FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Incidentrapportering för betaltjänstleverantörer och annan finansiell verksamhet

– Kravbild och gemensamma nämnare

2019-12-16
FSPOS Arbetsgrupp Kontinuitetssäkring

Inledning

Samhället i stort, liksom den finansiella sektorn, digitaliseras allt mer, vilket bidrar till bättre samhällstjänster, exempelvis i termer av effektivitet och kostnadsbesparingar. Detta innebär samtidigt att viktiga samhällsfunktioner blir kraftigt beroende av it. Europaparlamentet skriver bland annat att ”Nätverks- och informationssystem spelar en viktig roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion.”[1]. Med digitalisering följer exponering mot it-relaterade störningar som kan drabba privatpersoner, organisationer, grundläggande samhällsfunktioner och Sveriges säkerhet. I syfte att få kunskap om händelser som får negativ påverkan på information, nätverk och informationssystem och för att kunna stärka samhällets robusthet, har flera incidentrapporteringsregelverk antagits den senaste tiden. Detta PM handlar om dessa regelverk, som alla är tillämpbara för betaltjänstleverantörer i den finansiella sektorn.

Frågan om informations- och cybersäkerhet och förmågan att hantera it-incidenter har lyfts på högsta EU-nivå av avgående EU-kommissionsordförande Jean-Claude Junker, som vid sitt årliga State of the Union Address sade: "In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks.[2]"

Förutom att incidentrapportering är reglerat i lag, är det också en viktig del i organisationers systematiska informationssäkerhetsarbete. Vid hantering av incidenter och förebyggande åtgärder är effektiv incidentrapportering centralt. Störst effekt uppnås om organisationer kan arbeta med proaktiva incidentrapporteringsprocesser och rutiner ur ett helhetsperspektiv, samt dra nytta av de gemensamma nämnare som förenar olika incidentrapporteringsramverk.

Syfte

Dokumentets syfte är att beskriva de krav på incidentrapportering som träffar framförallt betaltjänstleverantörer och som finns i de nyligen införda regelverken GDPR, PSD2, NIS-direktivet och Säkerhetsskyddslagen, samt att identifiera gemensamma nämnare i de olika regelverken. Även aktörer som levererar tjänster inom sektorn finansmarknadsinfrastruktur enligt MSBFS 2018:7[3] kan ha viss nytta av dokumentet, då de regelverk som behandlas i detta dokument utom PSD2 är relevanta även för dem.

---

[1] Europaparlementets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (1)

[2] European Commission - Press release, State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks, Brussels, 19 September 2017

[3] MSBFS 2018:7 - Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster

Metod och avgränsning

I arbetet med att ta fram underlag till detta PM har en skrivbordsstudie genomförts. Studien baserar sig på inventering av öppna källor och intervjuer. I skrivbordsstudien har enbart rapportering till centrala myndigheter i Sverige analyserats. Hur kunder och användare ska informeras har inte analyserats och kommer inte presenteras vidare.

Regelverkens kravbild – en summering

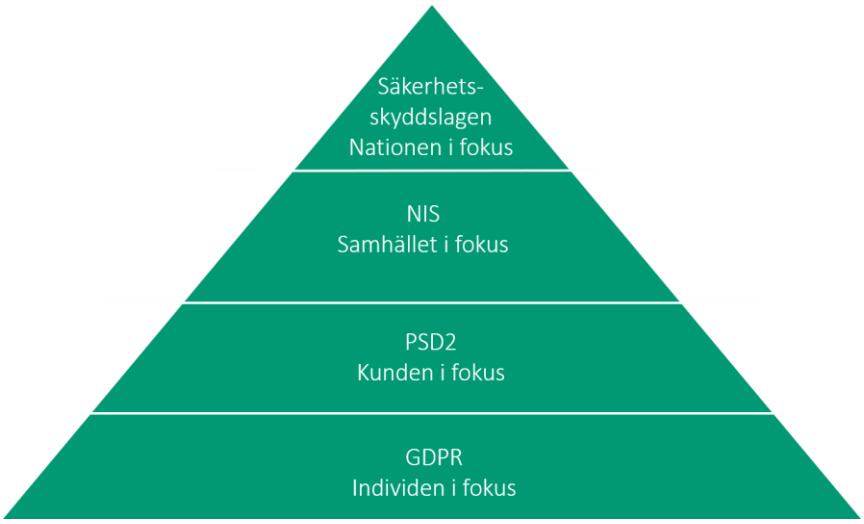
Allt eftersom samhället digitaliseras ökar behovet av att stärka informationssäkerheten för att skydda den personliga integriteten, samhällsviktiga funktioner och också Sveriges säkerhet. Under de senaste tio åren har ett antal nya eller uppdaterade regelverk trätt ikraft som ställer krav på samhällets aktörer att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete och att rapportera incidenter till berörda myndigheter.

Dataskyddsförordningen, GDPR, som trädde i kraft i maj 2018, ställer krav på samhällets alla organisationer rörande behandling av personuppgifter. Dessa krav ska stärka skyddet för privatpersoner. Incidentrapportering ska ske till Datainspektionen.

Det andra betaltjänstdirektivet, PSD2, som trädde i kraft i januari 2018, ställer krav på betaltjänstleverantörer rörande bland annat informationssäkerhet. Dessa krav ska skydda leverantörernas kunder. Incidentrapportering ska ske till Finansinspektionen.

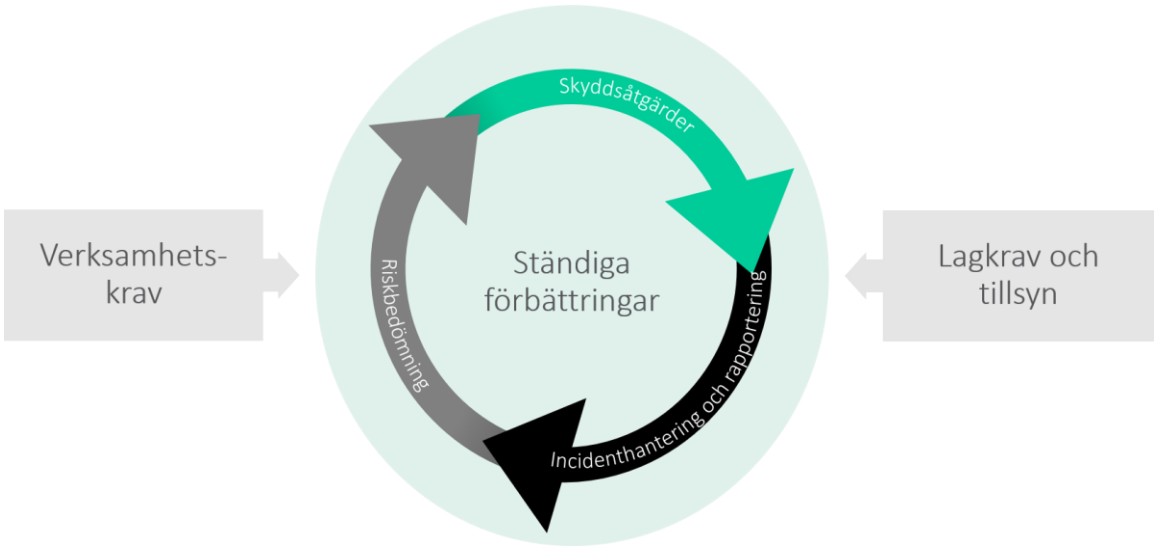
Nät- och informationssäkerhetslagen, NIS-lagen, som trädde i kraft i augusti 2018, ställer krav på leverantörer av samhällsviktiga tjänster och leverantörer av vissa digitala tjänster att vidta säkerhetsåtgärder för att skydda sina nätverk och informationssystem. Dessa krav ska skydda samhället i stort. Incidentrapportrering ska ske till Myndigheten för samhällsskydd och beredskap som i sin tur utan dröjsmål tillgängliggör informationen för Finansinspektionen avseende sektorn bankverksamhet och finansmarknadsinfrastruktur.

