Från: [redacted]

Ärende: Remiss om förslag på vägledning till föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn, dnr 2021-42391

Datum: den 24 maj 2022 08:50:40

Bilagor:
image001.png
image002.png
image003.png
Kopia av Feedback - Vägledning till föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn.xlsx
Missiv - Vägledning NIS remiss.docx

” Statens Energimyndighet (STEM) har tagit fram förslag på vägledning tillhörande Energimyndighetens föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn i enlighet med lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (”NIS-lagen”) STEFS 2021:3.

STEM ger er härmed tillfälle att yttra er över förslaget till vägledning för föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn.

Skriftligt yttrande emottages tacksamt senast 4 juli 2022.

Övrig information finns bifogat i detta mejl.

Vänligen”

Registrator
Energimyndigheten
Tel. +46 (0)16 542 06 39
www.energimyndigheten.se

Avdelningen för systemanalys, försörjningstrygghet och statistik
Enheten Tillsyn försörjningstrygghet
Titti Norlin
0(0)16-544 22 73
titti.norlin@energimyndigheten.se

Remiss av förslag på vägledning till föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn (s.k. ”NIS-föreskrifter”)

Statens Energimyndighet (STEM) har tagit fram förslag på vägledning tillhörande Energimyndighetens föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn i enlighet med lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (”NIS-lagen”) STEFS 2021:3.

STEM ger er härmed tillfälle att yttra er över förslaget till vägledning för föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn.

Bakgrund

EU:s NIS-direktiv trädde i kraft år 2016 och det implementerades i Sverige genom NIS-lagen som trädde i kraft år 2018. Energimyndighetens föreskrift trädde i kraft 1 mars 2021 och återfinns på Energimyndighetens webbshop. Syftet med lagen är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för såväl samhällsviktiga som digitala tjänster. Med stöd av vägledningen ska energiföretagen kunna höja sin leveranssäkerhet avseende sin samhällsviktiga tjänst genom att reducera störningar och avbrott som beror på informationssäkerhetsincidenter.

Förslagets innehåll

Målet med denna vägledning är att aktörer inom energisektorn ska kunna få praktisk vägledning i *hur* kraven i föreskriften *kan* genomföras.

Vidare att:

- Komplettera föreskriften med praktiska vägledningar
- Ge vägledning till företagen i hur föreskriften kan tillämpas i energiföretagens verksamheter
- Omsätta de allmänna råden till mer praktiska råd.

Ert yttrande

Om ni vill yttra er över förslaget till vägledning ska ett skriftligt yttrande ha inkommit till STEM **senast måndag 4 juli 2022**. Vi föredrar att era kommentarer återfinns i det Excel ark som bifogas. Svar ska skickas till registrator@energimyndigheten.se, och märkas med diarienummer **2021-042391**.

Frågor om remissen kan skickas till nistillsyn@energimyndigheten.se.

Handläggare för remissen är enhetschefen Titti Norlin.

De handlingar som bifogas är:

- Förslag på vägledning föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för energisektorn.
- Excel ark för feedback – Vägledning till föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn.
- Missiv – Vägledning till föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn.

Sändlista

Samverkansmyndigheter inom NIS

- Myndigheten för samhällsskydd och beredskap
- Transportstyrelsen
- Livsmedelsverket
- Post och telestyrelsen
- Inspektionen för vård och omsorg
- Finansinspektionen
- Socialstyrelsen

Andra myndigheter

- Tillväxtverket (Regelrådet)
- Försvarets radioanstalt
- Säkerhetspolisen
- Totalförsvarets forskningsinstitut
- Försvarets materielverk
- Polismyndigheten
- Datainspektionen
- Affärsverket svenska kraftnät
- Energimarknadsinspektionen

Andra mottagare

- Sveriges Kommuner och Regioner
- Svensk Drivkraft
- Energigas Sverige
- Energiföretagen
- Energidataföreningen

Energimyndigheten

Krav nummer

Energimyndigheten

Kommentar

Remissutgåva vägledning

Innehåll

1. Inledning 2
   1.1 Syftet med regleringen och med vägledningen 3
   1.2 Målet med vägledningen 3
   1.3 Avgränsning för vägledningen 3
   1.4 Målgrupp för vägledningen 3
   1.5 Läsanvisning 3
2. Vägledning krav 5
   2.1 Analys för identifikation av nätverk och informationssystem för Samhällsviktig tjänst 5
   2.2 Riskanalys för identifierade nätverk och informationssystem samt säkerhetsåtgärder 6
   2.3 Informationssäkerhetskrav 13
      2.3.1 Tillgångshantering 13
      2.3.2 Skydd av Nätverk och Informationssystem 22
      2.3.3 Säkerhetskopiering och redundans 36
      2.3.4 Införande av Informationssäkerhetskraven 42

1. Inledning

Det finns två stora trender i dagens samhälle som är extra viktiga för hur informationssäkerhet kan och bör bedrivas för leverantörer av samhällsviktiga tjänster inom energisektorn.

- För det första blir beroenden mellan olika samhällsviktiga funktioner allt starkare, vilket leder till ökade risker för spridning av störningar från exempelvis elförsörjning till andra samhällssektorer och geografiska områden.
- För det andra blir ansvaret för drift, underhåll, och planering av olika typer av samhällsviktiga verksamheter alltmer uppdelat på olika aktörer, både offentliga och privata. Detta gör att även ansvaret för, och arbetet med, riskhantering och säkerhetsåtgärder blir alltmer uppdelat.

Tillsammans skapar de två trenderna stora utmaningar för informationssäkerhetsarbetet inom energisektorn.

Energiinfrastruktur är rimligen en av de mest komplexa och kritiska infrastrukturerna i ett modernt samhälle. Den utgör oftast grunden för ekonomiska aktiviteter och för att kunna upprätthålla samhällets funktionalitet. Givet att energisektorn levererar samhällsviktiga tjänster till stora delar av samhället är det av största vikt att informationssäkerheten möter risker och beroenden även i andra och tredje led, då risken för kaskadeffekter är stor.

Digitaliseringen erbjuder nya möjligheter att koppla samman existerande och kommande energisystem, samt att påskynda uppluckringen av energisystemets traditionella gränser mellan efterfrågan och produktion av energi. Utöver systemnyttan erbjuder digitaliseringen även möjligheter för en minskad energianvändning i kombination med en ökad kundnytta. Det innebär att digitaliseringen bland annat kommer att bli ett centralt verktyg för att nå dagens högt ställda energi- och klimatmål inom samhället.

Med en alltmer distribuerad och variabel elproduktion, innebär den omvandling som energisystemet för närvarande genomgår, växande utmaningar när det gäller att balansera produktion och användning, i realtid. Elsystemet digitaliseras inte bara på grund av nya behov och möjligheter utan även som konsekvens av de nya komponenter som tillkommer i systemet så som elfordon, serverhallar och vindkraft. Ett modernt energisystem som blir alltmer beroende av kvalificerade nätverk och informationssystem.

Digitaliseringen är en förutsättning för en konkurrenskraftig och flexibel marknad för energitjänster, men den kräver samtidigt en digital energiinfrastruktur som är säker, effektiv och motståndskraftig.

Den förestående vägledningen till Energimyndighetens föreskrifter och allmänna råd (STEMFS 2021:3) om *riskanalys och säkerhetsåtgärder för nätverk och informationssystem* inom energisektorn (härefter "föreskriften"), har tagits fram för att pedagogiskt förklara hur Energimyndigheten ser att föreskrifterna och allmänna råden *skulle kunna* omsättas i praktiskt handlande. Målet är också att förklara kraven i en för energisektorn relevant kontext.

Arbetet med vägledningen har skett tillsammans med aktörer på marknaden, andra myndigheter och konsulter.

1.1 Syftet med regleringen och med vägledningen

Syftet med NIS-lagstiftningens genomförande inom energisektorn är att säkerställa informationssäkerheten och i förlängningen trygga energiförsörjningen.

Energiförsörjningens tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och marknadens funktion.

Med stöd av vägledningen ska energiföretagen kunna höja sin leveranssäkerhet avseende sin samhällsviktiga tjänst genom att reducera störningar och avbrott som beror på informationssäkerhetsincidenter.

1.2 Målet med vägledningen

Målet med denna vägledning är att aktörer inom energisektorn ska kunna få praktisk vägledning i *hur* kraven i föreskriften *kan* genomföras.

Vidare att:

- Komplettera föreskriften med praktiska vägledningar
- Ge vägledning till företagen i hur föreskriften kan tillämpas i energiföretagens verksamheter
- Omsätta de allmänna råden till mer praktiska råd.

1.3 Avgränsning för vägledningen

Denna vägledning avgränsas till enbart de beslutade kraven i föreskriften och de efterföljande allmänna råden.

Det är också viktigt att förstå att det är föreskriften som beskriver kraven – vägledningen beskriver; *exempel* på hur föreskriften *skulle kunna omsättas* i praktiskt handlande, förklaringar kring varför dessa åtgärder är viktiga och ytterligare referenser för att underlätta arbetet. Beslutet om vad som ska genomföras i verksamheten för att nå upp till kraven i regleringen är fortfarande en fråga för leverantörens egen analys och Energimyndighetens påföljande tillsyn.

1.4 Målgrupp för vägledningen

Målgrupp för vägledningen är primärt energiaktörernas ansvariga för informationssäkerhet, samt IT- och OT-tekniker.

1.5 Läsanvisning

Vägledningen har delat in föreskriften i ett antal områden, med tillhörande krav. Områdena följer inte föreskriftens juridiska ordningsföljd, utan har strukturerats om för att underlätta för läsaren, och för uppfyllandet av föreskriften.

Varje krav har ett ID, en referens till föreskriften, en referens till de allmänna råden samt referenser till informationssäkerhets- och OT-säkerhetsstandarder. Läshänvisningen ger i många fall förslag på ytterligare åtgärder som är *relevanta*, men som kan gå utanför de explicita kraven i föreskriften.

För uppfyllande av kraven från föreskriften kan referenserna till informationssäkerhets- och OT-säkerhetsstandarden utgöra stöd för att säkerställa att en verksamhet som redan har ett ledningssystem för informationssäkerhet som är baserat på en informationssäkerhetsstandard, snabbt kan se ifall verksamheten uppfyller varje specifikt krav som framgår av föreskriften.

Tanken med föreskriften är inte att en verksamhet skall skapa ett nytt ledningssystem för att uppfylla föreskriften. Föreskriften ställer krav på ytterligare säkerhetsåtgärder som skall inkluderas i ett Ledningssystem för informationssäkerhet. MSBFS 2018:8, 5 §, första stycket, föreskriver att en leverantör skall bedriva ett systematiskt och riskbaserat arbetssätt *med stöd av ISO/IEC 27001:2017 och ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.*

2. Vägledning krav

2.1 Analys för identifikation av nätverk och informationssystem för Samhällsviktig tjänst

Krav 1: Leverantören ska identifiera vilka nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster genom att analysera sina nätverk och informationssystem.
Föreskrift: 1 kap. 2 §
Allmänt råd 1 kap. 2 §: Vid fastställandet av vilka nätverk och informationssystem som ingår i leverantörens tillhandahållande av samhällsviktiga tjänster, och vad som därmed omfattas av leverantörens riskanalys, kan leverantören använda den kartläggning som ska utföras enligt 3 kap. 2 § punkt 1 och 4 denna föreskrift. I analysen bör leverantören ta ställning till vilka delar av leverantörens nätverk och informationssystem som behövs för att kunna upprätthålla kontinuerligt tillhandahållande av samhällsviktiga tjänster, samt vilka delar av nätverket och informationssystemet som kan påverka tillhandahållandet om de inte fungerar på grund av bristande säkerhet. I analysen bör leverantören även ta ställning till vilka applikationer och verktyg som krävs för att åtgärda krav från tidigare riskanalyser och informationssäkerhetskrav enligt 3 kap.
Referenser: MSB: MSBFS 2021:9

För att identifiera en samhällsviktig tjänst, se MSBFS 2021:9.

