ENERGI FÖRETAGEN

En rapport från Energiföretagen

Att säkerhetsskyddsklassificera skyddsvärda uppgifter

En handledning

April 2022

Förord

Elförsörjning är en viktig del av infrastrukturen och en förutsättning för samhällets funktionalitet. Innehavare av verksamheter har ett stort ansvar att se till att svara mot samhällets krav på säkerhetsskydd som bland annat innebär att skyddsvärda uppgifter inte kommer i orätta händer, vilket om så sker, kan leda till skada för Sverige. Det är därför viktigt att alla ägare av verksamhet inom energisektorn arbetar systematiskt med att klassificera sina informationstillgångar och därefter vidtar nödvändiga åtgärder för att skydda dessa tillgångar så att endast de som har behov och är behöriga har tillgång till dem.

Denna vägledning från Energisäkerhetsgruppen (ESG) arbetsgrupp Säkerhetskyddsgruppen syftar till att beskriva förutsättningar och behov av klassificering av säkerhetsskyddade uppgifter. Vägledningen belyser även viktiga ingångsvärden, realistiska hot och hotnivåer, Säpos vägledande metodik samt sekretessprövning och hantering.

Denna publikation är sammansatt av en arbetsgrupp inom Energisäkerhetsgruppen (ESG). Arbetsgruppen har bestått av sakkunniga experter och säkerhetsskyddschefer från företagen. I arbetsgruppen har följande personer ingått:

Alireza Hafezi, Ellevio AB

Kristina Blomqvist, Vattenfall AB

Andreas Kertes, Öresundskraft AB

Berith Rannberg, Karlstad Energi AB

Ulf Gustafsson, Skellefteå Kraft AB

Anders Bergqvist, Stockholms Exergi

Peter Valvassori, Tekniska verken i Linköping AB

Emma Johansson, Energiföretagen Sverige AB

April 2022

Innehåll

1. Inledning

1.1 Syfte och mål

Hantering av uppgifter blir allt viktigare i dagens informationssamhälle då information är en av de värdefullaste tillgångarna för verksamheter. Syftet med denna vägledning är att ge energiföretag ytterligare stöd i arbetet med identifiering och analys av säkerhetsskyddade uppgifter.

Klassificering och hantering av uppgifter syftar till att leva upp till verksamheternas krav som finns på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Vägledningens värde har verifierats genom att utvalda ESG-medlemmar i säkerhetsskyddsgruppen skrivit och utvärderat dokumentet. Dokumentet kan tillämpas och användas som ett hjälpmedel för att leva upp till säkerhetskyddslagstiftningen.

Slutsatsen är att behovet av denna typ av dokument för klassificering av uppgifter behövs inom verksamheter. Målet är att harmonisera bedömningen av säkerhetsskyddsklassificering av uppgifter inom energisektorn.

1.2 Målgrupp

Denna vägledning riktar sig till verksamhetsansvarig samt säkerhetsskyddschef som ansvarar för säkerhetsbedömningen. För fullständig förståelse av vägledningens innehåll bör personen eller personerna i fråga ha grundläggande förståelse för säkerhetsskydd och säkerhetsskyddsanalys.

2. Bakgrund

2.1 Säkerhetsskyddsklass och konsekvensnivå

Under säkerhetsskyddsanalysens genomförande och när det är definierat vilka tillgångar verksamheten har, klassificeras uppgifterna för att tilldelas en lämplig skyddsnivå. Det som avgör vilken konsekvensnivå uppgifterna får beror på hur kritisk den är för Sveriges säkerhet.

Säkerhetsskyddsklassificerade uppgifter delas in fyra säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet.

Tabell 1. Säkerhetsskyddsklass (A–D) och innebörd.

Konsekvensnivå	Säkerhetsskyddsklass	Innebörd
Nivå A	Kvalificerat hemlig	Synnerligen allvarlig skada för Sveriges säkerhet
Nivå B	Hemlig	Allvarlig skada för Sveriges säkerhet
Nivå C	Konfidentiell	En inte obetydlig skada för Sveriges säkerhet
Nivå D	Begränsat hemlig	Endast ringa skada för Sveriges säkerhet

Källa: Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).