Säkerhetsskyddslagen uppdaterades och trädde i kraft i april 2019 och ställer bl.a. informationssäkerhetskrav på verksamheter som har betydelse för Sveriges säkerhet. Incidentrapportering ska ske till Säkerhetspolisen.



Figur 1 – Säkerhetsregelverk i sina sammanhang

Trots skyddsåtgärder kommer incidenter att ske och för att lära sig av dem behövs kunskap om dem hos berörda aktörer och i samhället. Den obligatoriska incidentrapporteringen, som bör vara en integrerad del av organisationens systematiska informationssäkerhetsarbete, ger underlag till förbättrad riskbedömning och justerade eller nya skyddsåtgärder. Med tryck från verksamhetskrav, lagkrav och tillsyn, ger detta sammantaget förutsättningar för en uppåtgående spiral av lärande och ständiga förbättringar.



Figur 2 – Systematiskt informationssäkerhetsarbete

En utmaning för de finansiella aktörerna som träffas av de olika regelverken, är att incidentrapporteringsramverken har olika ursprung och syften. Det medför att de ställer olika krav på vilka incidenter som är rapporteringspliktiga, när och hur rapportering ska ske, till vem och vad rapporterna ska innehålla. Incidentrapporteringskraven kan dessutom se väldigt olika ut i olika länder beroende på reglering, vilket blir en extra utmaning för de aktörer som har nationsöverskridande verksamhet.

Dataskyddsförordningen (GDPR)

"Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet" skriver Europaparlementet[4]. GDPR trädde i kraft 25 maj 2018 och syftar som Europaparlamentet skriver till att skydda medborgarnas grundläggande rättigheter och friheter. Särskilt, skriver datainspektionen, är GDPR en förordning som skyddar enskilda personers rätt till skydd av personuppgifter[5].

Genom GDPRs krav och rapportering upprättas en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU. Den information som inkommer genom incidentrapporter beskriver riskbilden och vanliga incidentorsaker i Sverige och Europa. Enligt Datainspektionen gör rapporteringen det möjligt för myndigheten att bland annat bevaka vad de personuppgiftsansvariga gör för att motverka negativa effekter. Om det blir nödvändigt kan myndigheten också utöva sina tillsynsbefogenheter för att få personuppgiftsansvariga att vidta nödvändiga åtgärder[6]. Det oberoende rådgivande EU-organet i frågor rörande dataskydd och integritet, den så kallade Artikel 29-arbetsgruppen, och som i maj 2018 ersattes av EDPB, The European Data Protection Board, anger i sina riktlinjer för rapportering av personuppgiftsincidenter att när personuppgiftsansvaraig anmäler en incident till tillsynsmyndigheten kan de få råd om huruvida de individer som påverkas måste informeras[7]. Genom att meddela enskilda att en incident har inträffat kan den personuppgiftsansvarige informera dessa om vilka risker incidenten medför och vilka åtgärder de kan vidta för att skydda sig mot potentiella konsekvenser. Vidare menar Artikel 29-arbetsgruppen att anmälan av incidenter bör integreras i personuppgiftsansvariges incidenthanteringsplaner och ses som ett verktyg för att skydda enskilda och deras personuppgifter. EU-förordningen möjligör verksamhetsgranskningar i syfte att säkerställa tillräckliga processer och skydd av personuppgifter. En sådan granskning genomfördes redan fem månader efter att lagen trätt i kraft[8].

Vilka incidenter ska rapporteras?

Enligt förordningen ska en organisation rapportera alla personuppgiftsincidenter, vilket definieras som[9]

"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."

Enligt artikel 29-arbetsgruppen kan dessa personuppgiftsincidenter kategoriseras utifrån tre informationssäkerhetsprinciper[10].

---

[4] Europaparlementets och rådets direktiv (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
[4] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, sid 7
[5] https://www.datainspektionen.se/vagledningar/en-introduktion-till-dataskyddsforordningen/
[6]https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/personuppgiftsincident/
[7] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s. 5.
[8] https://www.datainspektionen.se/nyheter/2018/forsta-svenska-gdpr-granskningen-klar/
[9] Dataskyddsförordningen, 4.12

- ”Konfidentialitetsbrott” – vid obehörigt eller oavsiktligt röjande av eller åtkomst till personuppgifter.
- ”Integritetsbrott” – vid obehörig eller oavsiktlig ändring av personuppgifter.
- ”Tillgänglighetsbrott” – vid obehörig eller oavsiktlig förlust av åtkomst till, eller förstöring av, personuppgifter.

Utöver personuppgiftsincidentdefinitionen och de tre principerna saknas tröskelvärden för rapportering. En personuppgiftsincident som faller inom ovan definition ska bedömas utifrån vilka effekter incidenten riskerar att få för enskilda. Artikel 29-arbetsgruppen rekommenderar att bedömningen tar hänsyn till följande kriterier [11] :

- Typen av incident,
- Personuppgifternas natur,
- Känslighet och volym,
- Hur lätt det är att identifiera enskilda personer,
- Konsekvensernas svårighetsgrad för enskilda personer,
- Den enskildes speciella egenskaper,
- Den personuppgiftsansvariges speciella egenskaper,
- Antalet personer som påverkas och
- Allmänna aspekter.

Om det är osannolikt att incidenten medför en risk för fysiska personers fri- och rättigheter, behöver incidenten inte anmälas till Datainspektionen. Det samma gäller om personuppgifterna som incidenten rör är oläsbara för obehöriga genom kryptering och krypteringsnyckelns säkerhet inte har äventyrats[12].

När ska det rapporteras?

Organisationers personuppgiftsansvarige ska anmäla personuppgiftsincidenter[13]:

> *1. utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den*

Tidskravet för rapportering gäller enbart om det inte är osannolikt att rapportering medför en risk för fysiska personers rättigheter och friheter (se ”Vilka incidenter ska rapporteras?”). Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen. Om det inte är möjligt att tillhandahålla all

[10] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, sid 8
[11] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s 25-26
[12] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s 20
[13] Dataskyddsförordningen, 33.1

informationen samtidigt får den tillhandahållas i omgångar utan onödigt ytterligare dröjsmål[14].

Vetskapsformuleringen har betydande vikt då den styr tidsramen för när rapportering ska ske. 72 timmar räknas från den tidpunkt organisationen fått vetskap om incidenten, inte från när den faktiskt skett. Vetskap anses en personuppgiftsansvarig ha fått när den denna är rimligt säker på att en säkerhetsincident har ägt rum som har medfört att personuppgifter äventyrats[15]. Det framgår dock av förordningen att organisationer bör ha sådana tekniska skyddsåtgärder och lämpliga organisatoriska åtgärder för att omedelbart kunna fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade[16]. En organisation bör alltså ha såväl system och organisatorisk förmåga att snabbt kunna identifiera, analysera och bedöma en personuppgiftsincident. Hänsyn ska också tas till personuppgiftsincidentens art och svårighetsgrad samt dess följder och negativa effekter för den registrerade.