När den samhällsviktiga tjänsten identifierats ska en analys genomföras för att utreda vad tjänsten består av och identifiera vilka nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten. Analysen kan genomföras genom en workshop där olika delar av verksamheten tillsammans identifierar regulatoriska krav på tjänsten, kundernas avtalade specifikationer och förväntningar, samt dokumenterar vilka nätverk och informationssystem som används för att kunna leverera tjänsten.

Grunden till identifieringen av nätverk och informationssystem är uppfyllandet av krav 7.1 – 7.5.

Analysen och resultatet ska dokumenteras. Ett av resultaten kan vara en nätverkskarta, se krav 7.5.

2.2 Riskanalys för identifierade nätverk och informationssystem samt säkerhetsåtgärder

Grunden i att arbeta systematiskt med informationssäkerhet är att utgå från de risker som verksamheten kan utsättas för. Det är genom att förstå sina informationssäkerhetsrisker som ett bra och väl avvägt skydd för informationen kan upprättas. För att kunna arbeta systematiskt med era informationssäkerhetsrisker måste ni som verksamhet ha en riskanalysmodell att utgå ifrån. Krav 2-6 nedan beskriver de krav som ställs på riskanalysmodellen.

Det rekommenderas att ni som verksamhet utgår från en redan fastställd riskanalysmodell, om sådan finns. Det rekommenderas även att en och samma modell används för hela er verksamhet, inte enbart när informationssäkerhetsrisker bedöms, och gärna att samma modell används över längre tidsperioder. Samma modell bör används för att exempelvis bedöma kvalitets- och miljörisker. Genom att använda samma modell kan riskvärden för olika risker jämföras och prioriteras.

För att få stöd i riskanalysarbetet, samt hitta mallar, rekommenderas webbsidan informationssäkerhet.se eftersom där har MSB har samlat erfarenheter för hur arbetet med informationssäkerhet bör bedrivas, däribland genomförandet av riskanalyser. Informationsäkerhet.se drivs av MSB och kopplar mot MSB:s föreskrift om kravet på systematiskt informationssäkerhetsarbete.

Krav 2: Leverantören ska genomföra en riskanalys för de identifierade nätverken och informationssystemen. Riskanalysen ska innehålla en bedömning av konsekvens och sannolikhet, varvid risken tilldelas ett riskvärde.
Föreskrift: 2 kap 1 § 1-2 st.
Allmänt råd 2 kap. 1 § I samband med utförandet av riskanalysen kan leverantören ta i beaktande hur befintliga säkerhetsåtgärder påverkar de identifierade riskernas sannolikhet eller konsekvens. I samband med riskanalysen kan följande behöva beaktas för OT: 1. Realtidsfunktionalitet, en mycket kort störning kan få stora konsekvenser, 2. En mindre störning i OT kan få följdverkningar och innebära stor påverkan på omkringliggande informationssystem, 3. OT kan vara föråldrat på så sätt att det inte är avsett att vara uppkopplat enligt nuvarande användning. Detta kan medföra särskild sårbarhet i leverantörens nätverk och informationssystem. Leverantörens bedömning i riskanalysen av de incidenter som kan uppstå i dess nätverk och informationssystem bör avse både incidenter som kan ske direkt i dessa, liksom incidenter som kan uppstå utanför leverantörens nätverk och informationssystemen men som kan påverka dem. Leverantören bör i riskanalysen beakta risker som kan påverka tillgänglighet, riktighet eller konfidentialitet i leverantörens nätverk och informationssystem. Även risker som kan påverka befintliga säkerhetsåtgärder i leverantörens nätverk och informationssystem bör beaktas. Incidenter som bör ingå i riskanalysen kan exempelvis vara antagonistiska angrepp, tekniska fel, fel orsakade av människa eller naturpåverkan.

Referenser:
ISO 27001: 6.1.2
ISO 31000
NIST: ID.RA-4
NIST SP 800-53 rev 5.: RA-3
NIST SP 800-30
ISA/IEC 62443-3-2

Genomförandet av riskanalys bör ägas av en verksamhetsansvarig, men flera individer i verksamheten bör inkluderas i arbetet. Det blir sällan en bra riskanalys när en individ själv genomför riskanalysen. Det är när flera individer deltar i riskanalysen, som resultatet blir som bäst. Alla individer bidrar med sina perspektiv på riskanalysen utifrån erfarenhet samt funktion och det blir lättare att identifiera förgivettaganden. För genomförandet av riskanalys för nätverk och informationssystem för samhällsviktiga tjänster, rekommenderas att det finns deltagare med kompetens från både IT och OT. Ta i beaktning att även ha med funktionsföreträdare eller aktörer som kan komma att bli föremål för att vidta åtgärder.

Vidare rekommenderas att den riskanalys för nätverk och informationssystem som används vid tillhandahållandet av en samhällsviktig tjänst, delas upp med en riskanalys per nätverk och informationssystem. Genom att genomföra en riskanalys per nätverk och informationssystem kommer ni som verksamhet att enklare kunna identifiera specifika hot mot det de enskilda nätverken och informationssystemen och därefter bättre anpassat kunna vidta åtgärder mot dessa identifierade hot. För OT kan uppsättandet av olika OT-nätverk vara väldigt snarlikt, om inte identiskt i vissa fall. För analys av dessa nätverk kan det vara fördelaktigt och tidssparande att genomföra en riskanalys, som sedan är applicerbar för andra OT-nätverk som är byggda på samma sätt.

Ett viktigt ingångsvärde i att göra en bra riskanalys är att förstå vilka tillgångar som finns för varje nätverk och informationssystem. Identifiering av tillgångar för respektive nätverk och informationssystem återfinnas i krav 7.2-7.7.

Vid upprättandet av den riskanalysmodell som er organisation ska använda, ska modellen innehålla en bedömning av riskens konsekvens och sannolikhet. Konsekvens och sannolikhet ska utgå ifrån olika skalor. Antalet nivåer på skalan kan variera, men rekommendationen är att från början bör fyra nivåer användas, detta på grund av att vid 5 nivåer i skalan är det lätt att deltagarna vid bedömningen anger medelvärdet, 3:or. Nivåerna kan se ut som följande;

- Väldigt hög
- Hög
- Låg
- Väldigt låg

Vid fastställandet av nivåerna på skalorna för konsekvens och sannolikhet ska ett antal aspekter beaktas. Avseende konsekvens kan nivåerna utgå ifrån två perspektiv, att nivåerna baseras på monetär skada och att nivåerna utgår ifrån den skada och det tidsperspektiv som en konsekvens drabbar verksamheten med. Båda perspektiven har sina för och nackdelar och kompletterar varandra. Det monetära perspektivet gör det enkelt för användaren av modellen att förstå vilken konsekvens en risk kan få, medan det blir svårt att avgöra vilken konsekvens i monetära siffor en risk kan få. Det andra

perspektivet, att utgå ifrån skada och tidsperspektiv, gör det enklare att göra bedömningen av vilken konsekvens en risk får, men nackdelen är att modellen blir väldigt svårförståelig.

För samhällsviktiga tjänster, är det nödvändigtvis inte det monetära perspektivet som är det viktiga, och det är också svårt att bedöma de samhällskonsekvenserna utifrån monetära skador. En sådan nivåskala kan se ut enligt följande:

- Väldigt hög-*Väldigt hög direkt eller indirekt skada på verksamheten som påverkar affärsprocessen och leveransen av samhällsviktig tjänst på kort och lång sikt.*
- Hög- *Hög direkt eller indirekt skada på verksamheten som drabbar affärsprocessen och leveransen av samhällsviktig tjänst på kort sikt, men ej på lång sikt.*
- Låg-*Låg direkt skada eller indirekt skada som drabbar affärsprocessen och leveransen av samhällsviktig tjänst på kort sikt, men ej på lång sikt.*
- Väldigt låg-*Väldigt låg, eller ingen, direkt skada eller indirekt skada. Drabbar inte affärsprocessen eller leveransen av samhällsviktig tjänst på kort eller lång sikt.*

Sannolikhet ska också bedömas på samma antal nivåer som konsekvens, alltså rekommenderas samma antal nivåer. Sannolikhetsnivåerna ska bedömas utifrån sannolikheten att ett hot inträffar. Sannolikheten kan sättas utifrån hur sannolikt det är att en konsekvens blir realitet under ett visst definierat tidsperspektiv, inom exempelvis 1, 3 eller 5 år, beroende vad för typ av verksamhet organisationen bedriver och hur ofta man genomför riskanalyser. Sannolikhetsnivåerna kan se ut som följande:

Hur sannolikt är det att ett hot blir verklighet inom 3 år?

- Väldigt hög - >50%
- Hög - 30-50%
- Låg - 5-29%
- Väldigt låg - <5%

Utifrån bedömningen av konsekvens och sannolikhet ska riskanalysmodellen ge ett riskvärde. Riskvärdet ger er verksamhet möjlighet att se var verksamhetens största risk finns, så kallad riskexponering, samt ger er möjlighet att prioritera olika mitigerande åtgärder. Riskvärdet i modellen kan också ge er verksamhet råd i hur en risk bör mitigeras, vilket också speglas av verksamhetens riskaptit. Åtgärder ska alltså föregås av informerade beslut kring er verksamhets risk i förhållande till riskacceptans.

Risk- och sårbarhetsmodellen kan se ut som följande:

Konsekvens					
Väldigt hög	2	3	3	3
Hög	2	2	3	3
Låg	1	2	2	3
Väldigt låg	1	1	2	2
	Väldigt låg	Låg	Hög	Väldigt hög

Sannolikhet

Vid genomförandet av riskanalysen bör hot mot er verksamhet och dess information analyseras. Det kan med fördel vara scenariobaserat, för att på ett bra sätt värdera riskerna. Ett scenario kan exempelvis vara att verksamheten drabbas av lyckat ransomware-angrepp genom e-post. Varje risk/hot/scenario bör ha ett unikt risk-ID.

Metoden som ni tar fram ska huvudsakligen kunna svara på två frågor; vidtar jag rätt åtgärder och ökar min säkerhet med de åtgärder vi vidtar?

För verksamheter som redan har en riskanalysmodell och som vill förbättra sitt riskanalysarbete kan en stor förbättringspotential finnas i att identifiera förgivettaganden och uttrycka det okända. En bra metod för detta kan vara approximation med explicita konfidensintervaller. På detta sätt kan utövarna dokumentera och sätta värden på sina osäkerheter i analysen.

Krav 3: Leverantören ska införa säkerhetsåtgärder för att hantera riskerna som identifierats i 2 kap. 1 § 1-2 st. Säkerhetsåtgärden ska antingen sänka ett riskvärde eller uppfylla ett informationssäkerhetskrav i 3 kap. (Krav 7-9)
Föreskrift: 4 kap. 1 §
Allmänt råd 4 kap. 1 § För att kunna sänka en risks riskvärde bör åtgärden minska riskens sannolikhet (vara förebyggande) eller minska riskens konsekvens (avse redundans och kontinuitet) Leverantören bör utvärdera planerade säkerhetsåtgärder för att säkerställa att de inte leder till nya risker i leverantörens nätverk och informationssystem.
Referenser: ISO 27001: 6.1.3 NIST: ID.RA-1-6, ID.RM-1-3 NIST SP 800-30 ISA/IEC 62443-3-2

Riskanalysmodellen, som nämnts under krav 2, ska inkludera hur en risk bör hanteras, utifrån det riskvärde som risken tilldelats. Riskvärdet bör kunna ge en riktlinje för hur en risk bör mitigeras utifrån er verksamhets riskaptit.

En mitigerande åtgärd kan antingen vara att acceptera, transferera, reducera eller eliminera en risk.

- Acceptera: Risken finns, men konsekvensen och sannolikheten är så låg att verksamheten kan acceptera risken.
- Transferera: Att transferera en risk innebär att låta risken föras över till en annan part, antingen genom avtal med en avtalspart eller ett försäkringsbolag.
- Reducera: Att reducera en risk innebär att vidta en mitigerande åtgärd som antingen minskar konsekvensen eller sannolikheten, eller både två.
- Eliminera: Att eliminera en risk innebär att vidta mitigerande åtgärder så att risken inte längre finns.

