att vatten förekommer i serverhallen
Avsaknad av underhåll av vattenrören som hade inneburit att röret hade bytts ut innan de sprack	Avsaknad av fuktsensor som skulle kunna varna om onormalt höga nivåer av fukt förekommer i serverhallen
Svaga väggar som inte kunde motstå vattentrycket	
Inga avledningsrör i väggen som hade kunnat leda bort vattnet när väl rörledningen sprack	

Utifrån den ovanstående uppställningen kan vi förklara hur *fem* servrar kunde sluta fungera. Fyra servrar slutade antingen fungera på grund av den höga fuktnivån *eller* för att vattennivån nådde hela vägen upp till dem. Den femte servern som slutade fungera nåddes aldrig av vattennivån, utan slutade förmodligen fungera p.g.a. den höga nivån av fukt.

Att incidenten ens kunde uppstå, d.v.s. att det varma vattnet kunde hamna i serverhallen orsakades av att det sitter ett vattenrör i serverhallens vägg och att det gick sönder. Incidenten hade kunnat undvikas om underhåll hade genomförts när det började bli dags för det. Serverhallen *i sig* var dessutom sårbar då den har svaga väggar, och saknar avledningsrör. Vattennivån kunde nå så högt innan den upptäcktes dels för att golvbrunnen var blockerad av en propp, och dels för att det saknas en vattensensor som kan varna när det kommer in flytande vatten i lokalen. Fuktnivån kunde också förekomma länge innan den upptäcktes då det saknas en fuktsensor.

I incidentrapporteringsformulären skulle incidenten beskrivits som en incident i kringmiljö av typen *incident i klimat* och *incident i lokal*. Konsekvenserna för informationssystem och nätverk skulle förmodligen vara:

Tillgänglighet?	**Riktighet**?	**Konfidentialitet**?
Tillgång för behöriga kan inte upprättas, Avbrott har uppstått i behörigas befintliga tillgång, Information kan inte tas emot från behöriga användare, Information från behöriga användare kan inte behandlas, Information från behöriga användare kan inte skickas, Uppgifter utförs inte på behörigas begäran, Systemet eller nätverket utför inte uppgifter det konfigurerat att utföra, Systemet eller nätverket kan inte konfigureras på behörigas begäran	Riktigheten har inte påverkats negativt	Konfidentialiteten har inte påverkats negativt

Konsekvenserna för information skulle förmodligen vara:

Tillgänglighet?	**Riktighet**?	**Konfidentialitet**?
Tillgång för behöriga kan inte upprättas till information,	Riktigheten hos information har inte påverkats negativt	Konfidentialiteten hos information har inte påverkats negativt

Avbrott har uppstått i behörigas befintliga tillgång till information		

Förebyggande åtgärder

Förebyggande åtgärder definieras i modellen för NIS-incidentrapporteringen som åtgärder som åtgärdar hoten som driver fram incidenter eller störningar, eller som åtgärdar sårbarheterna som innebär att incidenter eller störningar inte stoppas. Frågan om vilken den avsedda effekten med åtgärden är speglar därför uppställningen med hot och sårbarheter ovan. Då hot är saker som finns syftar åtgärder som förbygger hot till att ta bort eller förändra hoten. Då sårbarheter är avsaknad av något syftar åtgärder som förebygger sårbarheter till att införskaffa eller införa sådant som kan täcka upp för det som saknas.

Fortsättning på det tidigare exemplet: Förebyggande åtgärder mot de identifierade hoten och sårbarheterna

Tabellen nedan är samma som användes i exemplet ovan, men nu kompletterat med möjliga åtgärder:

Hot – Något som orsakar eller bidrar till att orsaka att:	
En incident inträffar	**Konsekvenserna av en incident förvärras**
Vattenrör finns i väggen intill serverrummet **Förebyggande åtgärd**: Ta bort (eller flytta) vattenröret så att det inte längre sitter i serverrummets vägg.	Det fanns en propp i golvbrunnen som förhindrade avrinning och hade kunnat innebära att vattennivån steg även till de övre servrarna **Förebyggande åtgärd**: Ta bort proppen. Kan kombineras med en åtgärd som gör att det blir svårare för proppar att bildas.
Vattnet i röret är varmt och ångar varför fara för servrarna uppstår direkt när vattnet kommer in i serverhallen **Förebyggande åtgärd**: Ta bort (eller flytta) vattenröret så att det inte längre sitter i serverrummets vägg. Om det inte går, se över möjligheterna att ändra så att det är kallvatten som leds i röret istället.	Det fanns lådor på golvet vilket gjorde att vattennivån steg fortare än den annars skulle ha gjort **Förebyggande åtgärd**: Ta bort lådorna. Kan kombineras med att införa nya rutiner för var saker får förvaras.
Sårbarheter – Avsaknad av något som skulle kunna:	
Förhindra eller bidra till att förhindra att en incident inträffar	Förhindra eller mildra eller bidra till att förhindra eller mildra konsekvenserna av incidenter
Avsaknad av vattensensor som skulle kunna varna om att vatten förekommer i serverhallen **Förebyggande åtgärd**: Införskaffa en vattensensor.	Avsaknad av vattensensor som skulle kunna varna om att vatten förekommer i serverhallen **Förebyggande åtgärd**: Införskaffa en vattensensor.

Avsaknad av underhåll av vattenrören som hade inneburit att röret hade bytts ut innan de sprack **Förebyggande åtgärd**: Inför löpande underhåll av vattenrören (oavsett om de blir kvar i serverrummets väggar eller inte).	Avsaknad av fuktsensor som skulle kunna varna om onormalt höga nivåer av fukt förekommer i serverhallen **Förebyggande åtgärd**: Införskaffa en fuktsensor.
Svaga väggar som inte kunde motstå vattentrycket **Förebyggande åtgärd**: Införskaffa förstärkning av väggarna in mot serverhallen.	
Inga avledningsrör i väggen som hade kunnat leda bort vattnet när väl rörledningen sprack **Förebyggande åtgärd**: Införskaffa och utrusta väggarna med avledningsrör.	