Innan personuppgiftsansvarig antas ha fått vetskap om att en rapporteringsskyldig personuppgiftsincident ägt rum får denna genomföra en kort undersökning för att analysera händelsen och utröna huruvida en incident ägt rum eller inte. Undersökning ska inledas så snart som möjligt och med en rimlig grad av säkerhet fastställa huruvida en incident har ägt rum. Vetskap om att incident inträffat får personuppgiftsansvarig först efter att undersökningen genomförts och alltså inte under tiden den genomförs[17].

Hur ska det rapporteras?

Personuppgiftsincidenter rapporteras[18]:

*genom att fylla i en blankett (*Anmälan av personuppgiftsincident *för en incident som enbart har inträffat i Sverige och enbart har drabbat registrerade i Sverige och* Anmälan av gränsöverskridande personuppgiftsincident *för en incidenten som har inträffat i flera länder eller påverkat registrerade i andra länder) och skicka den till Datainspektionen via brev*

Vad ska rapporteras?

Övergripande ska information om fyra områden rapporteras[19]:

---

[14] Dataskyddsförordningen, 33.1.
[15] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s 10-11
[16] Europaparlementets och rådets direktiv (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (87)
[17] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, sid 12
[18] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/anmala-personuppgiftsincident/hur-du-anmaler/
[19] Dataskyddsförordningen artikel 33, Anmälan av en personuppgiftsincident till tillsynsmyndigheten, 3. a-c.

1. beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
2. förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
3. beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
4. beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Strikt tolkat ska varje enskild personuppgiftsincident rapporteras. Med hänsyn till den arbetsbörda detta skulle innebära anges därför att personuppgiftsansvarig kan göra en så kallad samlad anmälan i de fall flera liknande incidenter inträffar under en relativt kort tidsperiod[20]. Oavsett hur rapportering sker ska personuppgiftsansvarige dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Syftet med detta är att göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av förordningen[21].

[20] Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s. 17
[21] Dataskyddsförordningen artikel 33, Anmälan av en personuppgiftsincident till tillsynsmyndigheten, s. 5

PSD2

I januari 2018 trädde EU:s andra betaltjänstdirektiv, PSD2, i kraft i Sverige[22]. Syftet med direktivet är att utveckla marknaden för elektroniska betalningar och skapa bättre förutsättningar för säkra och effektiva betalningar. Direktivet inför bl.a. nya bestämmelser som medför krav på en betaltjänsteleverantörs hantering av säkerhet och risker. Europeiska bankmyndigheten (EBA) har utfärdat riktlinjer för rapportering vid allvarliga incidenter enligt PSD2 [23]. Riktlinjerna innehåller bland annat information om hur man bör bedöma om en operativ incident eller säkerhetsincident ska anses allvarlig. Fr.o.m. maj 2018 gäller nya regler om rapporteringskrav för betaltjänstleverantörer genom Finansinspektionens föreskrifter om verksamhet för betaltjänsteleverantörer, FFFS 2018:4. Enligt föreskrifterna ska betaltjänsteleverantörer rapportera allvarliga operativa incidenter och säkerhetsincidenter till Finansinspektionen.

Genom de rapporteringskrav som åligger betaltjänstleverantörerna är syftet att bygga en motståndskraft inom den finansiella sektorn och som skyddar konsumenten. Kraven på betaltjänstleverantörer att underrätta Finansinspektionen om dessa incidenter utgör en del av det system med åtgärder, kontrollmekanismer och interna regelverk som ska finnas enligt 45 b kap. 1. § LBT[24]. Rapporteringen ställer vissa organisatoriska krav, som om de integreras i betaltjänsteleverantörernas systematiska informationssäkerhetsarbete, kan bidra till deras förebyggande arbete, samt hantering av och lärdomar från incidenter.

Inrapporterade PSD2-incidenter utgör ett viktigt underlag för Finansinspektionen vid kontakter med media och för att motverka ryktesspridning. Vidare genererar rapporteringen viktig incidentstatistik som tydliggör trender och sårbarheter för sektorn. Denna information delges berörda aktörer kontinuerligt och styr även Finansinspektionens tillsynsarbete genom en så kallad riskbaserad och systematisk tillsyn. På längre sikt syftar rapporteringen till att verka för en finansiell sektor som är mer motståndskraftig mot störningar i samhällsviktiga finansiella tjänster.

[22] (EU) 2015/2366
[23] EBA/GL/2017/10
[24] Remisspromemoria, FI Dnr 15-10584, 2018-01-30, 2.14

Vilka incidenter ska rapporteras?

Händelser som enligt föreskrifterna är rapporteringspliktiga är operativa incidenter eller säkerhetsincidenter, vilka definieras.[25] som:

"En enskild händelse eller en serie av sammanhängande händelser som inte har planerats av betaltjänstleverantören vilka har eller sannolikt kommer att få negativa effekter på betalningsrelaterade tjänster vad gäller integritet, tillgänglighet, konfidentialitet, autenticitet och/eller kontinuitet." .

För vetskap om en händelse faller inom ramen för vad som är rapporteringspliktigt måste organisationen 1) analysera om händelsen faller inom incidentens kriterium samt 2) avgöra om incidenten är allvarlig. Som underlag för beslut om huruvida incidenten är allvarlig används fördefinierade tröskelvärden[26], se *Tabell 1. Tröskelvärden PSD2*. En operativ incident eller säkerhetsincident är allvarlig om den uppfyller[27]:

a. ett eller flera av kriterierna för den "högre effektnivån", eller

b. tre eller flera av kriterierna för den "lägre effektnivån" .

Kriterier	Lägre effektnivå	Högre effektniv
Berörda transaktioner	> 10 % av betaltjänstleverantörens normala transaktionsnivå (vad gäller antalet transaktioner) > 100 000 euro	> 25 % av betaltjänstleverantörens normala transaktionsnivå (vad gäller antalet transaktioner) > 5 miljoner euro
Berörda betaltjänstanvändare	> 5 000 > 10 % av betaltjänstleverantörens betaltjänstanvändare	> 50 000 > 25 % av betaltjänstleverantörens betaltjänstanvändare
Driftavbrott	> 2 timmar	Ej tillämpligt
Ekonomiska effekter	Ej tillämpligt	> Max. (0,1 % av primärkapitalet,* 200 000 euro) > 5 miljoner euro
Hög intern upptrappningsnivå	Ja	Ja, och krisläge (eller liknande) kommer sannolikt

[25] EBA/GL/2017/10 (Punkt 14)
[26] EBA/GL/2017/10 Kap. 4, punkt 1.4
[27] EBA/GL/2017/10 Kap. 4, punkt 1.1

		att utlysas
Andra betaltjänstleverantörer eller relevanta infrastrukture som kan beröras	Ja	Ej tillämpligt
Effekter på anseendet	Ja	Ej tillämpligt

Tabell 1 - Tröskelvärden PSD2

I de fall en betaltjänstleverantör saknar tillräckliga faktiska uppgifter som stöd för sin bedömning av tröskelvärden uppmanas betaltjänstleverantören att göra en uppskattning under den inledande utredande fasen[28]. Vidare ska betaltjänstleverantörer kontinuerligt analysera och bedöma situationen under den tid incidenten pågår för att identifiera eventuella statusförändringar, antingen uppåt (från mindre allvarlig till allvarlig) eller neråt (från allvarlig till mindre allvarlig)[29].

När ska det rapporteras?