En riskhanteringsmodell kan se ut som följande:

- Riskvärde 1 - Accepteras, transfereras
- Riskvärde 2 - Transfereras, reduceras, elimineras
- Riskvärde 3 - Reduceras, elimineras

Ett riskvärde kan sänkas, antingen genom att en åtgärd minskar konsekvensen vid en oönskad händelse, eller sannolikheten för en oönskad händelse. Oftast siktar en säkerhetsåtgärd till att minska sannolikheten för att en oönskad händelse inträffar, men genom att arbete med kontinuitet och redundans för viktiga processer inom verksamheten kan en risks konsekvens på verksamheten minskas.

För säkerhetsåtgärder som uppfyller 3 kap. i STEMFS 2021:3, se även krav 10 och krav 10.1.

Krav 4: I riskanalysen ska det framgå en åtgärdsplan. Åtgärdsplanen ska innehålla följande information avseende varje säkerhetsåtgärd som ingår i planen: 1. Vilken risk säkerhetsåtgärden påverkar 2. Vilket nätverk eller informationssystem som säkerhetsåtgärden ska införas inom. 3. Person eller funktion hos leverantören som ansvarar för säkerhetsåtgärden. 4. Planerad tidsram för införandet av säkerhetsåtgärden. 5. Säkerhetsåtgärdens påverkan på riskens konsekvens eller sannolikhet enligt värderingen som gjorts i 2 kap. 1 §. 6. Riskvärde efter säkerhetsåtgärdens införande.
Föreskrift: 4 kap. 2 §
Allmänt råd: 4 kap 2 § En säkerhetsåtgärd kan påverka en eller flera risker.
Referenser: ISO 27001: 6.1.3 NIST: ID.RA.1-6, ID.RM.1-3 NIST SP 800-30 ISA/IEC 62443-3-2

När riskvärderingen är genomförd och ett riskvärde är tilldelad varje risk, ska varje risk hanteras enligt den uppsatta riskanalysmodellen.

För varje risk ska en mitigerande åtgärd vidtas beroende på riskvärdet. Den mitigerande åtgärden ska antingen minska konsekvensen eller sannolikheten. Den mitigerande åtgärden ska vara tydlig, och det ska framgå på vilket nätverk eller informationssystem som åtgärden ska implementeras (om riskanalysen är uppdela per nätverk och informationssystem, enligt rekommendation i krav 2, är detta enklare). En utpekad individ eller funktion ska ansvara för att åtgärden blir implementerad, men behöver nödvändigtvis inte vara den som genomför implementeringen. Ansvarig ska säkerställa att åtgärden blir implementerad inom utsatt, och dokumenterad, tidsram.

Efter att en säkerhetsåtgärd blivit tilldelad ansvarig, samt tidsramar är satta, ska deltagarna i riskanalysen bedöma den kvarvarande risken efter att åtgärd är implementerad. Detta betyder att konsekvens och sannolikhet på nytt ska bedömas, för att se ifall riskvärdet på risken minskar och hur mycket. Minskar ej riskvärdet, har säkerhetsåtgärden ingen effekt, och bör därför ej av den anledningen vidtas, och en annan säkerhetsåtgärd bör vidtas i stället, eller en kombination av ytterligare säkerhetsåtgärder.

För säkerhetsåtgärder som uppfyller 3 kap. i STEMFS 2021:3, se även krav 10 och krav 10.1.

Krav 5: Genomförandet av säkerhetsåtgärden ska prioriteras med beaktande av leverantörens riskvärdering enligt 2 kap. 1 § samt med beaktande av de ekonomiska och tidsmässiga resurser som vidtagandet av säkerhetsåtgärden kan kräva.
Föreskrift: 4 kap. 4 §
Allmänt råd 4 kap. 4 § Leverantörens prioritering av säkerhetsåtgärder bör göras utifrån: 1. säkerhetsåtgärdens ändamål, 2. det aktuella informationssystemets kritikalitet för tillhandahållande av samhällsviktiga tjänster enligt den analys som ska göras enligt 3 kap. 2 §, punkt 1, 3. informationssystemets tekniska förutsättningar, samt 4. de kostnader och övriga resurser som införandet av säkerhetsåtgärden medför.
Referenser: ISO 27001: 6.1.3 ISO 31000 ISA/IEC 62443-3-2: ZCR 5.8 NIST SP 800-30

När ni som verksamhet ska prioritera införandet av säkerhetsåtgärderna (de mitigerande åtgärderna) skall ni beakta riskvärderingen. Risker med högt riskvärde bör prioriteras först och dess säkerhetsåtgärder, för att senare ta säkerhetsåtgärder kopplade till risker med lägre riskvärdering senare. Det kan dock finnas enkla åtgärder som identifierats under processen som ger en hög effekt i förhållande till ianspråktagna resurser, det kan då självklart vara motiverat att åtgärda dessa parallellt med högre prioriterade åtgärder.

Krav 6: Leverantören ska bedöma hur de identifierade riskerna påverkar leveransen av den samhällsviktiga tjänsten.
Föreskrift: 2 kap. 1 § 3 st.
Allmänt råd
Referenser:

För att få en så bra riskanalys som möjligt är det viktigt att tydligt beskriva de konsekvenser som ett hot kan få om det blir verklighet. Genom att tydligt beskriva konsekvenser är det enklare att vidta rätt mitigerande åtgärder.

Vid genomförandet av riskanalysen enligt krav 2-5 skall det i den beskrivande texten över ett hot, framgå hur hotet påverkar leveransen av den samhällsviktiga tjänsten, om hotet skulle bli verklighet, se krav 2.

2.3 Informationssäkerhetskrav

2.3.1 Tillgångshantering

Krav 7: Leverantören ska ha en dokumenterad process och metod för tillgångshantering. Processen och metoden ska innehålla krav 7.1-7.7.
Föreskrift: 3 kap. 1 § p. 1, 3 kap. 2 § andra st.
Allmänt råd:
Referenser: ISO 27001: A.8.1.1 ISO 27002: A.8.1.1 NIST: ID.AM-1 NIST SP 800-53 rev.5: CM-8 ISA/IEC 62443-2-1: A.2.3.3.8.2

Att ha en dokumenterad process och metod för tillgångshantering är viktigt för en aktör för att kunna skydda sina tillgångar på ett korrekt sätt över tid. En process och en metod bör innehålla ägarskap för att införskaffa och skapa tillgångar, skydda tillgångarna på ett korrekt sätt under dess livstid, samt göra sig av med tillgångarna på ett säkert sätt när de inte längre ska användas. Som minst ska processen för tillgångshantering innehålla aktiviteter för att uppfylla kraven 7.1-7.7. Vill ni som aktör skapa separata processer för respektive krav i 7.1-7.7, är det möjligt.

En process för tillgångshantering bör innehålla att tillgångsinventering ska genomföras med hjälp av systemstöd, men kan också genomföras i ett manuellt register. Det viktiga är att tillgångsinventeringen är dokumenterad och att inventeringen kan utgöra ett bra stöd för det fortsatta arbetet att skydda de identifierade tillgångarna samt som underlag för att kunna upprätta en riskanalys enligt krav 2-5.

Vid tillgångsinventering kan en aktör ha två perspektiv. Det ena är informationsperspektivet och det andra är informationsbärar-perspektivet. I informationsperspektivet är informationen i centrum för att förstå vilken information det är som ska skyddas. I informationsbärar-perspektivet är det hårdvaran, mjukvaran eller IT/OT-systemen som är i fokus, som behandlar informationen.

Krav 7.1: Kartläggning och analys av IT- och OT-tjänster samt nätverk och informationssystem som används vid tillhandahållandet av samhällsviktiga tjänster samt hur de kommunicerar med och är beroende av varandra.
Föreskrift: 3 kap. 2 § p. 1
Allmänt råd: 3 kap. 2 § p. 1 Vid kartläggningen och analysen enligt p.1 bör leverantören ta ställning till hur kritiskt informationssystemet är för leverantörens tillhandahållande av samhällsviktiga tjänster, liksom hur känslig informationen är som hanteras i informationssystemet.
Referenser: ISO 27001: A.13.2 ISO 27002: A.13.2 ISO 27 005: 8.2.2, B 1.2, samt B.1.3 NIST SP 800-53 Rev. 4: AC-4, CA-3, CA-9, PL-8

Nätverk och informationssystem är oftast inte oberoende av varandra, och kan både utgöra stöd till varandras del av en verksamhetsprocess, men de kan även utgöra sårbarheter. Er verksamhet har därmed incitament till att förstå hur olika nätverk och informationssystem kommunicerar med varandra och är beroende av varandra, för att förstå vilka sårbarheter som finns för nätverken och informationssystemen. Detta är viktigt att förstå för att kunna göra en bra riskanalys i krav 2-6.

För att kunna göra en kartläggning av IT-och OT-tjänster samt nätverk och informationssystem rekommenderas att ni som verksamheter gör en dataflödesanalys för att förstå hur er information flödar mellan olika nätverk och informationssystem. En dataflödesanalys kan med fördel göras med program som är avsedda för detta ändamål. Genom att ha visualiserat ert dataflöde, kan ni snabbt förstå hur kritiska vissa nätverk och informationssystem är, för tillhandahållandet av den samhällsviktiga tjänsten.

Krav 7.2: Inventering av hårdvaror som används för leverantörens IT och OT
Föreskrift: 3 kap. 2 § p. 2
Allmänt råd: 3 kap. 2 § p. 2 Leverantören bör hantera hårdvaruinventering enligt punkt 2 genom att upprätta en så kallad ”vitlista” med godkänd hårdvara. Nätverket bör övervakas så att leverantören uppmärksammar om en otillåten enhet kopplas upp mot leverantörens IT eller OT.
Referenser: ISO 27001: A.8.1.1 ISO 27002: A.8.1.1 ISO 27 005: 8.2.2, B 1.2, samt B.1.3 NIST: ID.AM-1 NIST SP 800-53 rev.5: CM-8

Det är viktigt för er verksamhet att ha kontroll över vilka hårdvaror som används för tillhandahållandet av en samhällsviktig tjänst. Hårdvaror kan utgöra en sårbarhet för leveransen av en samhällsviktig tjänst, och hanteras inte hårdvaror på ett korrekt sätt kan det få allvarliga konsekvenser för verksamheten. Att ha en inventering över sina hårdvaror utgör också ett stöd för att upptäcka icke-godkända hårdvaror och utrustning som inte tillhör den egna verksamheten, utan kanske som tillhör en hotaktör som försöker skaffa sig åtkomst till verksamhetens IT och OT-nätverk.

Det är viktigt att både resultatet av, och processen för, en tillgångsinventering är lättillgänglig och enkel att arbeta i för att arbetet ska kunna ske systematiskt och utan friktioner. En tillgångsinventering för hårdvaror bör hanteras genom en, för ändamålet anpassad, applikation. Men inventeringen kan även göras i ett manuellt register.

Tillgångsinventering bör innehålla:

- Vad det är för typ av hårdvara
- Modell av hårdvara
- Vem som är ansvarig för hårdvaran
- När hårdvaran togs i bruk
- Planerad att tas ur bruk
- Var hårdvaran fysiskt finns.
- Om det finns några hälso- eller säkerhetsrisker (*safety*) med hårdvaran som måste tas i beaktning. (Specifikt för OT-hårdvara)
- Om hårdvaran används för leveransen av den samhällsviktiga tjänsten, direkt eller indirekt

Hårdvaruinventeringen/hårdvarulistan kan senare används som en så kallad vitlista. En hårdvaru-vitlista är en lista över tillåtna enheter som får koppla upp sig på, eller vara en del utav, ett OT- eller IT-system. Det är enbart de tillåtna hårdvaruenheterna som ska kunna komma åt nätverket. Hårdvaruenheter som ej är del av vitlistan ska ej kunna koppla upp sig, eller komma åt OT- eller IT-systemen. En hårdvaru-vitlista används för att skydda OT- och IT-system mot hotaktörer som vill skaffa sig åtkomst till OT- och IT-systemen.