2.2 Antagande

I denna vägledning görs antagandet att verksamheten i sin säkerhetskyddsanalys kommit fram till slutsatsen att de bedriver en säkerhetskänslig verksamhet samt har identifierat skyddsvärden enligt konsekvensnivå A-D. Hamnar uppgiften under konsekvensnivå D så betraktas det inte som en säkerhetsskyddsklassificerad uppgift.

2.3 Avgränsning

Det som inte är säkerhetskyddsklassificerat kan ha ett skydd under Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och/eller enligt offentlighets- och sekretesslag (2009:400) (OSL). NIS-lagen gäller dock inte om säkerhetsskyddslagstiftningen är tillämplig enligt 8 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

3. Säkerhetsskyddsklassificerad uppgift

Bestämmelserna om säkerhetsskyddsklassificerade uppgifter finns under säkerhetsskyddslagen *(2018:585)* 1 kap. 2 §. Med säkerhetskyddskvalificerad uppgift avses uppgifter som:

1. rör säkerhetskänslig verksamhet och
2. omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

Det är viktigt ur ett rättsligt perspektiv att båda villkoren ska vara uppfyllda innan en uppgift ska avses vara säkerhetsskyddsklassificerad uppgift. Grunden för om någon uppgift är säkerhetsskyddsklassad är inte bara att det rör säkerhetskänslig verksamhet, utan också att uppgiften omfattas av sekretess enligt OSL (2009:400). Detta förhållande tydliggörs även i Säkerhetspolisens vägledning *Introduktion till säkerhetsskydd* (2019). Följande text är hämtat därifrån:

”För att bedöma om en uppgift är säkerhetsskyddsklassificerad behöver alltså enskilda verksamhetsutövare i praktiken göra en fiktiv sekretessprövning liknande den som myndigheter gör. Om bedömningen görs att en myndighet hade varit förhindrad att röja motsvarande uppgift är den att anse som säkerhetsskyddsklassificerad (förutsatt att den rör den säkerhetskänsliga verksamheten).”

4. Viktiga ingångsvärden

Andra viktiga ingångsvärden till säkerhetsskyddsklassning av uppgifter är att det ramverk som sätts upp för bedömning av uppgifter bland annat bygger på:

- Realistiska hotscenarion. Det är viktigt att innan bedömning av uppgifter ha en tydlig beskrivning av hotbilder som är aktuella i och kring säkerhetskänslig verksamhet. Det är också av vikt att identifiera vilka uppgifter i verksamheten som kan möjliggöra eller underlätta realisering av de identifierade hoten/hotbilderna. Att utgå från orealistiska hotscenarion kan resultera i över- eller underdimensionerade skyddsåtgärder.
- Omedelbara konsekvenser. En annan grundprincip i bedömning av uppgifter är att undvika scenarier där en uppgift behöver kombineras med flera andra uppgifter innan den skulle kunna nyttjas för att skada säkerhetskänslig verksamhet. Det är av vikt att klargöra vad som är en rimlig kombination i analysarbetet, annars kan det finnas risk att mängden säkerhetsskyddsklassificerade uppgifter ökar mer än nödvändigt.
- Rimlig hänsyn till andra verksamheters beroende. Att ta hänsyn till andra verksamheters beroende till den egna är förstås viktigt. Svårigheten är att det ofta av säkerhetsskäl är omöjligt att ha insyn i andra verksamheters sårbarheter. I de fall det inte finns ett uttalat beroende blir det ofta någon form av ”spekulationer eller gissningar” kring andra verksamheters beroende till den egna. Det är således viktigt att ha regelbunden dialog med kunder som anses bedriva samhällskritisk verksamhet och med sektorsansvariga myndigheter om samhällskritiska beroenden till den egna verksamheten.

5. Realistiska hot och hotscenarion

En viktig del i säkerhetsskyddsanalysen är att identifiera vad den säkerhetskänsliga verksamheten ska skyddas mot. För att besvara frågan ska verksamhetsutövaren utifrån myndigheternas hotbildsbeskrivningar och egna identifierade hot bedöma hur de aktuella hoten kan påverka den egna verksamheten.