Betaltjänstleverantören ska rapportera allvarliga operativa incidenter eller säkerhetsincidenter i tre skeden enligt nedan tidsfrist[30]:

1. *inom fyra timmar efter det att incidenten upptäckts*
2. *med uppdaterad information när det finns sådan och senast inom tre dagar från det att uppgifterna enligt 1 har kommit in, och*
3. *senast två veckor efter det att verksamheten fungerar normalt igen.*

Begreppet *upptäckt* förtydligas inte vidare i de reglerande föreskrifterna.

För att identifiera och rapportera en operativ incident eller säkerhetsincident inom givna tidsfrister krävs att betaltjänstleverantören har såväl system som organisatorisk förmåga att agera inom de relativt korta tidsramarna. Denna förmåga innebär en välfungerande incidenthanteringsprocess med tydliga roller för eskalering och rapportering. Processen bör bara väldokumenterad med tydliga instruktioner, eskaleringsnivåer och beslutspunkter. Större organisationer bör även ta stöd i anpassade it-system för incidenthantering.

Hur ska det rapporteras?

På Finansinspektionens webbplats finns anvisningar om hur rapportering av allvarliga operativa incidenter eller säkerhetsincidenter ska ske[31]:

[28] EBA/GL/2017/10, Kap 4. Punkt 1.5
[29] EBA/GL/2017/10, Kap 4. Punkt 1.6
[30] FFFS 2018:4, 4 § Kap. 6
[31] https://www.fi.se/sv/bank/andra-betaltjanstdirektivet-psd-2/rapportering-enligt-andra-betaltjanstdirektivet-psd-2/

Leverantören ska då använda blanketter som finns på sidan Blanketter under rubriken Betaltjänster/Andra betaltjänstdirektivet (PSD 2).

Blanketten ska lämnas in med krypterad mejl till: incidentrapportering.betaltjanster@fi.se.

Som anges under rubriken ”När ska det rapporteras?” sker rapportering i tre etapper. Betaltjänstleverantören ska vid vardera av dessa tre tillfällen rapportera i en mall i tre delar, som alla efterfrågar olika typer av information. Anledningen till att mallen fylls i etappvis är att betaltjänsteleverantören rimligen har mer kunskap och information att rapportera allteftersom deras interna utredning framskrider.

Vad ska rapporteras?

Information om vad betaltjänstleverantören förväntas rapportera i de tre etapperna är kortfattat beskrivet nedan.

Inledande rapport (fyra timmar)

Den inledande rapporten ska innehålla information kopplat till rubrikerna:

1. Allmänna uppgifter och
2. Upptäckt av incidenten och inledande klassificering.

Genom information kopplat till dessa punkter rapporteras grundläggande uppgifter om incidenten och dess uppskattade effekter på grundval av den information som var tillgänglig direkt efter det att den upptäcktes eller omklassificerades. Betaltjänstleverantören ska även ange datum för nästa uppdatering i sin inledande rapport, vilket ska vara så snart som möjligt och under inga omständigheter senare än inom tre bankdagar[32].

Mellanliggande rapport (tre dagar)

Den mellanliggande rapporten innehåller information kopplat till rubrikerna

1. Allmänna uppgifter,
2. Klassificering av incidenten/information om incidenten,
3. Beskrivning av incidenten,
4. Incidentens effekter och
5. Begränsning av incidenten.

En mellanliggande rapport ska rapporteras varje gång betaltjänstleverantören får kännedom om ny, relevant information eller betydande förändringar sedan den föregående rapporten (t.ex. huruvida incidenten har trappats upp eller minskat i

[32] EBA/GL/2017/10, Kap 4. Punkt 2.10

betydelse, nya orsaker har identifierats eller åtgärder har vidtagits för att lösa problemet)[33].

Den första mellanliggande rapporten innehåller mer detaljerad beskrivning av incidenten och dess konsekvenser än den inledande rapporten. Vid samtliga rapporteringstillfällen ska betaltjänstoperatörer ange datum för nästa uppdatering[34].

Den sista mellanliggande rapporten ska skickas in när den reguljära verksamheten har återupptagits och driften är normal igen. Med normal drift menas när verksamheten/driften har återgått till samma servicenivå/villkor som definierats av betaltjänstleverantören eller fastställts externt genom ett avtal om servicenivå vad gäller behandlingstider, kapacitet, säkerhetskrav osv. och det inte längre föreligger några beredskapsåtgärder[35].

Slutrapport (två veckor efter normal verksamhet)

Slutrapporten innehåller information kopplat till rubrikerna

1. Allmänna uppgifter,
2. Analys av de grundläggande orsakerna och uppföljning och
3. Ytterligare information.

I slutrapporten ska betaltjänstleverantören försöka inkludera fullständig information, dvs. i) faktiska uppgifter om effekterna istället för uppskattningar (samt andra uppdateringar som krävs enligt avsnitten A och B i mallen) och ii) avsnitt C i mallen, vilket omfattar den grundläggande orsaken, om denna redan är känd, och en sammanfattning av vidtagna eller planerade åtgärder för att avhjälpa problemet och motverka att det återkommer i framtiden[36].

[33] EBA/GL/2017/10, Kap 4. Punkt 2.12
[34] EBA/GL/2017/10, Kap 4. Punkt 2.14
[35] EBA/GL/2017/10, Kap 4. Punkt 2.15
[36] EBA/GL/2017/10, Kap 4. Punkt 2.20

NIS

Direktivet om åtgärder för en gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) är ett EU-direktiv som infördes med anledning av det stora beroendet som samhällsviktiga funktioner har till nätverks- och informationssystem[37]. Direktivet började gälla 2016 och berör leverantörer av vissa digitala tjänster (molntjänster, sökmotorer och webbaserade marknadsplatser) samt leverantörer av samhällsviktiga tjänster. Dessa samhällsviktiga tjänster har delats upp i sju sektorer där de finansiella aktörer som berörs faller inom de två områdena Bankverksamhet och Finansmarknadsinfrastruktur. Därutöver berörs sektorerna Energi, Transporter, Hälso- och sjukvård, Leverans och distribution av dricksvatten samt Digital infrastruktur av direktivet. NIS-direktivet har genomförts i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen), förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen) samt myndighetsföreskrifter. Regelverket ställer krav på säkerhet i nätverk och informationssystem hos leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster samt krav på att rapportera incidenter som påverkar kontinuiteten i tjänsterna som tillhandahålls individer, organisationer och samhället i stort[38]. För varje sektor har i förordningen en sektorsmyndighet utsetts att bedriva tillsyn inom ramen för NIS. För sektorerna Bankverksamhet respektive Finansmarknadsinfrastruktur är Finansinspektionen tillsynsmyndighet.

Incidentrapportering är en central del i NIS-regleringen. Rapporteringen möjliggör stöd på nationell nivå under pågående incident samt utgör underlag för analys och lärande vilket i sin tur bidrar till relevanta prioriteringar och åtgärder i sektorn, Sverige och i EU. Rapporteringen sker till MSB som i sin tur vidarebefordrar rapporterna till relevant tillsynsmyndighet, i det här fallet Finansinspektionen. Vid nationsöverskridande incidenter informerar MSB dessutom berörda medlemsstater. En rapport skickas till MSB i tre skeden. Från konstaterad rapporteringsplikt sker rapportering inom 6 timmar, 24 timmar respektive fyra veckor, se avnittet ”När ska det rapporteras?” nedan.