Krav 7.3: Inventering av mjukvaror som används för leverantörens IT och OT
Föreskrift: 3 kap. 2 § p. 3
Allmänt råd: 3 kap. 2 § p. 3 Leverantören bör hantera mjukvaruinventering enligt punkt 3 genom att upprätta en så kallad ”vitlista” med godkänd mjukvara. Leverantören bör övervaka sin mjukvara i syfte att möjliggöra upptäckt av en otillåten installering (eller installation) i leverantörens nätverk och informationssystem.
Referenser: ISO 27001: A.8.1 ISO 27002: A.8.1 ISO 27 005: 8.2.2, B 1.2, samt B.1.3 NIST: ID.AM-2 NIST SP 800-53 rev.5: CM-8

Att ha kontroll över vilka mjukvaror som används inom er verksamhet är lika viktigt som vilka hårdvaror som en organisation äger. Att ha kontroll på vilka mjukvaror som er verksamhet har ger både ekonomiska och säkerhetsmässiga fördelar. Från ett ekonomiskt perspektiv kan er verksamhet spara pengar på att veta hur många licenser som verksamheten har, samt hur många licenser som används. Från ett säkerhetsperspektiv ger kontroll över de mjukvaror som används en bra bild över de sårbarheter som introduceras till verksamheten. Genom att veta vilka mjukvaror som används inom verksamhet kan man snabbt få en överblick om er verksamhet är påverkad när information om nya sårbarheter framkommer samt snabbt vidta mitigerande åtgärder för att stänga sårbarheten, om det är genom att sluta använda mjukvaran eller installera en uppdaterad version.

En mjukvaruinventering bör innehålla:

- Namn på mjukvara
- Produkt ID
- Version av mjukvara
- Hur många licenser organisationen har
- Hur många användare av mjukvaran organisationen har
- Vilka användare som har mjukvaran installerad.
- Om mjukvaran används för leveransen av den samhällsviktiga tjänsten, direkt eller indirekt

Ni kan upprätthålla en mjukvaruinventering genom; dels en programvara, Software Asset Management-verktyg (SAM), dels genom att upprätthålla inventeringen i ett manuellt register. Fördelen med ett SAM-verktyg är att dessa oftast brukar vara smartare, har möjligheten att söka igenom IT-miljöer efter programvaror samt ha kontroll på när licenser går ut. Att ha inventeringen i ett manuellt register kan snabbt leda till att det manuella registret blir föråldrat.

Vidare, för att ni ska få ytterligare bättre kontroll över vilka mjukvaror som används, bör en vitlista användas. En vitlista för mjukvara används genom att er organisation bestämmer vilka mjukvaror som får installeras och användas på de interna nätverken. En mjukvara som ej är på vitlistan kan således ej installeras eller användas.

Krav 7.4: Identifiering av vilka interna och externa nätverk och informationssystem, liksom vilka hårdvaror och mjukvaror som är mest kritiska för leverantörens tillhandahållande av samhällsviktiga tjänster.
Föreskrift: 3 kap. 2 § p. 4
Allmänt råd: 3 kap. 2 § p. 4 Systemförteckningen kan vara manuellt upprättad eller genererad genom övervakningsapplikationer. Om en övervakningsapplikation används för att identifiera informationssystem och flöden bör applikationen även konfigureras till att larma vid påträffande av nya system och flöden.
Referenser: ISO 27001: Saknas, specifik åtgärd för NIS. NIST: ID.AM.4 NIST SP 800-53 Rev. 5: AC-20, SA-9 ISA/IEC 62443-2-1 A.2.3.3.8.4

Genom identifieringen av interna och externa nätverk och informationssystem enligt krav 1, och identifieringen av de hårdvaror och mjukvaror som används enligt krav 7.1, 7.2 och 7.3, ska er organisation bedöma vilka av dessa som är mest kritiska för tillhandahållandet av den samhällsviktiga tjänsten.

Vilka nätverk och informationssystem, hårdvaror och mjukvaror som är mest kritiska för tillhandahållandet av den samhällsviktiga tjänsten framkommer utav riskanalysen; genom konsekvensbedömningen, där de nätverk och informationssystem (om riskanalysen är uppdelad med en riskanalys per nätverk och informationssystem) med högst genomsnittlig konsekvens för sina hot borde vara de mest kritiska för tillhandahållandet av den samhällsviktiga tjänsten.

Krav 7.5 En upprättad nätverkskarta avseende leverantörens IT och OT.
Föreskrift: 3 kap. 2 § p. 5
Allmänt råd:
Referenser: ISO 27001: A.13.2 ISO 27002: A.13.2 ISO 27 005: 8.2.2, B 1.2, samt B.1.3 NIST: ID.AM.3 NIST SP 800-53 Rev. 5: AC-4, CA-3, CA-9, PL-8 ISA/IEC 62443-2-1 A.2.3.3.8.4

Att ni som verksamhet har koll och kontroll över ert närverk är viktigt, dels för att förstå vilka förbättringar ni som verksamhet kan göra i era nätverk, dels för att förstå vilka sårbarheter som era nätverk har. Genom att ha en nätverkskarta/nätverksdiagram blir det enklare för en organisation att felsöka i ett nätverk vid problem, men också enklare att kunna dimensionera skyddet i nätverket.

En nätverkskarta/nätverksdiagram är en översiktsbild över hur nätverket ser ut, inkluderat hur datorer och nätverk sitter ihop, identifierar komponenter som routrar, brandväggar och enheter samt visar visuellt hur dessa samverkar.

Det finns produkter på marknaden som automatiserar processen med att skapa en nätverkskarta. Vid användandet av dessa produkter ska ni som verksamhetsutövare vara försiktiga, för dessa produkter kan fortfarande missa viktiga komponenter, vilket gör att viss handpåläggning fortfarande kan krävas.

Krav 7.6: Hantering av förändringar i nätverk och informationssystem med metoder som minimerar risk för störning eller förändringar i IT och OT:s informationssäkerhet.
Föreskrift: 3 kap. 4 § p. 2
Allmänt råd:
Referenser: ISO/IEC 27002:2017 12.1.2, 14.2.2--4 ISO/IEC 27019:2020 12.1.2 ISA/IEC 62443-2-1 4.3.4.3.2--5, A.3.3.5.3.12, A.3.4.3.6 NIST-CSF PR.IP-3 NIST SP 800-53 Rev. 5: CM-3, CM-4, SA-10 ATT&CK ICS: T0800, T0821, T0835, T0836, T0839, T0845, T0851, T0857, T0858, T0872, T0873, T0878, T0881, T0889

Som utfall av exempelvis ett underhåll, sårbarhetscanning eller organisatoriska förändringar kan ett ändringsbehov uppstå för ett nätverk eller informationssystem. Detta kan till exempel vara behovet av mjukvaruuppdateringar, ändringar i brandväggsregler, skapandet av nya konton eller åtkomsträttigheter. För att hantera dessa ändringar ska en process införas - ändringshanteringsprocess (Change Management process).

Anledning till att ni ska ha en ändringshanteringsprocess är för att säkerställa att en ändring inte medför en risk för personskador-, drifts- eller informationssäkerheten, och för att säkerställa att en ändring resulterar i det som var avsett, samt att en ändring inte får oavsiktliga konsekvenser på systemet själv eller kringliggande system. Ansvaret för korrekt genomförande av ändringshanteringsprocessen måste vara tydligt definierat. När ändringar genomförs av underleverantörer (till exempel av en leverantör av en managerad tjänst) bör kraven på ändringshanteringsprocessen fastslås i tjänsteavtalet.

Ni som verksamhet bör sätta upp kriterier för när en ändring kräver hantering efter ändringhanteringsprocessen. Rekommendationen är att en ändring bör följa ändringshanteringsprocessen om ändringen ökar de ovan nämnda riskerna.

ISO/IEC 27002:2017 12.1.2 beskriver kraven för vad en sådan process bör innehålla. Notera att i OT miljöer så bör följande beaktas, utöver rekommendationerna i 12.1.2:

- Ändringar i hårdvaran medför ofta ändringar i informationssystem eftersom mjukvara ofta är inbyggt i dessa system (jämför ISO/IEC 27019:2020 12.1.12).
- Vid ändringar i OT system bör även risker kring personskador och fysisk skada till utrustning beaktas (jämför ISA/IEC 62443-2-1 A.3.3.5.3.12).
- Acceptansprovning inför leverans (FAT), acceptansprovning efter leverans (SAT) och integrationsprovning (SIT) kan med fördel integreras i ändringshanteringsprocessen när det gäller nyförvärv eller stora ändringar av OT utrustning (jämför IEC 62381:2012).

Krav 7.7: Hantering av informationssystem som upphört att användas för att säkerställa att känslig information inte avslöjas.
Föreskrift: 3 kap. 4 § p. 3
Allmänt råd:
Referenser: ISO/IEC 27002:2017 8.2.3, 8.3.2, 11.2.7 ISO/IEC 21964 ISA/IEC 62443-2-4 SP 03.10 RE(4) NIST-CSF PR.DS-3 NIST SP 800-53 Rev. 5: CM-8, MP-6, PE-16 NIST SP800-88

För att upprätthålla god informationssäkerhet bör er tillgångshanteringsprocessen inkludera regelverk för hur informationshanteringssystem skall hanteras när de upphört att användas. Skälet till detta är för att dels det inte ska finnas system som inte längre används som kan utgöra en sårbarhet för informationssystem och nätverk som fortfarande används i verksamheten, dels för att information som finns i dessa informationssystem som inte används längre inte ska kunna hamna i händerna hos konkurrenter eller hotaktörer.

När ett informationssystem når slutet av sin livscykel, ska all känslig information raderas från systemet innan det avvecklas. Det inkluderar till exempel loggfiler, nätverkskonfiguration, användarkonton, certifikat, lösenord, och produktionsdata. Hos andra system som var kopplade till det avvecklade systemet ska konfiguration också uppdateras för att radera relaterade inställningar (till exempel åtkomsträttigheter, brandväggsregler, proxy-inställningar).

För vissa moderna lagringsmedium (t.ex. USB-minnen, SSD-disk) är det mycket svårt att säkerställa att information inte kan återställas av en angripare med goda tekniska resurser och kompetens. Därför rekommenderas det att sådana enheter destrueras fysiskt, i stället för att bara radera data på dem.

Om känslig information som finns lagrad i informationssystemet behövs efter systemets livstid, ska denna information på ett säkert sätt överföras till ett lagringssystem som skyddas proportionerligt till informationens känslighet.

Ansvaret för att genomföra dessa åtgärder bör vara tydligt definierad i tillgångshanteringsprocessen (eller motsvarande hos er verksamhet), och den ansvariga bör ha tillgång till rätt teknisk kompetens för att kunna hantera avvecklingsprocessen korrekt.

ISO/IEC 27002:2017 ger allmänna råd kring hantering av informationssystem i slutet av deras livscykel. ISO/IEC 21964 och NIST SP800-88 ger specifika råd kring radering eller destruktion av känsliga data på lagringsmedia.

Krav 7.8: Leverantören ska utföra loggning av tillgångarna i syfte att möjliggöra upptäckt, larm och spårning av transaktioner och händelser.
Föreskrift: 3 kap. 1 § p. 2
Allmänt råd:
Referenser: ISO/IEC 27001:2017 A.12.4 ISO/IEC 27002:2017 A.12.4 NIST-CSF DE.AE-3 NIST SP 800-53 Rev. 5: AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 NIST SP 800-92 ISA/IEC 62443-3-3: SR 2.8 NIST SP 800-82r2: 5.16

Loggning är ett fundamentalt område inom IT och OT, oavsett om man pratar om säkerhet, drift, felsökning eller användarspårning. Säkerhetsloggning kan användas av er som ett verktyg för att hitta oönskad aktivitet i system, men kräver fortlöpande säkerhetsarbete, utveckling och uppföljning.

Er verksamhet bör upprätta mål och rutiner för att implementera säkerhetsloggning i nya såväl som befintliga system, och kontinuerligt följa upp efterlevnad.

Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras och granskas regelbundet.

Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst. Systemadministratörers och systemoperatörers aktiviteter ska loggas och loggarna ska skyddas och granskas regelbundet.

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän ska synkroniseras mot en och samma säkra och robusta referenskälla för tid.

För att inte bli överväldigad av information, bör ni analysera vilka aktiviteter i ett system som genererar loggdata som är relevant för säkerhetsarbetet, för att sedan se till att detta är informationen som vidarebefordras till en central plats där analys regelbundet utförs. Undvik att skicka samtlig loggdata ett system kan generera till samma punkt, då säkerhetsarbetet kan försvåras om man vid analys måste ta hänsyn till och gallra bort driftrelaterade logghändelser. Se till att loggningsnivåerna är hanterbara.