Mål inom energisektorn för ett antagonistiskt angrepp kan vara infrastruktur, informationssystem, information (uppgifter) och personal. Infrastruktur kan angripas fysiskt eller via IT-system, till exempel med en cyberattack. Vissa informationssystem är kritiska för elförsörjningen samtidigt som de kan vara svåra att skydda eftersom det ofta ligger i deras funktion att vara tillgängliga dygnet runt, för flera aktörer och från flera geografiska platser. Information om viktiga anläggningar och IT-system, och personer i kritiska funktioner men även information om kritiska sårbarheter i elförsörjningen kan vara mål för informationsinsamling och kartläggning.

Realistiska hot mot energisektorn bedöms vara:

- Spionage
  - Traditionellt spionage med hjälp av agenter som genom fysisk närvaro kartlägger och insamlar uppgifter om till exempel kritiska informationssystem och anläggningar.
  - Cyberspionage som utnyttjar informationssystem och öppna källor kring säkerhetskänslig verksamhet för insamling av information.
- Total- och civilförsvar (uppgifter om beredskapsplanering och åtgärder)
- Sabotage
  - Fysiskt (slår ut en eller flera anläggningar, sannolikt genom sprängning av hela eller delar av anläggning(ar)).
  - Cyber (slår ut strömförsörjningen och/eller tar över styrförmågan att kontrollera distributionen av energi och produktion av el till ett eller fler geografiska områden). Detta kan bland annat ske genom att ta över eller slå ut SCADA-systemen eller tillhörande nätverk.

6. Säkerhetspolisens vägledande metodik

I Säpos vägledning *Introduktion till säkerhetsskydd* (2019) definieras fem steg för att på ett systematiskt sätt identifiera, bedöma konsekvenser av ett röjande, klassificera säkerhetsskyddsuppgifter ur ett konfidentialitet perspektiv, sekretesspröva uppgifterna mot OSL och bedöma uppgifternas klassning ur ett riktighets- och tillgänglighetsbehov i en säkerhetskänslig verksamhet.

”I första steget görs en bedömning av om uppgiften över huvud taget rör säkerhetskänslig verksamhet. För den som endast till någon del bedriver säkerhetskänslig verksamhet innebär detta att många uppgifter kommer falla utanför kraven på säkerhetsskydd.

I det andra steget bedöms om ett röjande av uppgiften kan medföra skada för Sveriges säkerhet. Flertalet uppgifter, såsom tidigare exempel med meteorologiska data, behöver inte skyddas mot att röjas och är därmed inte säkerhetsskyddsklassificerade uppgifter. Uppgifterna kan dock fortfarande behöva vara riktiga (i bemärkelsen oförändrade) och/eller tillgängliga, vilket medför att de ändå omfattas av kraven på säkerhetsskydd.

I det tredje steget delas uppgiften in i en säkerhetsskyddsklass utifrån den skada ett röjande av uppgiften kan medföra för Sveriges säkerhet.

I det fjärde steget identifieras sekretessbestämmelser i offentlighets- och sekretesslagen som är, eller skulle varit, tillämplig på uppgiften. Om ett röjande av uppgiften skulle medföra skada för Sveriges säkerhet så kommer uppgiften i princip alltid att omfattas av en eller flera sekretessbestämmelser.

I det femte och avslutande steget görs bedömningen om uppgiften även behöver vara riktig och/eller tillgänglig eller om den endast behöver skyddas mot att röjas såsom kan vara fallet med exempelvis kopior och arbetsmaterial.”