Mer specifikt utgör incidentrapporteringen centralt underlag vid:

- Stöd från MSB/CERT-SE till den drabbade aktören vid hantering av incidenten
- Lägesbild och lägesbedömning hos MSB för eventuell eskalering
- Varningar från MSB till berörda sektorer och aktörer samt nationell samordning från MSB gällande incidenten i nätverk och informationssystem och störningen i den samhällsviktiga tjänsten

[37] (EU) 2016/1148
[38] Vägledning om rapportering av incidenter för leverantörer av samhällsvitkiga tjänster enligt NIS-regleringen, Sid 5.

- Information till andra berörda medlemsstater vid nationsöverskridande incidenter
- Information till allmänheten från MSB och vissa tillsynsmyndigheter
- Risk- och sårbarhetsanalyser hos MSB och vissa tillsynsmyndigheter
- Erfarenhetsutbyten i privat-offentlig samverkan
- Systematiskt tillsynsarbete
- Årsrapport från MSB till EU avseende inrapporterade incidenter
- Prioriteringar gällande regelutveckling och förebyggande stöd och regelutveckling på EU-, nationell och sektoriell nivå

Vilka incidenter ska rapporteras?

Definitionen av en rapporteringspliktig händelse som leverantörer av samhällsviktiga tjänster ska rapportera är[39]:

"Incidenter som orsakar störningar vilka får betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten."

Med *incident* avses "en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem".[40] Som förtydligande av formuleringen *störning i samhällsviktig tjänst* anges definitionen "En konsekvens av incidenten som innebär att den samhällsviktiga tjänsten inte levereras i förhållande till normalt tillhandahållande."[41]

Innan en rapporteringspliktig incident rapporteras måste leverantören utesluta att det inte är en incident som även faller under säkerhetsskyddslagen. Vid rapportering av incidenter som även påverkar Sveriges säkerhet måste leverantören säkerställa att känslig information om en sårbarhet i informationssystem kommuniceras på ett tillräckligt säkert sätt och till rätt myndighet[42].

Som underlag för beslut om huruvida incidenten har en betydande verkan på kontinuiteten, har MSB i föreskrifterna om incidentrapportering för leverantörer av samhällsviktiga tjänster definierat tröskelvärden som anger om händelsen är en rapporteringspliktig incident[43]. Dessa tröskelvärden varierar mellan sektorer. Tröskelvärden för bankverksamheter och finansmarknadsinfrastruktur anges nedan.

[39] MSBFS 2018:9, Kap 2, 1 §
[40] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
[41] Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen, Sid 6.
[42] Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd, Sid 15
[43] MSBFS 2018:9

Samhällssektor	Tröskelvärde för rapportering
Leverantörer inom **bankverksamhet** ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som:[44]	1. innebär att transaktioner inte kan eller sannolikt inte kommer att kunna initieras eller behandlas för a. minst 25 % av leverantörens normala antal transaktioner, eller b. minst 25 % av leverantörens användare, eller 2. pågår sammanlagt minst tre timmar under en 24-timmars period.
Leverantörer inom **finansmarknadsinfrastruktur** ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som[45]:	1. 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, 2. påverkar väsentliga tjänster hos systemviktiga finansiella infrastrukturföretag och har pågått i minst en timme, eller 3. har pågått i minst två timmar.

Tabell 2 - Tröskelvärden NIS

Begreppet konnektivitet som beskrivs för ett av tröskelvärdena kopplat till finansmarknadsinfrastruktur definieras som *"förmågan att utbyta information mellan två separata it-system eller datacenter som är uppkopplade genom nätverk."*. Tröskelvärdet används för att konnektivitet har stor betydelse för en väl fungerande marknad och finansiell stabilitet, samt för att en konnektivitetsstörning hos handelsplatser innebär att en ordnad handel i finansiella instrument inte kan genomföras[46].

När ska det rapporteras?

Samhällsviktiga aktörer ska rapportera incidenter med betydande inverkan på kontinuiteten i en samhällsviktig tjänst utan onödigt dröjsmål i tre steg:

[44] MSBFS:2018:9, Kap 5, 1 §
[45] MSBFS:2018:9, Kap 6, 1 §
[46] Vägledning om rapportering av incidenter för leverantörer av samhällsvitkiga tjänster enligt NISregleringen, Sid 18

1. *senast inom sex timmar från det att leverantören har identifierat att en incident är rapporteringspliktig, rapportera uppgifter enligt förbestämda områden,*
2. *senast inom 24 timmar från det att leverantören har identifierat att en incident är rapporteringspliktig rapportera uppgift enligt förbestämda områden, samt vid behov ändra eller komplettera tidigare rapportering.*
3. *inom fyra veckor från det första rapporteringstillfället rapportera uppgift enligt förbestämda områden, samt vid behov ändra eller komplettera tidigare rapportering.*

Tidsfristen om sex timmar för den första rapporteringen räknas från den tidpunkt då leverantören med stöd av sina interna regler och arbetssätt identifierat en incident som rapporteringspliktig. Exemplifierat innebär detta att en incident kan inträffa under lördag morgon men inte upptäckas förrän måndag morgon då personal är på plats. Incidenten behöver då rapporteras senast måndag eftermiddag[47].

Hur ska det rapporteras?

Rapportering av incidenter som orsakar störningar vilka får betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten sker genom:

…att besvara förbestämda frågor i tre skeden genom MSB:s webbaserade incidentrapporteringsverktyg. Föranmälda incidentrapportörer får tillgång till incidentrapporteringsverktyget genom personunika och certifikatbaserade incidentrapporteringskonton.

När detta PM publiceras håller MSB på att slutföra implementeringen av ett webbaserat incidentrapporteringsverktyg, som leverantören ska rapportera i. Enligt uppgift från MSB lanseras verktyget under kvartal 1 2020. Fram till dess ska rapporteringen ske enligt följande:

- Den inledande rapporten (inom sex timmar) rings in till MSB/CERT-SE på 010-240 40 40.
- Den mellanliggande rapporten (inom 24 timmar) skickas skriftligen tillsammans med den inledande rapporten med rekommenderat brev till MSB/CERT-SE.
- Slutrapporten (inom fyra veckor) skickas skriftligen med rekommenderat brev till MSB/CERT-SE.

Den skriftliga rapporteringen sker genom att fylla i anvisat pdf-formulär som finns på MSB: hemsida[48].

MSB tillgängliggör utan dröjsmål informationen i incidentrapporterna för berörd tillsynsmyndighet, i det här fallet Finansinspektionen. Det kommande webbaserade incientrapporteringsverktyget är förberett för att omedelbart vidarebefordra rapporten i respektive skede till Finansinspektionen.

---

[47] Vägledning om rapportering av incidenter för leverantörer av samhällsvitkiga tjänster enligt NIS-regleringen, Sid 8
[48] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/incidentrapportering-for-nis-leverantorer/incidentrapportering-for-leverantorer-av-samhallsviktiga-tjanster/

Leverantören har vid anmälan till Finansinstpektionen utsett en rapporteringsansvarig som har mandat att delegera rapporteringen till en eller flera incidentrapportörer. Rapportören kan vara en medarbetare hos leverantören eller anställd hos en utkontrakterad aktör, t.ex. en driftsleverantör. Incidentrapportören kommer att få ett personunikt och certifikatbaserat konto hos MSB genom vilket rapportören loggar in för att få tillgång till incidentrapporteringsverktyget.

Vad ska rapporteras?

Rapportören delger information utifrån 11 punkter samt ett antal underpunkter. Frågor ställs dels gällande incidenten som drabbar nätverk och informationssystem och dels gällande den störning som drabbar den samhällsviktiga tjänsten som en följd av incidenten.