Lägg tid på analysen i samband med implementation av nya system, eller då nya funktioner tillkommer, och gör bedömningen om vilka loggar (om några) som är av relevans för säkerhetsarbete.

Separation av rättigheter är viktigt. En systemadministratör bör inte ha rättigheter att manipulera en central lagring av säkerhetsloggar, då ALL användaraktivitet skall sparas och medföra möjlighet till granskning av användaraktivitet.

Här är det viktigt att säkerställa att loggdata inte kan manipuleras i efterhand, till exempel genom att lagra detta på lagringsytor som inte möjliggör raderande eller manipulerande av data. Ett exempel är att filsystemet enbart tillåter "*append*"-händelser på filer.

Det kan finnas en säkerhetsmässig vinst i att överlåta övervakning av säkerhetsloggar till en separat enhet, inom eller utanför den egna organisationen (exempelvis till en SOC), så att verksamhetsnära

individer inte har i uppdrag att övervaka sin egen aktivitet. Rekommenderad läsning: NIST SP 800-92. (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf)

2.3.2 Skydd av Nätverk och Informationssystem

Krav 8: Leverantören ska ha en dokumenterad process och en metod för att skydda sina nätverk och informationssystem. Processen och metoden för att skydda sina nätverk och informationssystem ska innehålla krav 8.1-8.8.
Föreskrift: 3 kap. 1 § p. 1, 3 kap. 3 §
Allmänt råd:
Referenser: ISO 27001: A.14.1.1 ISO 27002: A 14.1.1 NIST-CSF PR.IP-2 NIST SP 800-53 Rev. 5: PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI13, SI-14, SI-16, SI-17

Att skydda sina nätverk och informationssystem är inte en engångsaktivitet. Hot och risker kan förändras och nya kravbilder från lagstiftare och kunder kan tillkomma under ett nätverks och informationssystems livscykel. Det är därför viktigt att ni har process och metod för att skydda era nätverk och informationssystem löpande.

En process och en metod för att skydda era nätverk och informationssystem vid införskaffning eller upprättande, kallas ackrediteringsprocess. En ackrediteringsprocess hjälper er verksamhet att utforma skyddet för ett nätverk eller ett informationssystem och processen är risk- och kravbaserad.

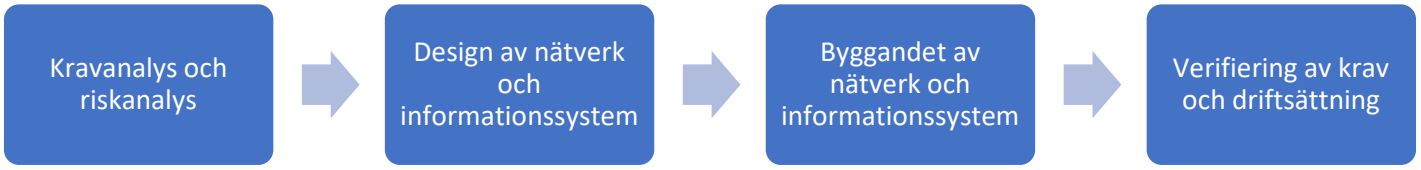
En ackrediteringsprocess kan se olika ut, men processen bör innehålla:

1. Kravanalys och riskanalys
    a. Inför inskaffandet eller byggandet av ett nätverk eller informationssystem bör en kravinsamling genomföras. Det kan vara legala krav, kundkrav, interna krav och dylikt. Kravanalysen ska dokumenteras. De legala krav är delvis de som framgår av krav 7.1-7.7 och krav 8.1-8.8.
    b. Innan inskaffandet eller byggandet av ett nätverk eller informationssystem bör även en riskanalys genomföras för att förstå riskerna med nätverket eller informationssystemet. Genom riskanalysen kan ytterligare krav framgå för vilket skydd nätverket eller informationssystemet ska ha. Riskanalysen ska dokumenteras, och dess tillkommande krav.
2. Design baserad på kravanalysen
    a. Inför byggandet av ett nätverk eller informationssystem bör en design av det nya nätverket eller informationssystemet dokumenteras och godkännas, för att säkerställa att designen uppfyller de krav som framkommit av kravanalysen och riskanalysen. Designkraven bör dokumenteras om ni som leverantör har detta processteg.
    b. Vid införskaffandet av ett nätverk eller informationssystem bör kravanalysen ligga som grund för offert mot leverantör. Design för nätverket och informationssystemet bör

granskas innan leverantör/ produkt väljs. Designkraven bör dokumenteras om ni som leverantör har detta processteg.

3. Byggandet av nätverket eller informationssystemet
    a. Efter att design godkänts utifrån dess kravuppfyllnad kan nätverket eller informationssystemet byggas utefter såsom designen dokumenterats.
    b. Vid införskaffandet av ett nätverk eller informationssystem kan nätverket eller informationssystemet sättas upp av leverantören.
4. Verifiering av krav och driftsättas.
    a. När nätverket eller informationssystemet är byggt eller införskaffat, ska de krav som framkommit i kravanalysen och riskanalysen verifieras att de är uppfyllda i nätverket eller informationssystemet. För de krav som ej är uppfyllda, ska en GAP-analys genomföras. Verifieringen ska dokumenteras. Först därefter kan nätverket eller informationssystemet driftsättas.

Ackrediteringsprocess:



Vid användandet av ackrediteringsprocess för befintliga nätverk och informationssystem kan vissa steg i processen användas för att säkerställa att nätverket och informationssystemet har ett tillräckligt gott skydd. Kravanalys och riskanalys är en viktig del för att säkerställa att befintliga nätverk och informationssystem har ett gott skydd. Riskanalysen i krav 2-6 kan med fördel användas för detta ändamål. Design av nätverk och informationssystem, byggandet av nätverk och informationssystem och verifiering av krav och driftsättning kan användas för implementeringen av åtgärder av nya säkerhetsåtgärder-tillsammans med ändringshanteringsprocessen.

Under ett nätverks- och informationssystems livscykel kan krav och risker förändras, tillkomma eller försvinna, därför är det viktigt att processen har kontinuerliga assuransaktiviteter för att säkerställa att nätverken och informationssystemen har tillräckligt gott skydd under dessas livslängd. Det är därför viktigt att riskanalysen i krav 2-6 återbesöks för att kontinuerligt förbättra skyddet.

Krav 8.1: Segmentering av nätverk och filtrera trafiken mellan olika nätverkssegment.
Föreskrift: 3 kap. 3 § p. 1
Allmänt råd: 3 kap. 3 § p. 1 Vid segmentering av nätverk enligt punkt 1, bör leverantören ta ställning till vilken typ av information som finns i segmentet, vilka säkerhetsfunktioner som är införda och om segmentet kommunicerar externt.
Referenser: ISO/IEC 27002:2017 13.1.3 ISO/IEC 27019:2020 13.1.3 ISA/IEC 62443-3-3 SR 5.1, 5.2, 5.3, 5.4 NIST-CSF PR.AC-5 NIST SP 800-53 Rev. 5: AC-4, AC-10, SC-7 NIST SP800-82r2 avsnitt 5

Rimliga nivåer för säkerheten skiljer sig från system till system. I stora, komplexa system är det inte praktiskt genomförbar att ha samma säkerhetsnivå för alla komponenter. Säkerhetsåtgärder medför alltid en kostnad, och eftersom resurser för säkerhetsarbete är begränsade så bör man arbeta målriktat i stället för generellt. Dessutom är vissa säkerhetsåtgärder som är vanliga i IT miljöer inte lämpliga i OT miljöer (till exempel automatiska uppdateringar, skärmlåsning vid inaktivitet). För att begränsa riskerna med olika säkerhetsnivåer och för att minska risken för att incident sprider sig mellan system och nätverk, bör er verksamhet dela upp sina nätverk och sina applikationer i olika nätverkssegment. Ett segment bör omfatta system som har liknande säkerhetskrav och som ofta behöver kommunicera med varandra.

Kommunikation över segmentgränserna är möjligt, men måste övervakas och kontrolleras (till exempel via en brandvägg). Ett segment kan vara fysiskt (till exempel enheter som står i samma produktionscell) eller logiskt (enheter som kan stå på olika ställen men som räknas som samhöriga på grund av deras funktion eller deras egenskaper).

Vid incidenter kan det vara nödvändigt att kapa förbindelsen mellan olika nätverkssegment för att hindra incidenten ifrån att sprida sig mellan segmenten. Därför bör nätverkssegment designas på ett sätt som möjliggör att komponenterna inom ett segment kan bibehålla sin funktion under en viss tid om segmentet isoleras från andra nätverk. Hur länge ett segment ska kunna fungera i isolerat läge bör fastställas genom en riskanalys.

Följande, ytterligare, rekommendationer kan vägleda er verksamhet i hur en bra nätverkssegmentering kan upprättas:

- Segmentering ska separera kontors-IT från produktions-nätverken (operationell teknologi - OT), s.k. vertikal segmentering.
- Det kan vara lämpligt att ytterligare dela upp nätverkssegment i subsegment, särskilt i OT-nät där segmentering bör tillämpas mellan komponenter (till exempel maskiner, servrar, *human machine interfaces* - HMI) som sällan behöver kommunicera och som har olika säkerhetskrav (horisontell segmentering).

- Kommunikationen över segmentgränserna ska i normalfall vara förbjuden och bara tillåtas efter särskild prövning (*deny by default, allow by exception*). Detta bör säkerställas via tekniska åtgärder (till exempel *default-deny* inställning i brandväggen).
- Om övervakningssystem (till exempel *Intrusion Detection System*, IDS) används för att kontrollera kommunikation över segmentgränserna, bör man fastställa profiler för vad som betraktas som förväntad kommunikation.
- Nätverkssegment som har särskilda skyddsbehov (till exempel OT-nät) bör skiljas från andra nät med hjälp av en demilitariserad zon (DMZ). Det rekommenderade tillvägagångssättet för att överföra information från ett OT-nät till ett IT-nätet är envägskommunikation med hjälp av så kallade *datadioder*. Detta är nätverksenheter som fysisk säkrar att information bara kan flöda åt ett håll (dvs från OT-nätet till IT-nätet).
- Det rekommenderade tillvägagångssättet för att överföra information från ett IT-nät till ett OT-nät är att skicka informationen från IT-nätet till en mellanlagringsplats i DMZ:n och sedan låta OT-applikationen hämta informationen därifrån. Detta gör det svårare för angripare att kringgå säkerhetsåtgärder som finns i DMZ:n och att skicka oönskad trafik direkt till OT-enheter.
- Nätverkskonfigurationen i ett segment bör döljas i kommunikation med andra segment, till exempel via *Network Address Translation* (NAT).
- Om skyddsmekanismer som är uppsatta för att kontrollera om trafiken mellan segment får driftsstopp bör de drabbade segment isoleras från nätverket (*fail-close*).
- Kommunikation mellan segment bör övervakas, till exempel med hjälp av intrångsdetektionsverktyg (*Intrusion Detection System*, IDS) eller applikationsbrandväggar (även känd som *Layer-7* brandväggar).
- Kommunikationsprotokoll som används mellan segment bör konfigureras så att de inte lämnar ut information som kan vara nyttiga för angripare i sina svar (inkluderat felmeddelanden).
- Det kan även vara nödvändigt att begränsa fysisk åtkomst till enheter i ett nätverkssegment. En risk- och konsekvensanalys bör beakta, och eventuellt fastställa, ett sådant behov.
- Trådlösa nätverk kräver särskild hantering på grund av att dess yttre avgränsningar är otydliga. För känsliga miljöer bör organisationen överväga att hantera all trådlös åtkomst som externa anslutningar.
- Segmentering kan även användas för att skydda gamla enheter som behöver bibehållas i drift men som har sårbarheter som inte går att uppdatera bort. I dessa fall kan enheten placeras i ett eget segment och kommunikationen till enheten kan skyddas med särskild hänsyn till de kända sårbarheterna (även känd som virtuell patchning)

Enheter med flera nätverkskort skapar en särskild risk för att bryta gränserna mellan nätverkssegment. Konfigurationen i dessa enheter bör därför övervakas noga för att säkerställa att de inte kringgår säkerhetsåtgärder som har satts in mellan segmentgränserna.