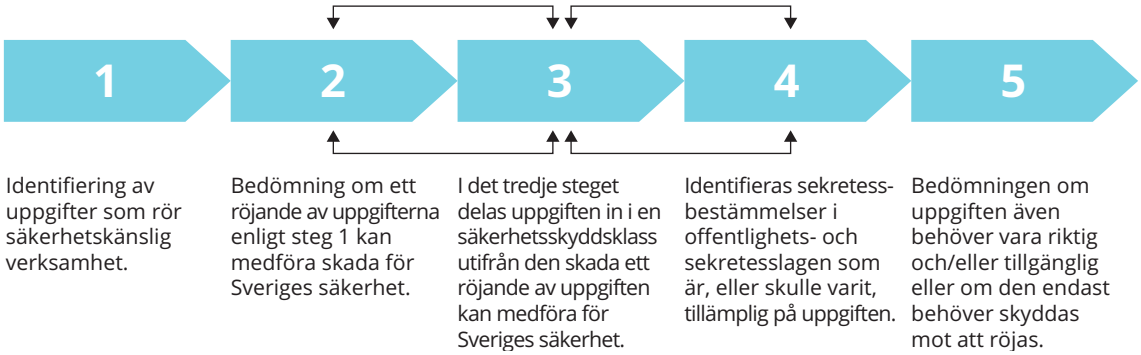
Fem steg – Säpos vägledning

1. Identifiering av uppgifter som rör säkerhetskänslig verksamhet.
2. Bedömning om ett röjande av uppgifterna enligt steg 1 kan medföra skada för Sveriges säkerhet.
3. I det tredje steget delas uppgiften in i en säkerhetsskyddsklass utifrån den skada ett röjande av uppgiften kan medföra för Sveriges säkerhet.
4. Identifieras sekretessbestämmelser i offentlighets- och sekretesslagen som är, eller skulle varit, tillämplig på uppgiften. Om ett röjande av uppgiften skulle medföra skada för Sveriges säkerhet så kommer uppgiften i princip alltid att omfattas av en eller flera sekretessbestämmelser.
5. Bedömningen om uppgiften även behöver vara riktig och/eller tillgänglig eller om den endast behöver skyddas mot att röjas.

6.1 En iterativ process

Det som inte riktigt framgår i Säpos vägledning är att vissa av de steg som definieras behöver ofta genomföras iterativt. Det praktiska genomförandet av en säkerhetsskyddsklassificering är inte alltid så sekventiellt som modellen visar, därför kan vissa delar sammanfalla eller behöva göras flera gånger. Det viktiga är att alla delar i modellen genomförs och att arbetet dokumenteras så att det finns spårbarhet.

Ordet iterativ betyder upprepande, och i grunden så innebär **en** iterativ process att man upprepar en sekvens av processen om och om igen för att nå det önskade resultatet. För att fastställa om en uppgift i ens verksamhet kan vara av betydelse för Sveriges säkerhet krävs som tidigare nämnts att två villkor ska vara uppfyllda, vilket innebär att en iterativ analysprocess mellan framför allt steg 2–4 är att rekommendera. En iterativ analysprocess mellan dessa steg innebär att den analys som görs med fördel kan göras om och ändras.



För att uppgifter ska anses vara säkerhetsskyddsklassificerade måste de röra säkerhetskänslig verksamhet och omfattas av någon sekretessbestämmelse i offentlighets- och sekretesslagen. Det är viktigt att komma ihåg att båda två kriterierna måste vara uppfyllda.

7. Sekretessprövning

För att bedöma om en uppgift är säkerhetsskyddsklassificerad behöver alltså enskilda verksamhetsutövare i praktiken göra en fiktiv sekretessprövning liknande den som myndigheter gör. Om det görs bedömningen att en myndighet hade varit förhindrad att röja motsvarande uppgift är den att anse som säkerhetsskyddsklassificerad (förutsatt att den rör den säkerhetskänsliga verksamheten).

Säkerhetsskyddsklassificerade uppgifter är enligt Säpos vägledning *Introduktion till säkerhetsskydd* (2019) framför allt sådana uppgifter som är eller skulle ha varit sekretessbelagda enligt 15 kap. 2 § i offentlighets- och sekretesslagen (försvarssekretess).

Men även andra sekretessbestämmelser kan vara tillämpliga på uppgifter som rör säkerhetskänslig verksamhet, exempelvis:

- 15 kap. 1 § (utrikessekretess),
- 18 kap. 1 § (förundersökningssekretess),
- 18 kap. 2 § (sekretess i underrättelseverksamhet) och
- 18 kap. 8 § (säkerhets- och bevakningsåtgärder).