Sex av elva punkter kräver större analysarbete:

- En beskrivning av inträffad incident och störning
- Bedömning av konsekvenser för andra än användare av den samhällsviktiga tjänsten.
- Bedömning av konsekvenser i andra medlemsstater inom EU
- Uppgift om åtgärder för att minimera konsekvenserna av incidenten.
- Uppgift om tidigare vidtagna åtgärder för att förebygga och hantera liknande incidenter.
- Uppgift om nya åtgärder för att förhindra att liknande incidenter inträffar på nytt

Av naturliga skäl har incidentrapportören mindre information om händelsen i det tidiga skedet då den första informationen ska lämnas in efter sex timmar. Med bakgrund mot detta efterfrågas mer information vid det andra och tredje rapporteringstillfället än vid det första. Information om vad leverantören förväntas rapportera vid varje tillfälle är kortfattat beskrivet nedan.

Inledande rapport - Skede 1 (sex timmar)

Syftet med första skedets rapportering är att MSB och den berörda tillsynsmyndigheten ska få en första preliminär bild av incidenten och störningen för att kunna förbereda för eventuellt direkt stöd och varningar till andra aktörer nationellt och nationsöverskridande.

Vid rapportering i det första skedet ska rapporten innehålla information kopplat till rubrikerna:

1. Allmänt
2. Om incidenten i nätverk och informationssystem
3. Om störningen i den samhällsviktiga tjänsten
4. Sekretessbedömning för Skede 1

Vid rapporteringens första skede ombes leverantören delge en rad konkret data som inte kräver större analys, exempel på sådan information är kontaktperson samt tid för när incidenten inträffade, uppmärksammades och började hanteras. I skede 1 ska leverantören även beskriva incidenten som påverkar it-miljön samt störningen i den samhällsviktiga tjänsten. Detta sker dock utifrån preliminär information, då leverantören antas ha mindre information om incidenten efter sex än 24 timmar. Givet detta innehåller frågeformuläret färre frågor om incidenten i skede 1 än skede 2.

Mellanliggande rapport - Skede 2 (24 timmar)

Syftet med rapporteringen i Skede 2 är att MSB och den berörda tillsynsmyndigheten ska få en fördjupad bild av incidenten och störningen som underlag för eventuellt direkt stöd, lägesuppfattning och varningar till andra aktörer nationellt och gränsöverskridande och att kunna möta frågor från media och allmänheten.

Vid rapportering i det andra skedet ska rapporten innehålla information kopplat till rubrikerna:

1. Typ av incident
2. Incidentens konsekvenser
3. Orsakerna till incidenten
4. Hanteringsåtgärder
5. Sekretessbedömning för Skede 2

Efter 24 timmar har leverantören haft möjligheten att samla in mer och kvalitativare information om incidenten, varför frågorna blir mer krävande. Utöver en mer utförlig beskrivning av incidenten ska leverantören nu ange vad de tror orsakat incidenten samt konkretisera de aktiviteter som genomförts och planerats i syfte att hantera de konsekvenser incidenten redan orsakat samt antas orsaka längre fram.

Slutrapport - Skede 3 (inom fyra veckor efter första rapporteringen)

Syftet med rapporteringen i Skede 3 är att MSB och den berörda tillsynsmyndigheten ska få en bild av incidentens orsak, hot och sårbarheter kopplade till incidenten samt lärdomar som dragits med avseende på incidenten. Denna slutrapport blir underlag för risk- och sårbarhetsanalyser på nationell nivå, återkoppling till sektorn på aggregerad nivå, systematisk och relevant tillsyn från tillsynsmyndigheten samt underlag för strategiska prioriteringar på nationell nivå.

Vid rapportering i det tredje skedet ska rapporten innehålla information kopplat till rubrikerna:

1. Allmänt
2. Upptäckten av incidenten respektive störningen

3. Ekonomiska konsekvenser
4. Tidigare vidtagna åtgärder för att hantera liknande incidenter
5. Hot, sårbarheter och hur störningen orsakades
6. Förebyggande åtgärder
7. Sekretessbedömning för Skede 3

När incidenten hanterats och verksamheten är åter i normal drift ska leverantören uppvisa en bred bild av såväl incidenten som sådan samt aktiviteter som genomförts eller planeras att genomföras i förebyggande syfte.

Säkerhetsskyddslagen

Säkerhetsskyddslagen genomgick en större förändring och blev gällande den 1 april 2019. Syftet med säkerhetsskyddet som sådant är att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot[49]. Grunden i lagen är att säkerhetskänslig information identifieras och skyddas på ett tillräckligt sätt. Arbetet styrs av Säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658) och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2) och gäller för alla som bedriver säkerhetskänslig verksamhet. I och med den nya lagen tydliggörs att samtliga verksamheter med säkerhetskänslig information omfattas, privat som offentlig. Alla som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet omfattas[50].

Den nya säkerhetsskyddslagen inkludrar krav på tillgänglighet som inte tidigare fanns. Genom att uppfylla lagen och identifera de delar av verksamheten som berörs kan det svenska samhället och dess mest elementära resurser prioriteras. Genom rapportering av incidenter som påverkat dessa resurser kan Säkerhetspolisen tydligare se vart angrepp sker och därmed konkretisera de största sårbarheterna.

Vilka incidenter ska rapporteras?

Säkerhetsskyddsförordningen anger att verksamhetsutövare som bedriver säkerhetskänslig verksamhet och som berörs av säkerhetsskyddslagen ska anmäla säkerhetshotande händelser, vilket är att[51]:

1. *en säkerhetsskyddsklassificerad uppgift kan ha röjts,*
2. *det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller*
3. *verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.*

Detta PM fokuserar på it-incidenter i informationssystem. Verksamhetsutövare med skyldighet att rapportera säkerhetshotande händelser är de som bedriver säkerhetskänslig verksamhet, det vill säga sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd[52]. Säkerhetshotande händelser ska enbart rapporteras om de påverkat säkerhetskänslig verksamhet, vilket inom många verksamheter endast är en viss del, tillgång eller funktion av betydelse för Sveriges säkerhet[53]. Huruvida

49 Vägledning i säkerhetsskydd, Introduktion till säkerhetsskydd, sid 6
50 Säkerhetsskyddslag (2018:585), 1 kap. 1 §.
51 Säkerhetsskyddsförordning 2018:658, 2 kap. 10 §.
52 Vägledning i säkerhetsskydd, Introduktion till säkerhetsskydd, sid 6
53 Vägledning i säkerhetsskydd, Introduktion till säkerhetsskydd, sid 17

verksamheten eller delar av den definieras som säkerhetskänslig verksamhet baseras på en säkerhetsskyddsanalys[54].

När ska det rapporteras?

Den verksamhetsutövare som bedriver säkerhetskänslig verksamhet och som uppmärksammar en rapporteringspliktig it-incident enligt säkerhetsskydds-förordningen ska[55]:

skyndsamt anmäla till Säkerhetspolisen

Vid anmälan av en säkerhetshotande händelse ska verksamhetsutövaren även överväga behovet av att informera andra verksamhetsutövare som från säkerhetsskyddssynpunkt kan vara berörda av händelsen. Detta ska göras snarast, dock senast i samband med att en anmälan till Säkerhetspolisen[56].

Hur ska det rapporteras?