Krav 8.2: Minimering av användandet av administrationsrättigheter.
Föreskrift: 3 kap. 3 § p. 2
Allmänt råd: 3 kap. 3 § 2 st. För att minimera användandet av administratörsrättigheter enligt punkt 2, bör leverantören dels konfigurera sina behörighetsregler så att en administratör bara använder administrativa behörigheter i de fall det är nödvändigt, dels säkerställa att så få personer som möjligt har tillgång till administrativa behörigheter.
Referenser: ISO/IEC 27002:2017 A.9.2.3, A.9.2.5--6, A.9.4.4 ISA/IEC 62443-2-4 SP.03.08 ISA/IEC 62443-3-3 4.4 NIST: PR.AC.4 NIST SP 800-53r5 AC-6(5)

Användarkonton med priviligierade rättigheter som administrerar informationssystem är särskilt värdefulla för angripare på grund av de arbetsuppgifter man kan utföra med sådana konton och den information användaren har tillgång till. Denna sorts användare brukar dock ofta också ha andra befattningar där de utför mer vardagliga uppgifter, som inte kräver administratörsrättigheter. Vid sådana mer vardagliga arbetsuppgifter ökar angreppsmöjligheter mot användarens priviligierade konto rejält, framför allt om arbetsuppgiften innebär att användaren läser e-mejl eller besöker externa webbsidor med det privilegierade kontot. Därför rekommenderas följande:

- Skilj vanliga konton från administratörskonton (och ge således en användare med administratörsuppgifter ett vanligt och ett administratörskonto).
- Förbjud användning av administratörskonton för andra uppgifter. Om möjligt undvik att ha mjukvara som webbläsare och e-mejlklient installerad på administratörskonton.
- Använd aldrig gruppkonton för administratörsuppgifter.
- Dokumentera åtkomsträttigheter, arbetsroller knutna till dessa rättigheter och varför dessa rättigheter behövs för arbetet. Bibehåll en historik av åtkomsträttigheter även efter att de har tagits bort. Detta för att säkerställa att kunna granska åtkomsträttigheter enligt nästa punkt och för att kunna följa upp missbruk av åtkomsträttigheter.
- Granska användarens åtkomsträttigheter vid tilldelning och regelbunden därefter för att säkerställa att de bara har rättigheter de behöver för att utföra sina uppgifter.

Krav 8.3: Installering av säkerhetsuppdateringar enligt vedertagna metoder
Föreskrift: 3 kap. 3 § p. 3
Allmänt råd:
Referenser: ISO/IEC 27002:2017 A.12.1.2. NIST: PR.IP-1 NIST SP 800-53r5 CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10 ISA/IEC 62443-2-1: A.3.4.2.5.2

Informationssystem som inte har uppdaterade programvaror utgör ett hot mot verksamheten. Hotaktörer har möjlighet att upptäcka sårbarheterna som icke uppdaterad programvara innebär och utnyttja sårbarheterna. Därför är det viktigt att ni har en metod för att säkerhetsuppdatera de programvaror som används i verksamheten. Att regelbundet säkerhetsuppdatera era programvaror när uppdateringar finns tillgängliga är det mest grundläggande skyddet en verksamhet kan ha.

En metod för att systematisk hantera säkerhetsuppdateringar bör innehålla:

1. Omvärldsbevakning - För att upptäcka nya sårbarheter genom rapportering i medier. Exempelvis CERT-SE.
2. Rutiner för test och verifiering - för att kontrollera att uppdateringen överensstämmer med den av leverantörens publicerade uppdatering, och att inga kompatibilitetsproblem eller andra problem uppstår vid installation av säkerhetsuppdateringar eller nya programvaruversioner i driftsmiljön. Test bör göras i ett separat testmiljö eller i en begränsad del av driftsmiljön (exempelvis i vissa datorer). För OT-system rekommenderas leverantören att snabbt ska kunna göra en återställning till gamla versionen på kritiska system ifall uppdateringen påverkar driften.
3. Rutiner och system för distribution- så att uppdateringarna kan skickas ut snabbt och kontrollerat.
4. Rutiner och system för uppföljning- för att säkerställa att alla drabbade datorer har uppdaterat till senaste version.

För vissa informationssystem eller operationella system går det inte att genomföra säkerhetsuppdateringar omgående på grund av de konsekvenser för drift detta kan medföra.

Dessa system kan undantas från att omgående installera säkerhetuppdateringar. När säkerhetsuppdateringar finns tillgängliga bör ni ha en process som analyserar om säkerhetsuppdateringen kan installeras eller ej. Om det ej går, bör det dokumenteras att säkerhetsuppdatering ej kan göras, och skälen för att säkerhetsuppdatering ej kan göras. Vid dessa fall blir det extra viktigt att ni segmenterar era nätverk, enligt krav 8.1

Krav 8.4: Användandet av proportionerliga autentiseringsmetoder.
Föreskrift: 3 kap. 3 § p. 3
Allmänt råd: 3 kap. 3 § 3 st. När leverantören väljer proportionella autentiseringsmetoder enligt punkt 4, bör leverantören ta ställning till: 1. Vilken behörighetsnivå en användarprofil har, 2. i vilken mån åtkomst sker på distans eller från leverantörens lokaler, samt 3. Känsligheten i den information som hanteras via inloggningen.
Referenser: ISO/IEC 27002:2017 A.9.4.2 ISO/IEC 27019:2020 9.4.2 ISA/IEC 62443-3-3 5(FR 1) NIST: PR.AC.7 NIST SP 800-53 Rev. 5: AC-7, AC-8, AC-9, AC11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 ATT&CK ICS: T0800, T0806, T0811, T0812, T0816, T0822, T0830, T0831, T0832, T0838, T0839, T0842, T0843, T0845, T0848, T0855, T0856, T0857, T0858, T0859, T0860, T0861, T0866, T0868, T0883, T0871, T0885, T0886

Autentisering används för att säkerställa att en användare eller applikation som försöker komma åt ett konto eller en applikation verkligen är den som den ger sig ut för att vara. Vid bristande autentiseringsmetoder finns risk för att en hotaktör får åtkomst till känslig information eller får möjlighet att via priviligierade konton kunna utföra verksamhetspåverkande kommandon. Det är viktigt att observera att inte bara användare behöver autentisera sig, även applikationer som till exempel ett affärssystem som försöker komma åt en databas via ett applikationsprogrammeringsgränssnitt (API) ska kunna använda sig av autentisering.

Den vanligaste autentiseringsmetoden för användare brukar vara användarnamn och lösenord. Denna metod har många kända svagheter, och bör inte användas som enda skydd för åtkomst till känsliga system. En beprövad metod med bättre skyddsegenskap är så kallad multi-faktors autentisering (MFA), där användare endast beviljas åtkomst efter att framgångsrikt ha presenterat flera separata bevis för sin identitet (till exempel ett lösenord och en engångskod från en applikation i mobilen).

MFA bör framför allt användas för att skydda åtkomst till konton som har administratörsrättigheter, samt för fjärråtkomst till interna system, men bör även används i de fall det är möjligt att sätta igång MFA.

För applikationer brukar moderna kommunikationsprotokoll tillhandahålla möjligheten att skydda trafiken med bland annat autentisering. Denna funktion är dock ofta inte påslagen i grundinställningar och kräver god teknisk kunskap för att aktiveras på ett säkert sätt. Till exempel så tillåter protokollet TLS, som ligger till grunden för HTTPS, att autentisera både klienten och servern, dock är bara serverautentisering aktiverad i grundinställningen. För klientautentisering i TLS behöver man installera certifikat på klienterna och konfigurera servrarna att kräva klientautentisering.

Om en applikation tillhandahåller en API så bör denna skyddas med autentisering, även om den bara är tillgänglig i ett internt nät (Se till exempel IEC 62443-3-3 SR 1.2).

Krav 8.5: Där det är möjligt, använda antivirusprogram på enheter som är uppkopplade mot IT och OT.
Föreskrift: 3 kap. 3 § p. 5
Allmänt råd: 3 kap. 3 § 4 st. Leverantören bör använda säkerhetsåtgärder enligt punkt 5, som ger skydd mot skadlig kod i informationssystem inom OT.
Referenser: ISO/IEC 27002:2017 A.12.2.1 ISO/IEC 27019:2020 12.2.1 ISA/IEC 62443-3-3 SR 3.2 ISA/IEC 62443-2-4 SP.10.02--04 NIST: PR.MA.1 NIST SP 800-82r2 6.2.17.1 NIST SP 1058

Antivirusprogram (AV), eller dess utvecklade form *Endpoint Protection Platform* (EPP), utgör en viktig skyddsåtgärd mot skadlig mjukvara eftersom de kan övervaka enheter på en mycket systemnära nivå. Dessa kan bara fungera bra när de är aktiva över tiden, samt uppdateras kontinuerligt mot nya hot. Antivirusprogram är vanliga i IT miljöer, men deras användning i OT miljöer kräver särskilda åtgärder, så som att testa deras kompatibilitet för målsystemet, huruvida uppdateringar påverkar andra applikationer och om det bli problem med prestandan (om antivirusprogrammet till exempel skulle kunna påverka en tidskritisk process).

Det är viktigt att ni har en dedikerad process för ändringshantering av antivirusprogram i OT miljöer för att förhindra att ändringar har en negativ påverkan på kritiska processer, så som till exempel sådana som hanterar skydd av personer och utrustning mot fysisk skada (safety).

Många stora leverantörer av OT-system har särskilda rekommendationer eller till och med stödjer vissa antivirusprogram. I vissa fall genomför de tester mot sina produkter och tillhandahåller särskilda riktlinjer för konfiguration och drift.

Generellt bör vanliga Windows och Linux klienter och servrar i OT miljöer, som till exempel konsoler, operatörsstationer, *historians*, *Human-Machine-Interfaces* (HMI) och generiska SCADA system säkras med antivirusprogram som vanlig kontors-IT. För OT komponenter som till exempel programmerbara styrsystem (*Programmable Logic Controller* – PLC, *Digital Control System* – DCS, *Remote Terminal Units* – RTU), och instrument som kör tidskritiska processer eller har speciellt anpassade operativsystem bör tillverkarens rekommendationer hämtas in innan man överväger att installera antivirusprogram.

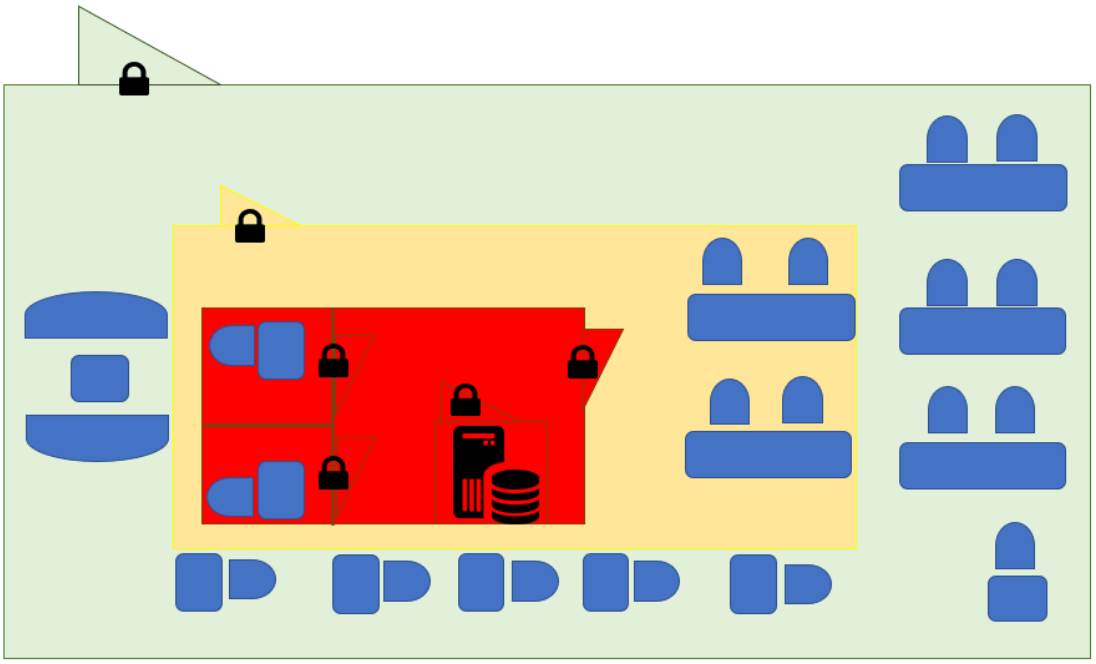
Krav 8.6 Begränsa fysisk tillgång till IT och OT.
Föreskrift: 3 kap. 3 § p.6
Allmänt råd: 3 kap. 3 § 5 st. Loggning bör ske avseende allt tillträde enligt punkt 6, till den hårdvara och de lokaler vari leverantörens nätverk och informationssystem är beläget.
Referenser: ISO 27001: A.11.1-6 ISO 27002: A.11.1-6 NIST: PR.AC-2 NIST SP 800-53 Rev. 5: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 CSI: ISA/IEC 62443-2-1 4.3.3.3 NIST SP 800-82r2 6.2.11

Det är lätt att glömma bort att fysisk säkerhet också är viktigt för att kunna ha ett systematiskt säkerhetsarbete. Att enbart fokusera på IT-säkerhet och nya IT-verktyg spelar ingen roll om en hotaktör kan gå rakt in på en arbetsplats och sätta in ett USB-minne med skadlig kod.