Sekretess som rör 15 kap. 1 § (utrikessekretess), 18 kap. 1 § (förundersökningssekretess), 18 kap. 2 § (sekretess i underrättelseverksamhet) förekommer sällan i verksamhet inom energisektorn. De paragrafer som är möjliga att pröva mot är således 15:2 och 18:8.

Vad gäller 15 kap. 2 § så skulle till exempel upprättade av planer rörande totalförsvaret kunna omfattas av sekretess enligt paragrafen och därför skulle motsvarande uppgifter kunna klassas som säkerhetsskyddsklassificerade uppgifter. 15 kap. 2 §:

”Sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.”

Vad gäller 18 kap. så är den 8 § som är relevant för verksamhet inom energisektorn. I 18 kap. 8 § står att läsa:

Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser:

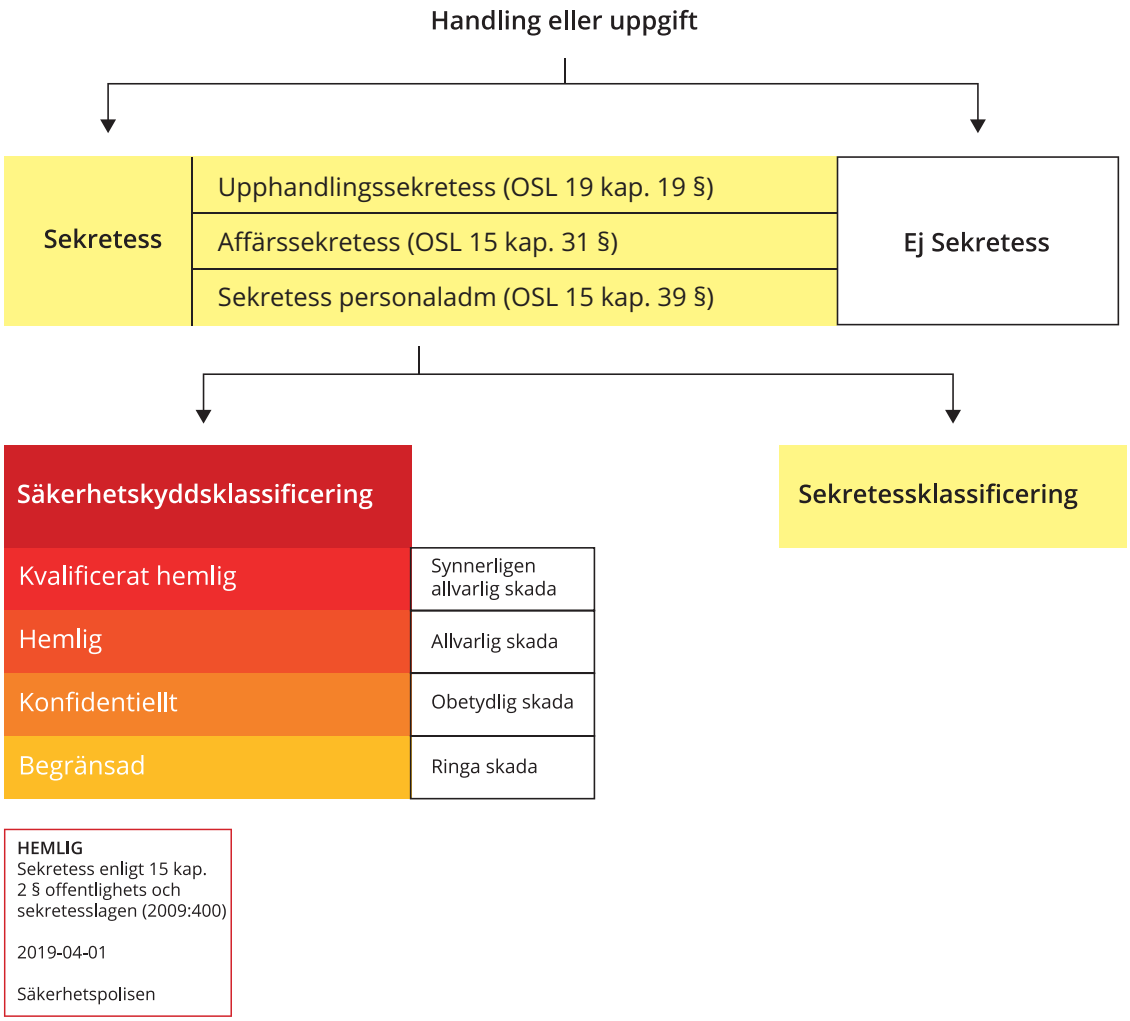
1. byggnader eller andra anläggningar, lokaler eller inventarier,
2. tillverkning, förvaring, utlämning eller transport av pengar eller andra värdeföremål samt transport eller förvaring av vapen, ammunition, sprängämnen, klyvbart material eller radioaktiva ämnen,
3. telekommunikation eller system för automatiserad behandling av information,

4. behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling,
5. den civila luftfarten eller den civila sjöfarten,
6. transporter på land av farligt gods, eller
7. hamnskydd

Det är viktigt att understryka att denna paragraf handlar om uppgifter om *säkerhets- och bevakningsåtgärder*. Det skulle exempelvis kunna röra sig om information om hur det fysiska skyddet kring förvaringen av radioaktivt material i kärnkraftverk är uppbyggt, eller information om skyddsmekanismerna vad gäller hur man får tillgång till system som i sin tur ger tillgång till säkerhetskänslig verksamhet (till exempel driftcentraler), om detta innebär att syftet med skyddsmekanismerna motverkas. Bedömningen är att punkterna 1, 2, 3 och 4 kan vara relevanta för verksamhet inom energisektorn.

Nedan är en bild från Säkerhetspolisen som översiktligt förklarar hur det förhåller sig mellan offentlighets- och sekretesslagen och Säkerhetsskydd.

Klassificering



8. Exempel på uppgifter

8.1 OSL 15:2

15 kap. 2 §: Sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för Sveriges säkerhet om uppgiften röjs.

Nedan följer några exemplar på uppgifter som kan prövas och/eller omfattas av 15:2.

- Uppgifter som rör planläggning eller annan förberedelse som görs inom ramen för totalförsvarsplanering, såsom uppgifter om vissa riktade beredskapsåtgärder eller krigsplacering av personal.
- Prövning av förekomsten av andra uppgifter i företagets verksamhet som kan falla under ”som i övrigt rör totalförsvaret”, till exempel uppgifter om Ö-drift eller Styrel.
- Detaljerade uppgifter om säkerhetsskyddsklassificerade anläggningar, krisledningsorganisation och reservrutiner i en säkerhetskänslig verksamhet bör, ifall de är av stor betydelse för upprätthållande av kritiska samhällstjänster, prövas mot denna paragraf.

8.2 OSL 18:8

18 kap. 8 §: Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

Nedan följer några exemplar på uppgifter som kan prövas och/eller omfattas av 18:8.

1. Byggnader eller andra anläggningar, lokaler eller inventarier, Säkerhets- och bevakningsåtgärd kan i första hand vara uppgifter som rör det fysiska skyddet. Kan till exempel vara uppgifter om skyddsåtgärder i och kring driftcentralen (DC) eller till säkerhetsskyddsklassificerade anläggningar som ingår i starta-Sverige, Ö-drift och/eller Styrelsprocessen. Uppgifter kan till exempel vara ritningar och tekniska dokumentationer över larmsystemen till de aktuella anläggningarna samt bevakningsinstruktioner.
2. Telekommunikation eller system för automatiserad behandling av information. Kan vara uppgifter om logiska skyddet i och kring SCADA och process- eller driftnätverket. Kan till exempel vara tekniska beskrivningar om tillämpning av skyddssystemen, krypteringsnycklar, granskningsrapporter som beskriver sårbarheter i dessa miljöer.
3. Behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling. Kan vara uppgifter om behörigheter till säkerhetssystem som behandlar säkerhetsloggar, lås och larm till säkerhetsklassade anläggningar.