Rapporten om it-incidenten skickas enligt de bestämmelser som finns i Säkerhetspolisens föreskrifter om säkerhetsskydd 3 kap. 14 § [57]:

En försändelse med en säkerhetsskyddsklassificerad fysisk handling eller elektronisk handling på ett lagringsmedium i säkerhetsskyddsklassen konfidentiell eller högre ska sändas med en distributör som har godkänts av verksamhetsutövaren. En sådan distributör ska kunna verifiera att försändelsen har levererats till mottagaren.

Vad ska rapporteras?

Säkerhetspolisen har för närvarande ingen mall för it-incidentrapportering[58]. Det saknas även allmänt tillgänglig vägledning om vad en it-incidentrapport till Säkerhetspolisen bör innehålla för information.

---

[54] Detta PM redogör inte för genomförandet av säkerhetsskyddsanalys. Om detta finns mer att läsa i Säkerhetspolisens vägledning Säkerhetsskyddsanalys.
[55] Säkerhetsskyddsförordning 2018:658, 2 kap. 10 §.
[56] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 2 kap. 25 §.
[57] Enligt mailkonversation med Säkerhetspolisen 191030, PMFS 2019:2, 3 kap. 14 §.
[58] Enligt mailkonversation med Säkerhetspolisen 191030

Regelverkens gemensamma nämnare

Vilka incidenter ska rapporteras?

Det som förenar alla fyra incidentrapporteringsramverk som tas upp i detta PM är att samtliga till viss del eller i sin helhet berör informationssäkerhetsincidenter, dvs. incidenter som påverkar information, nätverk och informationssystem.

Inom ramen för informationssäkerhetsincidenter har alla fyra regleringar gemensamt att kraven berör incidenter som kan påverka informationens konfidentialitet, integritet eller tillgänglighet.

En gemensam nämnare för PSD2, NIS och säkerhetsskyddslagen är begreppet kontinuitet eller tillgänglighet avseende påverkad tjänst när det ska avgöras om en incident är rapporteringspliktig.

För både PSD2 och NIS gäller att det föreligger rapporteringsplikt om berörda transaktioner inte kan initieras eller behandlas för minst 25 % av betaltjänstleverantörens normala antal transaktioner, eller minst 25 % av leverantörens användare.

När ska det rapporteras?

Alla incidenter ska rapporteras skyndsamt eller utan onödigt dröjsmål och i vissa fall vid upprepade tillfällen. Inga av rapporteringsramverken har gemensamma tider för rapportering.

De tidsramar som anges för den första rapporteringen varierar mellan 4 och 72 timmar.

PSD2 och NIS ställer krav på rapportering i tre huvudsakliga skeden, från inledande preliminär rapport till avslutande rapport.

De krav som föreligger på tid för rapportering i olika skeden påvisar höga krav på processer och rutiner för inhämtning, hantering och distribuering av information samt beslut gällande vad som ska rapporteras.

Hur ska det rapporteras?

Alla rapporteringsramverk som behandlas i detta PM har olika myndigheter som mottagare av incidentrapporterna.

Också på vilket sätt rapporten ska tillhandahållas myndigheterna varierar mellan alla fyra ramverk.

PSD2 och NIS anger möjligheten att delegera rapporteringen till annan extern organisation, t.ex. en kontrakterad driftsleverantör.

Vad ska rapporteras?

Utöver allmänna uppgifter om incidentrapportören och den tjänst eller de(t) system som påverkats, efterfrågas för alla utom säkerhetsskyddslagen uttryckligen att rapporten ska beskriva den inträffade incidenten, effekterna av den och de åtgärder som genomförs och/eller planeras för att hantera den. Utöver dessa gemensamma krav på beskrivning av händelsen, dess uppskattade konsekvenser samt åtgärder för hantering, efterfrågar PSD2 och NIS även en orsaksanalys.

Givet den relativt stora mängd information som efterfrågas ställs höga krav på organisationernas förmåga att analysera konsekvenserna av en incident, redovisa tydliga åtgärder, utreda orsaken samt påvisa det förebyggande arbetet.

Nedan följer en sammanställning med efterfrågad information som berör minst två ramverk för incidentrapportering. Då det saknas anvisningar för vad som ska rapporteras enligt Säkerhetsskyddslagen, är inte det ramverket med i sammanställningen.

Efterfrågad information	PSD2	NIS	GDPR
Namn på och org.nr för den rapporteringspliktiga organisationen	X	X	X
Namn på och org.nr för den rapporterande organisationen (om delegerad rapportering till annan organisation)	X	X	
Internt referensnummer	X	X	X
Kontaktperson för incidentrapporten (Namn, E-postadress, Telefonnummer)	X	X	X
När inträffade/började incidenten (datum, tidpunkt)?	X	X	X
När upptäcktes incidenten (datum, tidpunkt)?	X	X	X
Hur upptäcktes incidenten?	X	X	X
När upphörde incidenten/beräknas incidenten upphöra (datum, tidpunkt)?	X	X	

Beskrivning av incidenten	X	X	X
Orsak till incidenten (Tekniskt fel, naturfenomen, misstag, medveten handling etc)	X	X	X
Har incidenten påverkat ett annat land?		X	X
Inom vilket verksamhetsområde inträffade incidenten?	X	X	X
Typ av tjänst/verksamheter påverkade av incidenten	X	X	X
Typ av konsekvens (Konfidentialitet, riktighet, tillgänglighet, kontinuitet)	X	X	X
Konsekvenser för nätverk och informationssystem	X	X	
Berörda eller inblandade tredjepartsleverantörer	X	X	
Konsekvenser för tjänst/verksamheter/personer påverkade av incidenten	X	X	X
Antal användare påverkade av incidenten	X	X	X
Förväntade ekonomiska konsekvenser med avseende på incidenten	X	X	
Hur hanteras/hanterades incidenten (återställning, alternativ drift, begränsa konsekvenser etc)?	X	X	
Aktiverades organisationens kontinuitetsplan?	X	X	
Vidtagna eller planerade förebyggande åtgärder med anledning av incidenten	X	X	X

Tabell 3 – Gemensamma frågor vid incidentrapportering

Avslutning

Sammanfattningsvis kan kontasteras att det är relativt få gemensamma nämnare som går att utkristalisera vid en jämförelse av incidentrapporteringskraven mellan PSD2, NIS, GDPR och säkerhetsskyddslagen. De har alla olika ursprung, från EU-förordningar och nationella tillämpningar av EU-direktiv till unik nationell lagstiftning. De har också olika delsyften, tidsfristerna för rapportering skiljer sig, liksom vad som ska rapporteras och till vem.