Principen om att enbart behörig personal ska ha åtkomst till information, gäller även för åtkomst till fysiska informationsbärare, såsom datorer, servrar och nätverksutrustning. För IT och OT-utrustning gäller det att ni begränsar åtkomsten till viktig och känslig utrustning från obehöriga, där enbart behörig personal bör ha fysisk åtkomst. Servrar och nätverksutrustning är ett intressant byte för de antagonistiska krafter som vill komma åt information och kunna skapa avbrott i processer eller kartlägga arkitekturen. Det är därför viktigt att även fysisk åtkomst till dessa utrymmen begränsas.

Till annan utrustning som behandlar information som är viktig för tillhandahållandet av den samhällsviktiga tjänsten, såsom stationära datorer eller laptops, bör ni även begränsa åtkomst till dessa till enbart de som är behörig att ta del av informationen som finns på dessa. Med fördel bör dessa datorer hanteras i ett kontorsutrymme, eller produktionsutrymme, där enbart personal har tillgång som är behörig att ta del av informationen. Dessa utrymmen bör ha låsta dörrar som öppnas med kod och kort, eller nyckel.

Säkerhetspolisen beskriver en princip för att dimensionera det fysiska skyddet, lökprincipen. Lökprincipen innebär att verksamhet som är högst skyddsvärd placeras centralt inom ett kontor/utrymme, med åtkomstbegränsningar i det fysiska skyddet. Den näst mest skyddsvärda verksamheten placeras utanför den verksamhet med högst skyddsvärd verksamhet, med fysiska åtkomstbegränsningar för att komma in i det utrymmet. Se bild för exempel:



Denna princip kan användas både för kritisk information, IT-utrustning och OT-utrustning för att skydda dessa mot obehörig åtkomst.

Krav 8.7: Regler och metoder för fjärråtkomst till leverantörens nätverk och informationssystem
Föreskrift: 3 kap. 3 § p. 7
Allmänt råd:
Referenser: ISO/IEC 27002:2017 A.6.2.2 ISO/IEC 27019:2020 6.2.2 ISA/IEC 62443-3-3 SR 1.1 RE2, SR 1.13, SR 2.6, SR 3.2 RE1 NIST PR.AC.3 NIST SP 800-53r5 AC-12, AC-17

Fjärråtkomst är en mycket viktig förmåga i ett modernt informationssystem. Den behövs till exempel för att underleverantörer ska kunna underhålla deras utrustning eller när personer behöver arbeta på distans. Däremot öppnar fjärråtkomst också nya vägar in för en hotaktör att komma åt informationssystem. Därför är det viktigt att ni bara använder fjärråtkomstlösningar där så är nödvändigt och som har följande säkerhetsegenskaper:

- Lösningen ska autentisera användaren med multifaktorsautentisering (MFA) för att minimera risken att stulna användarkontouppgifter kan användas för att få åtkomst till informationssystemet.
- Lösningen ska logga all åtkomst till informationssystemet, inklusive inloggningsförsök. Det måste finnas mekanismer implementerade för att överföra dessa loggar till verktyg som används av en Incidenthanteringsorganisation (till exempel till ett Security Information and Event Management system - SIEM), se krav 7.8, 8.9 och 9.4.
- Lösningen ska stödja åtkomstkontroll på detaljerad nivå, så att användare kan tilldelas begränsad fjärråtkomst till vissa informationssystem baserad på olika förutsättningar. Mer specifikt:
    - Det ska vara möjligt att konfigurera att användaren behöver godkännande från en lokal operatör innan användaren får fjärråtkomst till informationssystemet.
    - Det bör vara möjligt att konfigurera åtkomsträttigheter baserad på vilken tid på dygnet och vilken dag i veckan användaren begär åtkomst.
    - Det ska vara möjligt att konfigurera åtkomst baserad på grupper (t.ex., baserad på roller som användarna innehar).
- Brandväggskonfigurationer som behöver implementeras för att tillåta fjärråtkomst till ett informationssystem ska dokumenteras i detalj och sparas i Asset Management systemet.
- Lösningen ska isolera informationssystemet, dit fjärråtkomst är etablerat, från klienten som initierar fjärråtkomstuppkopplingen för att förhindra överföringen av skadlig kod.
- Lösningen bör inneha möjligheten att integreras med existerande säkerhetslösningar, exempelvis EPP, EDR; IDS eller SIEM.
- Lösningen ska stänga ner öppna fjärruppkopplingar efter en viss tid av inaktivitet.

Krav 8.8 Härdning av informationssystem innan de börjar användas, i den mån det inte medför nya risker.
Föreskrift: 3 kap. 4 § p. 1
Allmänt råd: 3 kap. 4 § Informationssystem bör härdas enligt punkt 1, bland annat genom avstängning av förkonfigurerade tjänster, ändring av lösenord på förinställda användarprofiler och avstängning av schemalagda arbeten.
Referenser: ISO/IEC 27002:2017 A.12.6.1 ISO/IEC 27019:2020 12.2.1, 12.6.1 ISA/IEC 62443-4-1 SG-3 NIST: PR.DS-3,5, NIST SP 800-53r5 CM-6, CM-7

Säkerhetshärdning av ett system, hårdvara eller en mjukvara beskriver en process där man sätter konfigurationen på ett vis som reducerar möjligheterna för en angripare att få tillgång till, eller på annat sätt missbruka, systemet eller mjukvaran.

Det finns offentligt tillgängliga rekommendationer kring säkerhetshärdning för de flesta operativsystem.

Om en sådan rekommendation används i en OT-miljö, bör den anpassas med hänsyn till den önskade funktionaliteten och krav på föråldrade system som måste fortsätta fungera. Detta kan innebära att till exempel osäkra protokoll eller inställningar behöver köras vidare. Ett sådant beslut ska baseras på er risk- och konsekvensanalys.

Sedan ska er verksamhet även härda enskilda mjukvaror om de har kritisk betydelse för den samhällsviktiga tjänsten (till exempel Active Directory, SCADA system, Historians). För dessa brukar tillverkaren tillhandahålla rekommendationer som en verksamhet kan använda sig av. Om inte en sådan dokumentation finns bör verksamheten i samråd med tillverkaren ta fram en sådan för eget bruk.

Även era nätverk bör härdas genom att säkerhetshärda infrastrukturutrustningen (WiFi accesspunkter, switchar, brandväggar). Vid denna härdning bör särskild uppmärksamhet ägnas åt att hålla obehöriga utanför nätverket (till exempel genom att använda IEEE 802.1X).

Krav 8.9: Leverantören ska utföra loggning av tillgångarna i syfte att möjliggöra upptäckt, larm och spårning av transaktioner och händelser.
Föreskrift: 3 kap. 1 § p. 2
Allmänt råd:
Referenser: ISO/IEC 27001:2017 A.12.4 ISO/IEC 27002:2017 A.12.4 NIST-CSF DE.AE-3 NIST SP 800-53 Rev. 5: AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 NIST SP 800-92 ISA/IEC 62443-3-3: SR 2.8 NIST SP 800-82r2: 5.16

Loggning är ett fundamentalt område inom IT och OT, oavsett om man pratar om säkerhet, drift, felsökning eller användarspårning. Säkerhetsloggning kan användas som ett verktyg för att hitta oönskad aktivitet i system, men kräver fortlöpande säkerhetsarbete, utveckling och uppföljning.

Er organisation bör upprätta mål och rutiner för att implementera säkerhetsloggning i nya såväl som befintliga system, och kontinuerligt följa upp efterlevnad.

Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras och granskas regelbundet.

Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst. Systemadministratörers och systemoperatörers aktiviteter ska loggas och loggarna ska skyddas och granskas regelbundet.

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän ska synkroniseras mot en och samma säkra och robusta referenskälla för tid.

För att inte bli överväldigad av information, bör ni analysera vilka aktiviteter i ett system som genererar loggdata som är relevant för säkerhetsarbetet, för att sedan se till att detta är informationen som vidarebefordras till en central plats där analys regelbundet utförs. Undvik att skicka samtlig loggdata ett system kan generera till samma punkt, då säkerhetsarbetet kan försvåras om man vid analys måste ta hänsyn till och gallra bort driftrelaterade logghändelser. Se till att loggningsnivåerna är hanterbara.

Lägg tid på analysen i samband med implementation av nya system, eller då nya funktioner tillkommer, och gör bedömningen om vilka loggar (om några) som är av relevans för säkerhetsarbete.

Separation av rättigheter är viktigt. En systemadministratör bör inte ha rättigheter att manipulera en central lagring av säkerhetsloggar, då ALL användaraktivitet skall sparas och medföra möjlighet till granskning av användaraktivitet.

Här är det viktigt att ni säkerställer att loggdata inte kan manipuleras i efterhand, till exempel genom att lagra detta på lagringsytor som inte möjliggör raderande eller manipulerande av data. Ett exempel är att filsystemet enbart tillåter "*append*"-händelser på filer.

Det kan finnas en säkerhetsmässig vinst i att överlåta övervakning av säkerhetsloggar till en separat enhet, inom eller utanför den egna organisationen (exempelvis till en SOC), så att verksamhetsnära individer inte har i uppdrag att övervaka sin egen aktivitet.

Rekommenderad läsning: NIST SP 800-92.
(https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf)

2.3.3 Säkerhetskopiering och redundans

Krav 9: Leverantören ska ha en dokumenterad process och en metod för att minimera verkningar av incidenter. Processen och metoden för att minimera verkningar av incidenter ska innehålla krav 9.1-9.3.
Föreskrift: 3 kap. 1 § p. 1, 3 kap. 5 §.
Allmänt råd: 3 kap. 5 § Redundans och kontinuitetshantering kan införas på olika tekniska nivåer (t.ex. hårdvara för förvaring, databas, nätverk eller ett helt datacenter), och kan även innebära krav på manuella, analoga arbetssätt.
Referenser: ISO 27001: A.17.1-3 ISO 27002: A.17.1-3 NIST: PR.IP-9 NIST SP 800-53 Rev. 5: CP-2, CP-7, CP-12, CP13, IR-7, IR-8, IR-9, PE-17 ISA/IEC 62443-2-1: 4.3.4.5 NIST SP 800-82r2: 5.17, 6.2.8

För att kunna hantera en oönskad händelse ska er organisation ha en process för att kunna hantera kontinuiteten i verksamheten, en kontinuitethanteringsprocess. Att planera för oönskade händelser kortar tiden för att dels kunna arbeta på alternativa sätt, dels att återgå till normaltillstånd, och på så sätt minimera konsekvensen av en oönskad händelse.