9. Aggregerade och ackumulerade uppgifter

Säkerhetspolisens vägledning om informationssäkerhet säger följande:

”Aggregerade uppgifter betyder att flertalet olika typer av uppgifter samlas och tillsammans utgör ett nytt skyddsvärde, medan ackumulerade uppgifter betyder en ökad volym av samma typ av uppgifter. Om enskilda uppgifter som saknar säkerhetsskyddsklass eller är indelade i en av säkerhetsskyddsklasserna begränsat hemlig, konfidentiell eller hemlig samlas, kan det i vissa fall medföra att en högre säkerhetsskyddsklass ska tillämpas på uppgiftssamlingen. Så är fallet om den aggregerade eller ackumulerade informationen gör att en antagonist kan dra andra, helt nya slutsatser av uppgiftssamlingen än av varje enskild uppgift.

Av förarbetena till säkerhetsskyddslagen framgår att en klassificering av en samling av uppgifter inte bör göras i större utsträckning och med placering i högre klass än vad som är nödvändigt. Detta för att begränsa onödiga administrativa kostnader och onödiga ingrepp i enskildas integritet med mera. Endast i undantagsfall, där det finns ett tydligt samband mellan uppgifterna som gör att skadan av ett röjande skulle bli mer allvarlig, kan det därför vara aktuellt att höja klassificeringen på en sammanställning av uppgifter.

Det betyder att en aggregering eller ackumulering av uppgifter inte med nödvändighet medför en högre klassificering.”

10. Hantering

10.1 Kontinuerlig process

Utöver kunskap om klassificeringen ingår även förståelse för att klassificeringsarbetet aldrig tar slut. Klassificering av uppgifter är en process som inte behandlas en gång för att sedan vara färdigarbetat. Det som klassificeras på en nivå i dagsläget, behöver nödvändigtvis inte ha samma klassificering ett antal år senare. Vilket gör att processen för klassificering är en kontinuerlig och levande process som fortgår hela tiden.

All utförd klassificering har ett bäst-före-datum. Det är viktigt att sätta en rimlig gallringsfrist på all genomförd klassificering så att en kontroll genomförs regelbundet om att inte gällande klassificering är felaktig. Syftet med detta är att en gällande klassificering kan innebära en för hög klassificering vilket i sin tur innebär att en organisation eller verksamhet har en onödig kostnad i både tid och resurser vid hanteringen. Alternativt att en uppgift har en för låg klassificering vilket riskerar att informationen läcks till obehörig.

En uppdatering av klassificering av säkerhetsskyddade uppgifter bör även genomföras när minst en av följande saker sker där nya uppgifter har tillkommit:

- Ett nytt informationssystem ska utvecklas.
- Ett befintligt system används som inte tidigare har blivit klassificerat.
- Delar inom verksamheter förändras eller hela verksamheten som påverkar säkerheten.
- Förändringar eller krav genom lagändringar eller andra gällande avtal.
- Ny teknik eller andra tekniska förändringar har genomförts.
- En skyddsåtgärd har genomförts där hot och risker har upptäckts som påverkar klassificeringen. Då ska en ny analys genomföras efter en rimlig tid för att undersöka att åtgärderna har uppnått avsedd effekt.

11. Slutord

Vägledningen presenterar en process för hur ett klassificeringsarbete kan gå till och kontrollerar att säkerhetsskyddsklassificerade uppgifter uppnår tänkt säkerhetsnivå. Framställningen av vägledningen baseras utifrån tolkningar av bland annat Säpos vägledning för hur klassificering av uppgifter bör hanteras.

Verksamheter måste vara införstådda med att det endast är de själva som har ansvaret för att klassificering och värderingen av uppgifter är korrekt utförda. Vägledningen ska endast betraktas som ett hjälpmedel för klassificeringsarbetet. Den ska inte ses som en fullständig lösning för hur klassificeringsarbetet ska gå till.

12. Referenser

Offentlighets- och sekretesslag (2009:400) (OSL)

Säkerhetsskyddslagen (2018:585)

Säkerhetsskyddslagen (2021:955)

Säkerhetsskyddsförordning (2018:658)

Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen)

Säkerhetspolisens Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd (2019)

Energiföretagen Sverige • www.energiforetagen.se