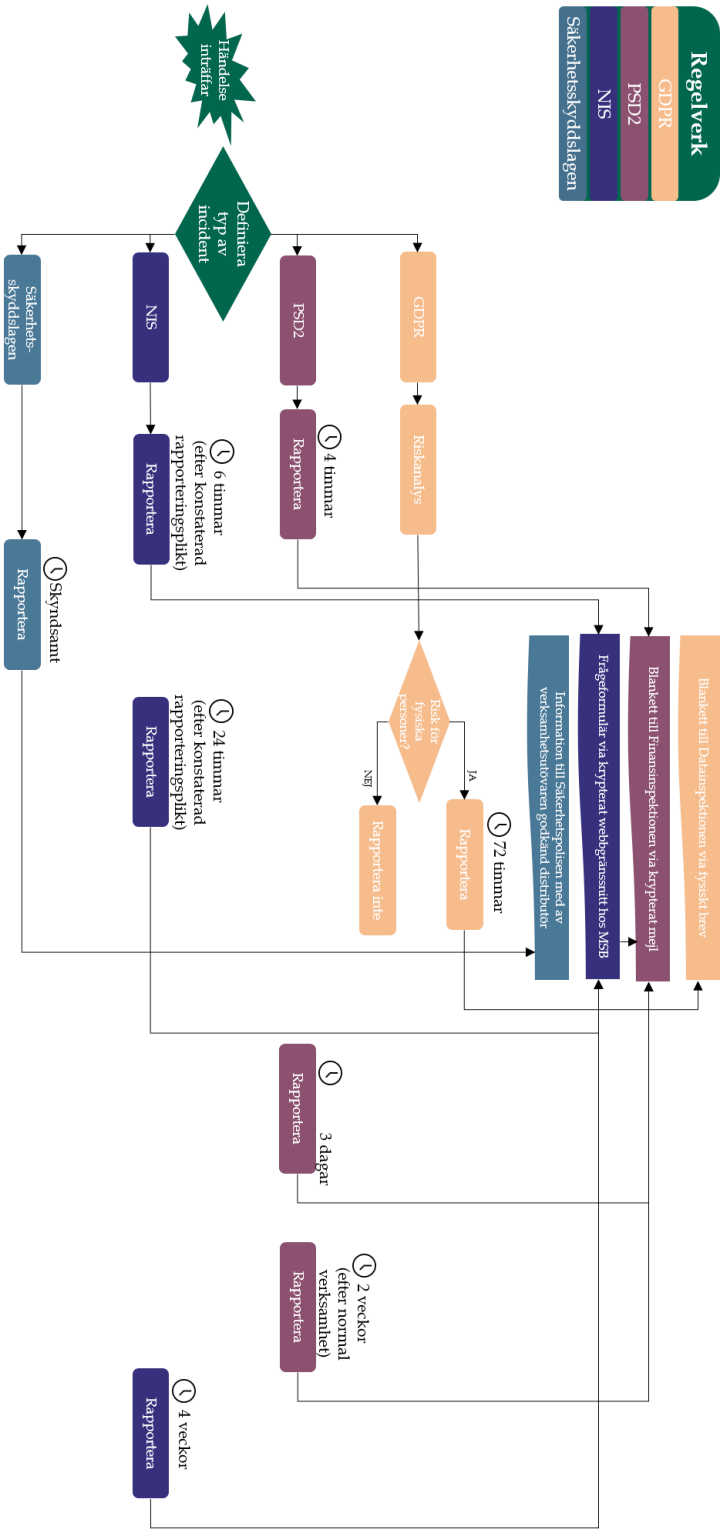
Det är en utmaning att behöva rapportera i olika spår. Därför behöver det läggas ett visst initialt arbete på att effektivisera den egna organisationens incidentrapportering och dra nytta av de syften och gemensamma nämnare avseende rapportinnehåll som ändå finns och som har tagits upp i detta PM. Om aktören har verksamhet i flera EU-länder, kanske med gränsöverskridande it-infrastruktur, kan ett övervägande vara att för hela koncernen tillämpa de regler som är mest strikta i en viss medlemsstat.

Det som de flesta incidentrapporteringsramverk anger i syftesbeskrivningen är att höja kunskapen om incidenter för att kunna vidta relevanta beslut om regler, tillsyn och säkerhetsåtgärder etc. Denna kunskap är värdefull både för organisationen själv, för reglerande myndigheter, för sektorns aktörer och andra sektorer. Vidare betonas för flera av ramverken vikten av att integrera den formella incidentrapporteringen i organisationens incidenthanteringsprocess och därmed i det systematiska informationssäkerhetsarbetet.

För att incidentrapporteringen ska skapa organisatoriskt lärande och samhällsnytta behöver rapporterna innehålla kunskapshöjande information och rapporteringen behöver stimuleras av tillsynsmyndigheten. I vissa av de jämförda regelverken är det till och med förenat med sanktioner att inte rapportera eller att skicka rapporter av undermålig kvalitet. Därmed handlar det om att om tillsynsmyndigheten ska kunna förvänta sig incidentrapporter med fyllig information om orsaken till incidenten och sårbarheter hos aktören, bör inte tillsynsmyndigheten använda den informationen till att straffa aktören med sanktionsavgifter. För att få till en bra rapportering bör den drabbade aktören istället känna tillit till att informationen hanteras på ett diskret sätt och att aktören får positiv återkoppling på att ha skickat en detaljerad rapport över incidenten. Samtidigt behöver den mottagande myndigheten visa på värdet av att ta emot rapporter samt rapportera tillbaka till sektorns aktörer utfallet av rapporteringen på en aggregerad nivå och utan att exponera enskilda aktörer.

Med en bra tillsynsrelation och rapportering av god kvalitet, uppnår organisationer och samhället ett tillstånd av lärande och ständiga förbättringar gällande informationssäkerhet. Förhoppningsvis kan också den formella incidentrapporteringen bidra till verksamhetens egna incidenhtanteringsprocess, vilket incidentrapporteringen är en del av.

Bilaga A – Förenklad incidentrapporteringsprocess



Bilaga B – Referenslista

GDPR

- Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679
- Dataskyddsförordningen artikel 33-34
- Dataskyddsförordningen beaktandesatser (skäl) 85–88

PSD2

- Remisspromemoria, FI Dnr 15-10584, 2018-01-30
- SFS nr: 2010:751_5 b kap.
- Lag om ändring i lagen (2010:751) om betaltjänster_5 b kap.
- Guidelines on incident reporting under PSD2_EBA-GL-2017-10
- Riktlinjer för säkerhetsåtgärder för operativa risker och säkerhetsrisker enligt PSD2_EBA-GL-2017-17
- fi-forum_betaltjanster_20180607
- Finansinspektionens föreskrifter om verksamhet för betaltjänstleverantörer FFFS 2018:4

NIS-direktivet

- MSBFS 2018:7, anmälan och identifiering av leverantörer av samhällsviktiga tjänster
- MSBFS 2018:8, informationssäkerhet för leverantörer av samhällsviktiga tjänster
- MSBFS 2018:9, rapportering av incidenter för leverantörer av samhällsviktiga tjänster
- Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster SFS 2018:1175
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster SFS 2018:1174
- EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/1148 (NIS-direktivet)
- Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen_2018.12.20
- Stöd för ifyllande av incidentrapporteringsformulären för samhällsviktiga respektive digitala tjänster, 2019-03-29
- Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (20 §)
- Incidentrapporteringsformulär leverantörer av samhällsviktiga tjänster - Skede 1 och 2

- Incidentrapporteringsformulär leverantörer av samhällsviktiga tjänster - Skede 3
- Exempel på it-incidenter april 2016
- FIs roll i NIS 20190503
- MSB Samlad NIS-presentation banksektorn 190503
- Om NIS för banksektorn 190503

Säkerhetsskyddslagen

- Säkerhetsskyddslag SFS 2018:585
- Säkerhetsskyddsförordning (2018:658)
- Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS_2019:2
- Säkerhetspolisens hemsida / Säkerhetsskydd
- Vägledning i säkerhetsskydd, Introduktion till säkerhetsskydd, Juni 2019
- Vägledning i säkerhetsskydd, Säkerhetsskyddsanalys, Juni 2019

Övrigt

- Årsrapport it-incidentrapportering 2017 (MSB)
- Forskningsrapport Driftavbrott i samhällsviktiga it-tjänster, 2018
- vagledning---grundlaggande-it-sakerhetsatgarder---forhandsutgava (MSB)