En kontinuitethanteringsprocess ska innehålla en bedömning av hur kritisk en process är för er verksamhet, konsekvensanalys, samt val av strategier för att kunna hantera verksamhetens kontinuitet. En strategi för att kunna hantera en er verksamhets kontinuitet kan vara att på era system, ta backuper som kan återläsas ifall något oönskat inträffar, planera för en manuell hantering, eller alternativ hantering ifall huvudsystem slås ut, men även planera för att ha redundans i era system.

Efter att kontinuitetsstrategi valts, ska ni upprätta en kontinuitetsplan som ska uppdateras med en periodicitet, eller när planen behövs uppdateras ifall förändring sker i verksamheten. Er kontinuitetsplan ska testas årligen för att förstå ifall planen fungerar när en oönskad händelse inträffar.

I OT miljöer bör ni beakta att prioriteringen oftast inte är lika som i IT miljöer vad gäller konsekvenser av incidenter som man vill minimera. Rangordningen i IT miljöer brukar vara Konfidentialitet > Integritet > Tillgänglighet, medan OT miljöer brukar ha rangordningen “Skydd av personer och utrustning mot skada (Safety)” > Drift > Effektivitet.

Krav 9.1: Säkerhetskopiering av applikationer och information från de delar av IT och OT som är kritiska för tillhandahållandet av samhällsviktiga tjänster.
Föreskrift: 3 kap. 5 § p. 1
Allmänt råd:
Referenser: ISO/IEC 27002:2017: 12.3.1 NIST: PR.IP-4 NIST SP 800-53 Rev. 5: CP-4, CP-6, CP-9 ISA/IEC 62443-2-1: 4.3.2.5.6, 4.3.4.3.9 ISA/IEC 62443-3-3: SR 7.3 NIST SP 800-82r2: 5.13, 6.2.6

När en incident inträffar är det viktigt att snabbt kunna få igång verksamheten igen, eller få fram kritisk information till verksamheten, eller att åtminstone kunna få fram kritisk information.

Regler och policys kring hur säkerhetskopiering skall göras, samt vilken data som skall omfattas, bör tas fram för varje system som bedöms som viktigt för tillhandahållande av samhällsviktiga tjänster.

Ni bör göra bedömningen utifrån vilken data som behövs för att kunna återställa drift vid total dataförlust, alltså utgå från värsta tänkbara scenario. Samtliga nödvändiga system för en tjänst måste tas i beaktande. Beroenden mellan system måste kartläggas och väsentliga kringliggande system inkluderas i säkerhetskopieringsplanen för aktuell tjänst, se krav 7.1.

Er verksamhet bör även göra en bedömning kring hur ofta säkerhetskopior behöver tas. Det kan t.ex. vara så att enbart en delmängd av ett systems data är föränderlig, eller föränderlig i högre takt än övriga data. Anpassa säkerhetskopieringsrutiner efter detta. Använd konsekvensbedömningen i krav 9 för att bedöma hur ofta säkerhetskopior behöver tas.

Det är också av vikt att ni bedömer hur länge information bör eller skall sparas, beroende på tjänstens beskaffenhet.

Säkerhetskopior bör med fördel förvaras på annan plats än aktuella system, för att förhindra total dataförlust vid katastrofal skada eller påverkan på aktuella system (t.ex. vattenskador, brand, stöld).

En rekommendation är att en er verksamhet arbetar utefter ”3-2-1” principen vad det gäller säkerhetskopior. Det bör finnas tre kopior av informationen (en kopia är den information leverantören arbetar med till vardags), två backuper på två olika medium, varav en backup lagras utanför verksamhetsstället.

Tänk på att säkerhetskopior som innehåller potentiellt känslig information, måste skyddas därefter med till exempel kryptering och åtkomstbegränsningar.

Krav 9.2: Regelbundet testa återställning av säkerhetskopior.
Föreskrift: 3 kap 5 § p. 2
Allmänt råd:
Referenser: ISO/IEC 27002:2017: 12.3.1 NIST: PR.IP-4 NIST SP 800-53 Rev. 5: CP-4, CP-6, CP-9 ISA/IEC 62443 2-1: A.3.2.5.3 ISA/IEC 62443 3-3: SR 7.3 RE1

Säkerhetskopiering är någonting som de flesta verksamheter har och anses vara en kritisk del av IT-infrastrukturen. Det som ofta förbises, är att kontrollera huruvida säkerhetskopiorna är användbara. Det kan röra sig om att validera säkerhetskopians riktighet, men också att säkerställa att samtliga beroenden ett system kan tänkas ha är inkluderade i en säkerhetskopia.

Säkerhetskopior skall regelbundet valideras och *återläsningstestas*. Det är viktigt att ni säkerställer att det finns tillräcklig information kring hur system återställs, samt att återläsning fungerar. Detta bör göras i en isolerad miljö, där samtliga system som är viktiga för en kritisk tjänst kan driftsättas i testsyfte.

Många applikationer som hanterar säkerhetskopior har inbyggda funktioner för återläsningstester, som i många fall kan automatiseras. Det är dock viktigt att inte blint lita på automatiserade återläsningstester. Dessa kan vara missvisande på grund av konfigurationsfel, tekniska fel eller övrig påverkan. Manuella återläsningstester bör utföras regelbundet vid sidan av automatiserade.

Frekvensen och rutinen för återläsningstester bör anpassas beroende på systemets väsentlighet för tillhandahållandet av den samhällsviktiga tjänsten.

Krav 9.3: Säkerställa att nätverk och informationssystem är så redundanta som möjligt utifrån deras väsentlighet för tillhandahållandet av den samhällsviktiga tjänsten och utifrån tekniska förutsättningar.
Föreskrift: 3 kap 5 § p. 3
Allmänt råd:
Referenser: ISO/IEC 27002:2017: 12.3.1 NIST: PR.IP-4, PR.IP-9

För vissa kritiska system är det inte alltid tillräckligt med att enbart ha säkerhetskopior som skydd för kontinuitet. Ifall en tjänst är så viktig för tillhandahållandet av en samhällsviktig tjänst kan det krävas att ni som verksamhet har redundanta system.

Vid bedömning av lämplig redundansnivå på infrastruktur kring system som tillhandahåller samhällsviktig tjänst, bör tillgänglighetskrav och påverkan på leveransförmåga beaktas, använd konsekvensbedömningen i krav 9.

Exempelvis kan bedömning göras huruvida en samhällsviktig tjänst kan levereras även under bortfall av berörda IT/OT-system, och i så fall, hur länge. Anpassa designen utefter resultaten på denna bedömning.

Redundans kan handla om till exempel *Disaster Recovery* (DR), med varma eller kalla redundanta kompletta system som står redo att ta över vid en driftstörning, men även redundans i kommunikationsvägar såsom *switchar*, *routrar* och dylikt. Vid nyttjande av DR, bör ni som verksamhet via regelbundna tester undersöka systemens riktighet, det vill säga att informationen på systemen faktiskt är aktuell. Tester där er verksamhet regelbundet växlar mellan primärdrift och DR-drift bör utföras.

Om system inte har stöd för flera nätverkskopplingar för att dra nytta av en redundant nätverksinfrastruktur, bör ni säkerställa att andra åtgärdsplaner finns etablerade (t.ex. Möjlighet till omgående byte av hårdvara).

Krav 9.4: Leverantören ska utföra loggning av tillgångarna i syfte att möjliggöra upptäckt, larm och spårning av transaktioner och händelser.
Föreskrift: 3 kap. 1 § p. 2
Allmänt råd:
Referenser: ISO/IEC 27001:2017 A.12.4 ISO/IEC 27002:2017 A.12.4 NIST-CSF DE.AE-3 NIST SP 800-53 Rev. 5: AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 NIST SP 800-92 ISA/IEC 62443-3-3: SR 2.8 NIST SP 800-82r2: 5.16

Loggning är ett fundamentalt område inom IT och OT, oavsett om man pratar om säkerhet, drift, felsökning eller användarspårning. Säkerhetsloggning kan användas som ett verktyg för att hitta oönskad aktivitet i system, men kräver fortlöpande säkerhetsarbete, utveckling och uppföljning.

Er verksamhet bör upprätta mål och rutiner för att implementera säkerhetsloggning i nya såväl som befintliga system, och kontinuerligt följa upp efterlevnad.

Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras och granskas regelbundet.

Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst. Systemadministratörers och systemoperatörers aktiviteter ska loggas och loggarna ska skyddas och granskas regelbundet.

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän ska synkroniseras mot en och samma säkra och robusta referenskälla för tid.

För att inte bli överväldigad av information, bör ni analysera vilka aktiviteter i ett system som genererar loggdata som är relevant för säkerhetsarbetet, för att sedan se till att detta är informationen som vidarebefordras till en central plats där analys regelbundet utförs. Undvik att skicka samtlig loggdata ett system kan generera till samma punkt, då säkerhetsarbetet kan försvåras om man vid analys måste ta hänsyn till och gallra bort driftrelaterade logghändelser. Se till att loggningsnivåerna är hanterbara.

Lägg tid på analysen i samband med implementation av nya system, eller då nya funktioner tillkommer, och gör bedömningen om vilka loggar (om några) som är av relevans för säkerhetsarbete.

Separation av rättigheter är viktigt. En systemadministratör bör inte ha rättigheter att manipulera en central lagring av säkerhetsloggar, då ALL användaraktivitet skall sparas och medföra möjlighet till granskning av användaraktivitet.

Här är det viktigt att säkerställa att loggdata inte kan manipuleras i efterhand, t.ex. genom att lagra detta på lagringsytor som inte möjliggör raderande eller manipulerande av data. Ett exempel är att filsystemet enbart tillåter "*append*"-händelser på filer.

Det kan finnas en säkerhetsmässig vinst i att överlåta övervakning av säkerhetsloggar till en separat enhet, inom eller utanför den egna organisationen (exempelvis till en SOC), så att verksamhetsnära individer inte har i uppdrag att övervaka sin egen aktivitet.

Rekommenderad läsning: NIST SP 800-92.
(https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf)

2.3.4 Införande av Informationssäkerhetskraven

Krav 10: Vid införandet av informationssäkerhetskraven enligt 3 kap. ska leverantören ange: 1. Vilket nätverk eller informationssystem som säkerhetsåtgärden ska utföras inom, 2. person eller funktion hos leverantören som ansvarar för säkerhetsåtgärden, samt 3. planerad tidsram för genomförandet av säkerhetsåtgärden.
Föreskrift: 4 kap. 3 §
Allmänt råd:
Referens:

Informationssäkerhetskraven enligt 3 kap STEMFS 2021:3. ska sänka en risks riskvärde, som identifierats i krav 2. Enligt krav 3 ska kraven i 3 kap. STEMFS 2021:3 sänka en risks riskvärde.

Vid införandet av informationssäkerhetskraven enligt 3 kap. ska det framgå vilka nätverk och informationssystem som säkerhetsåtgärden ska införas inom, vem som ansvarar för att säkerhetsåtgärden blir införd, samt när säkerhetsåtgärden ska vara implementerad.

Krav 10.1: Genomförandet av säkerhetsåtgärden ska prioriteras med beaktande av leverantörens riskvärdering enligt 2 kap. 1 §. samt med beaktande av de ekonomiska och tidsmässiga resurser som vidtagandet av säkerhetsåtgärden kan kräva.
Föreskrift: 4 kap. 4 §.
Allmänt råd: 4 kap. 4 §. Leverantörens prioritering av säkerhetsåtgärden bör göras utifrån: 1. Säkerhetsåtgärdens ändamål 2. Det aktuella informationssystemets kritikalitet för tillhandahållandet av samhällsviktiga tjänster enligt den analys som ska göras enligt 3 kap. 2 § punkt 1, 3. Informationssystemets tekniska förutsättningar, samt 4. de kostnader och övriga resurser som införandet av säkerhetsåtgärden medför.

Utöver det som framgår av kravet, är det viktigt att leverantören sätter varje säkerhetsåtgärd som framgår av krav 7-9 i den kontext som leverantören verkar i. Vissa åtgärder kan vara irrelevanta för en leverantör att vidta, och behöver av det skälet inte vidta den säkerhetsåtgärden. Det viktiga är då att det framgår av riskanalysen att en säkerhetsåtgärd inte är relevant, och av vilka skäl säkerhetsåtgärden ej kommer vidtas.

Allmänt: