Vägledning till Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn

(STEMFS 2021:3)

ER 2022:17

Energimyndighetens publikationer kan laddas ner eller
beställas via www.energimyndigheten.se

Statens energimyndighet, januari 2023

ER 2022:17
ISSN 1403-1892
ISBN (pdf) 978-91-7993-093-6

Tryck: Arkitektkopia AB, Bromma

Förord

Statens energimyndighet har tillsammans med aktörer på marknaden, andra myndigheter och konsulter tagit fram den här vägledningen för att pedagogiskt förklara hur föreskrifterna och allmänna råden (STEMFS 2021:3) kan omsättas till praktiskt handlande. Målet är även att förklara kraven i en, för energisektorn, relevant kontext.

Innehåll

Förord 1

1 Bakgrund till vägledningen 3

1.1 Informationssäkerhet i energisektorn 3

1.2 Syftet med föreskriften och vägledningen 3

1.3 Målet med vägledningen 4

1.4 Avgränsningar 4

1.5 Målgrupp för vägledningen 4

1.6 Läsanvisningar 4

1.7 Definitionslista 5

2 Vägledning till STEMFS 2021:3 7

2.1 Analys för identifikation av nätverk och informationssystem för samhällsviktig tjänst 7

2.2 Riskanalys för identifierade nätverk och informationssystem samt säkerhetsåtgärder 8

2.3 Informationssäkerhetskrav 16

2.3.1 Tillgångshantering 16

2.3.2 Skydd av nätverk och informationssystem 25

2.3.3 Säkerhetskopiering och redundans 38

2.3.4 Införande av Informationssäkerhetskraven 43

1 Bakgrund till vägledningen

1.1 Informationssäkerhet i energisektorn

Två stora trender i dagens samhälle som är viktiga för hur informationssäkerhet kan och bör bedrivas för leverantörer av samhällsviktiga tjänster inom energisektorn är:

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

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

Energiinfrastruktur är 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, eftersom risk 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 är ett centralt verktyg för att nå dagens högt ställda energi- och klimatmål i 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. Det moderna energisystemet 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.

1.2 Syftet med föreskriften och vägledningen

Syftet med NIS-lagstiftningens genomförande för energisektorn är att säkerställa informationssäkerheten och i längden trygga energiförsörjningen i samhället. Energiförsörjningens tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet samt för den inre marknadens funktion.

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

Det finns andra föreskrifter kopplade till NIS-direktivet som leverantörer också måste beakta, exempelvis Myndigheten för Samhällsskydd och beredskaps (MSB) föreskrifter. Det finns även annan lagstiftning som leverantörer måste beakta, exempelvis GDPR-lagstiftning.

1.3 Målet med vägledningen

Vägledningen har tagits fram för att pedagogiskt förklara hur Statens energimyndighet ser att föreskrifterna och allmänna råden, STEMFS 2021:3, *kan* omsättas i praktiskt handlande. Målet är även att förklara kraven i en, för energisektorn, relevant kontext.

1.4 Avgränsningar

Vägledningen 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 *kan* omsättas i praktiskt handlande, tillsammans med förklaringar om varför dessa åtgärder är viktiga och ytterligare referenser för att underlätta arbetet. Beslutet om vad som ska genomföras i verksamheten för att uppnå kraven i föreskriften är fortfarande en fråga för leverantörens egen analys och Statens energimyndighets påföljande tillsyn.

1.5 Målgrupp för vägledningen

Målgrupp för vägledningen är främst energiaktörernas ansvariga för informationssäkerhet samt IT- och OT-tekniker, men även andra målgrupper kan ha användning för vägledningen, exempelvis säkerhetsavdelningar.

1.6 Läsanvisningar

I vägledningen har föreskriften delats in i tre avsnitt med tillhörande krav.

1. *Analys för identifikation av nätverk och informationssystem för samhällsviktig tjänst*
2. *Riskanalys för identifierade nätverk och informationssystem samt säkerhetsåtgärder*
3. *Informationssäkerhetskrav*

Avsnitten följer inte föreskriftens juridiska ordningsföljd utan har strukturerats om för att underlätta läsningen och för att följa föreskriften.

Inför varje vägledningstext finns en informationsruta som innehåller:

- ett Krav-ID,
- det krav som framgår av föreskriften,
- en referens till föreskriften,
- en kopia av de allmänna råden till föreskriften samt

- referenser till informationssäkerhets- och OT-säkerhetsstandarder som anses vara relevanta och som kan ge ytterligare vägledning utöver denna vägledningstext.

Läshänvisningarna ger i många fall förslag på ytterligare åtgärder som är relevanta, men som kan gå utanför de explicita kraven i föreskriften.

Efter varje informationsruta kommer en vägledningstext som ger läsaren *förslag* på hur föreskriftskraven kan uppfyllas. Verksamhetsutövare kan uppfylla föreskriftskraven på andra sätt.

För att uppfylla kraven i föreskriften kan referenserna till informations- och OT-säkerhetsstandarden utgöra stöd genom 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 specifika krav som framgår av föreskriften.

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

1.7 Definitionslista

Computer Emergency Response Team Sweden (CERT-SE): Sveriges nationella team för hantering av informationssäkerhetsincidenter med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

Datadiod: En hårdvarubaserad cybersäkerhetslösning mellan två nätverk som säkerställer att information endast tillåts skickas i en riktning och blockerar all data i motsatt riktning.

*DeMilitarized Zone (DMZ)***:** Ett subnätverk som skiljer lokala nätverk från opålitlig nätverkstrafik.

Digital Control System (DCS): Ett komplext överordnande styrsystem för många separata funktioner och kontrollsystem.

Disaster Recovery (DR): En uppsättning processer och tekniska säkerhetsanordningar för att återupprätta driften efter en skadlig händelse, såsom strömavbrott eller dataintrång.

Endpoint Protection Platform (EPP): Ett agentbaserat system som installeras på datorer för att upptäcka och blockera kända hot. En modernare form av ett anti-virus-system.

Endpoint Detection and Response (EDR): Ett agentbaserat system som installeras på datorer för att upptäcka okända hot baserat på anomalidetektering, samla in och vidarebefordra information om misstänkta intrång samt underlätta åtgärder och analys.

Factory Acceptance Test (FAT): Test för att verifiera att en nytillverkad produkt uppfyller sitt avsedda syfte. Genomförs i testmiljö.

Funktionssäkerhet: Förmågan hos en enhet att utföra en krävd funktion under givna förhållanden under ett givet tidsintervall.

Hypertext Transfer Protocol Secure (HTTPS): Ett krypterat protokoll som används för att skicka data säkert mellan en websida och webbläsare.

Human-Machine-Interfaces (HMI): Ett gränssnitt eller en kontrollpanel som tillåter människor att kommunicera och interagera med en maskin.

Hårdvara: Annat uttryck för Maskinvara

Intrusion Detection System (IDS): Ett program för övervakning av nätverksaktiviteter som syftar till att söka efter hot och rapportera misstänkt aktivitet.

International Organization for Standardization (ISO): Internationellt organ för olika typer av standarder.

Lökprincipen: Lökprincipen är ett ”utifrån och in”-perspektiv där en antagonist måste ta sig igenom flera lager av säkerhetsskyddsåtgärder in till skyddsvärden som befinner sig i centrum.

Mjukvara: Annat uttryck för Programvara

Multi-Factor Authentication (MFA): En metod för autentisering som kräver två eller fler verifieringsfaktorer för att bereda en användare tillgång till viss information eller IT-system.

National Institute of Standards and Technology (NIST): En organisation som drivs av USA:s handelsdepartement och som arbetar för standardisering och forskning.

Network Address Translation (NAT): En process som går ut på att en anordning, vanligtvis en brandvägg, tilldelar en gemensam publik IP-adress till datorer inom ett internt nätverk.

Operational Technology (OT): Datorsystem som styr och övervakar industriella processer.

Programmable Logic Controller (PLC): En specialiserad dator som programmeras för att styra automationsprocesser.

Proxy: En server som agerar mellanhand mellan användarens dator och andra servrar och kan användas för att kringgå begränsningar, säkerställa anonymitet på internet eller undvika övervakning.

Remote Terminal Units (RTU): En mikroprocessorbaserad enhet som övervakar och styr avlägsna fältenheter.

Security Operations Center (SOC): En organisations centrala funktion som ansvarar för att detektera intrångsförsök och inleda åtgärder genom att övervaka och analysera relevanta informationskällor.

Security Information and Event Management system (SIEM): Samlingsbegrepp för en kategori av system som är till för att samla och organisera information från larm och loggar som har relevans för cybersäkerheten. Används till exempel av en SOC (se ovan).

Site Acceptance Test (SAT): Test för att verifiera att en nytillverkad produkt uppfyller sitt avsedda syfte. Genomförs i produktionsmiljö.

Software as a Service (SaaS): Webbaserad mjukvara som inte kräver lokal installation på datorn, utan körs via internet.

Software Asset Management (SAM): Programvara för att inventera mjukvara i verksamheten.

2 Vägledning till STEMFS 2021:3

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. Om leverantören anlitar underleverantör för att stödja tillhandahållandet av de samhällsviktiga tjänsterna ska dessa nätverk och informationssystem omfattas av leverantörens analys. Leverantören ska dokumentera den analysmetod som används enligt andra stycket liksom resultatet av analysen.

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 kap. 3

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 3 §.

Syftet med denna föreskriftsdel är att säkerställa att alla delar av den samhällsviktiga tjänsten täcks av leverantörens analyser och säkerhetsåtgärder, och på så vis förhindra att dolda beroenden skapar säkerhetsbrister.

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

När den samhällsviktiga tjänsten identifierats ska en analys genomföras. Analysen ska utreda följande:

- Vad tjänsten består av, samt
- Vilka nätverk och informationssystem som används.

För OT system rekommenderas det att även beakta funktionssäkerhet för system som tillhandahåller viktiga funktioner (till exempel nödavstängning) utöver nätverk och informationssystem.

Analysen kan genomföras genom en workshop där olika delar av verksamheten deltar tillsammans för att:

- Identifiera regulatoriska krav på tjänsten.
- Identifiera kundernas avtalade specifikationer och förväntningar.
- Identifiera och 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 ska 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 välavvägt skydd för informationen kan upprättas. För att kunna arbeta systematiskt med informationssäkerhetsrisker behöver en verksamhet ha en riskanalysmodell att utgå ifrån. Krav 2–6 nedan beskriver de krav som ställs på riskanalysmodellen.

En verksamhet bör utgå från en redan fastställd riskanalysmodell om sådan finns. Samma modell bör även används för hela verksamheten, inte enbart när informationssäkerhetsrisker bedöms. Samma modell kan gärna användas över längre tidsperioder. Genom att använda samma modell för att till exempel bedöma kvalitets- och miljörisker kan riskvärden för olika risker jämföras och prioriteras.

På MSB:s webbsida Informationssäkerhet.se finns mallar och stöd för riskanalysarbetet. Där finns erfarenheter samlade för hur arbetet med informationssäkerhet bör bedrivas, däribland genomförandet av riskanalyser. Informationsäkerhet.se drivs av MSB och är kopplat till 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-CSF: 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 som deltar i riskanalyser bidrar med sina perspektiv utifrån erfarenhet och funktion vilket gör att det blir lättare att identifiera sådant som tas för givet. När en riskanalys för nätverk och informationssystem för samhällsviktiga tjänster genomförs rekommenderas att det finns deltagare med kompetens från både IT och OT. Ta i beaktning att även ha med funktionsföreträdare eller aktörer vilka kan behöva vidta åtgärder.

Vidare rekommenderas att den riskanalys för nätverk och informationssystem som används vid tillhandahållandet av en samhällsviktig tjänst delas upp så att det genomförs en riskanalys per nätverk respektive per informationssystem. Genom att genomföra en riskanalys per nätverk och informationssystem kan specifika hot mot de enskilda nätverken och informationssystemen enklare identifieras för att därefter bättre kunna anpassa åtgärder att vidta mot dessa identifierade risker. 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.

En ytterligare rekommendation är att inte begränsa riskanalysen enbart till nätverk och informationssystem när det gäller OT eftersom viktiga delar av tjänsten kan bero på system som tillhandahåller en viss funktion (till exempel ett kylsystem) och inte primärt förarbetar information.

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 återfinns i krav 7.2–7.7.

Vid upprättandet av riskanalysmodellen bör modellen innehålla en bedömning av riskens konsekvens och sannolikhet. Konsekvens och sannolikhet bör utgå ifrån skalor. Antalet nivåer på en skala kan variera men rekommendationen är att utgå från fyra nivåer. Ett jämt antal nivåer, inte för många eller för få, är grundprincipen för antalet nivåer. Nivåerna kan se ut enligt följande:

- Mycket hög
- Hög
- Låg
- Mycket låg

Vid fastställandet av nivåerna på skalorna för konsekvens och sannolikhet bör ett antal aspekter beaktas. Avseende konsekvens kan nivåerna utgå ifrån två perspektiv:

- Att nivåerna baseras på monetär skada (Notera att MSB i sin mall för incidentrapportering kräver att en konsekvens av en incident ska anges i monetära siffror.)
- 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, samtidigt som det blir svårt att avgöra vilken konsekvens i monetära siffor ett hot 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 inte nödvändigtvis det monetära perspektivet som är det viktiga, dessutom är det svårt att bedöma samhällskonsekvenser utifrån monetära skador.

En nivåskala för konsekvens kan se ut enligt följande:

- Mycket hög – *Mycket 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.*
- Mycket låg – *Mycket låg, eller ingen, direkt skada eller indirekt skada. Drabbar inte affärsprocessen eller leveransen av samhällsviktig tjänst på kort eller lång sikt.*

Det är viktigt att leverantören skapar en konsekvensskala som är anpassad efter sin verksamhet. Det ovan nämnda är enbart ett exempel. Leverantören bestämmer själv vilket perspektiv konsekvensskalan ska utgå ifrån.

Sannolikhet bör också bedömas på samma antal nivåer som konsekvens, alltså rekommenderas samma antal nivåer. Sannolikhetsnivåerna bör bedömas utifrån sannolikheten att ett hot inträffar. Sannolikheten kan bedömas 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.

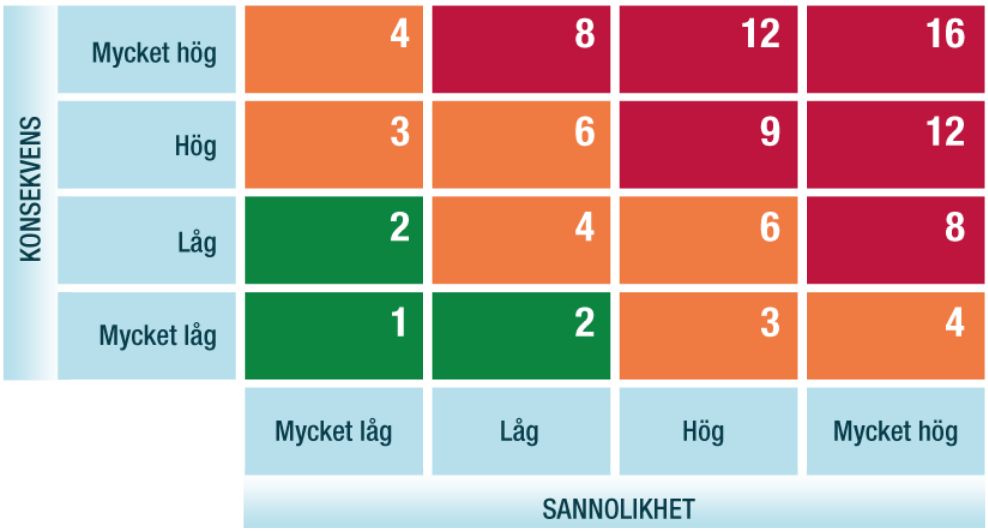
En nivåskala för sannolikhet kan se ut enligt följande:

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

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

Utifrån bedömningen av konsekvens och sannolikhet bör riskanalysmodellen ge ett riskvärde. Riskvärdet bör ge möjlighet att upptäcka var de största riskerna föreligger samt att prioritera olika risker där åtgärder ska införas (mitigerande åtgärder). Riskvärdet i kombination med hur stora risker verksamheten är beredd att ta (verksamhetens riskaptit) ger svar på vilka risker som ska åtgärdas. Åtgärder bör alltså föregås av informerade beslut kring verksamhetens risk i förhållande till riskacceptans.

Riskmatris kan se ut som följande:



Vid genomförandet av riskanalysen ska hot mot verksamheten och dess information analyseras. Det kan med fördel vara scenariobaserat. Ett scenario kan exempelvis vara att verksamheten drabbas av ett lyckat ransomware-angrepp genom e-post. Varje scenario bör ha ett unikt risk-ID. Därefter ska en beskrivning av vilket hot det innebär mot verksamheten, exempelvis att vissa delar av verksamheten behöver stängas ner under en viss tid. Därefter ska sårbarheten beskrivas, det vill säga vad som möjliggör att hotet kan realiseras. Därefter ska beskrivas den risk-konsekvens som hotet får om det realiseras och hur sannolikt det är.

Efter genomförd riskanalys ska lämpliga säkerhetsåtgärder införas. Metoden för att utvärdera de säkerhetsåtgärder som valts ska huvudsakligen kunna svara på två frågor: (1) vidtar vi rätt åtgärder och (2) ökar vår säkerhet med de åtgärder vi vidtar?

Införandet av säkerhetsåtgärder kan också styras av verksamhetens informationsklassificeringsmodell, där lägre klassificerad information får färre/mindre säkerhetsåtgärder, medan högre klassificerad information får fler säkerhetsåtgärder.

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 (avser 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-CSF: ID.RA-1-6, ID.RM-1-3

NIST SP 800-30

ISA/IEC 62443-3-2

Syftet med denna föreskriftsdel är att säkerställa att alla risker som identifierats i riskanalysen enligt krav 2 täcks av motsvarande åtgärder, samt att alla vidtagna åtgärder tydligt kopplas till antingen riskanalysen eller informationssäkerhetskraven enligt föreskriften.

Riskanalysmodellen, som nämnts under krav 2, ska inkludera hur en risk hanteras, utifrån det riskvärde som risken tilldelats. Riskvärdet bör ge vägledning för hur en risk åtgärdas utifrån verksamhetens riskaptit.

En säkerhetsåtgärd kan 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 föra över risken till en annan part, såsom 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 bådå 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 1-2 - Accepteras, transfereras
- Riskvärde 3-6 - Transfereras, reduceras, elimineras
- Riskvärde 8-16 - Reduceras, elimineras

Ett riskvärde kan sänkas, antingen genom att en åtgärd minskar konsekvensen eller sannolikheten. Oftast är syftet med en säkerhetsåtgärd att minska sannolikheten för att risken inträffar men genom att arbeta med kontinuitet, effektiv incidenthantering 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-CSF: ID.RA.1-6, ID.RM.1-3

NIST SP 800-30

ISA/IEC 62443-3-2

Syftet med denna föreskriftsdel är att säkerställa att åtgärder som fastställts enligt krav 3 blir en del av verksamhetsplaneringen och att åtgärdernas syfte och förväntad effekt dokumenteras.

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

För varje risk ska minst en mitigerande åtgärd utifrån riskvärdet vidtas. Den mitigerande åtgärden ska antingen minska konsekvensen eller sannolikheten, eller både och. Det ska tydligt 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 införd. Ansvarig behöver inte vara den som inför säkerhetsåtgärden. Ansvarig ska säkerställa att åtgärden blir införd inom utsatt, och dokumenterad, tidsram.

Efter att en säkerhetsåtgärd blivit tilldelad ansvarig och tidsram är satt ska deltagarna i riskanalysen bedöma den kvarvarande risken *efter* att åtgärden 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 så har säkerhetsåtgärden ingen effekt och bör därför inte vidtas. I stället bör en annan säkerhetsåtgärd vidtas eller en kombination av ytterligare säkerhetsåtgärder. Det kan dock finns skäl till att vidta en säkerhetsåtgärd även om riskvärdet inte minskas eftersom åtgärden kan ge en effekt som inte kan ses på riskskalan.

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

Syftet med denna föreskriftsdel är att säkerställa att åtgärder som fastställts enligt krav 3 blir prioriterade baserat på mätbara och dokumenterade grunder.

När verksamheten prioriterar införandet av säkerhetsåtgärderna (de mitigerande åtgärderna) ska riskvärderingen beaktas. Risker med högt riskvärde bör prioriteras före de riskerna med lågt riskvärde, och dess säkerhetsåtgärder. Det kan dock finnas mindre prioriterade åtgärder som ger en hög effekt i förhållande till ianspråktagna resurser, det kan då självklart vara motiverat att åtgärda dessa innan eller 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 konsekvenserna för varje oönskad händelse. Genom att tydligt beskriva konsekvenser är det enklare att vidta rätt mitigerande åtgärder.

Vid genomförandet av riskanalysen enligt krav 2-5 ska det i den beskrivande texten över ett hot framgå hur realisering av hotet påverkar leveransen av den samhällsviktiga tjänsten, se krav 2. Genom att göra detta får verksamhetsutövaren inriktning för vad som är viktigast att fokusera på för att minska informationssäkerhetsriskerna för sin leverans av samhällsviktig tjänst.

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-CSF: 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 lättare kunna skydda sina tillgångar på ett korrekt sätt över tid. En process bör innehålla ägarskap för att införskaffa och skapa tillgångar, skydd av tillgångarna på ett korrekt sätt under dess livstid samt ett sätt göra sig av med tillgångarna på ett säkert vis när de inte längre ska användas. Som minst ska processen för tillgångshantering innehålla aktiviteter för att uppfylla kraven 7.1–7.7. Vill en 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. Det kan göras med hjälp av systemstöd eller ett manuellt register. Det viktiga är att tillgångsinventeringen är dokumenterad och att inventeringen kan utgöra ett bra stöd för arbetet att genomföra riskanalyser, enligt krav 2–5, samt att skydda de identifierade tillgångarna.

Vid tillgångsinventering kan verksamheten ha två perspektiv. Det ena är informationsperspektivet och det andra är informationsbärarperspektivet. I informationsperspektivet är informationen i centrum för att förstå vilken information det är som ska skyddas. I informationsbärarperspektivet är det hårdvaran, mjukvaran eller IT/OT-systemen som först identifieras och därefter den information som behandlas i informationssystemen. För OT system är det rekommenderat att inkludera system i tillgångshanteringen som inte primärt är informationssystem men som tillhandahåller viktiga funktioner för den samhällsviktiga tjänsten (till exempel nödavstängning).

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 beroende av varandra. Beroendena består i att information utbyts som stöd till varandras verksamhetsprocesser. Beroendena kan dock även innebära att sårbarheter som drabbar ett system kan spridas till andra system. Att kartlägga beroenden ger förståelse för hur olika nätverk och informationssystem kommunicerar med och är beroende av varandra samt för att förstå vilka sårbarheter som finns eller som kan uppstå i nätverken och informationssystemen. Dessa sårbarheter är i sig underlag till att göra en bra riskanalys i krav 2–6.

För att kunna kartlägga beroenden mellan olika IT-och OT-tjänster samt nätverk och informationssystem rekommenderas att göra en dataflödesanalys för att förstå hur information flödar mellan olika nätverk och informationssystem. En dataflödesanalys kan med fördel göras med program som är avsedda för detta ändamål. Genom att visualisera dataflödet, kan en verksamhet snabbt förstå hur kritiska vissa nätverk och informationssystem är för tillhandahållandet av sin samhällsviktiga tjänst.

För OT miljöer rekommenderas att utöka kartläggningen från informationsflöden till kommando- och styrflöden för att även fånga kommunikation mellan system som inte har som primära funktion att förarbeta information (till exempel processtyrningssystem).

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-CSF: ID.AM-1

NIST SP 800-53 rev.5: CM-8

Det är viktigt för leverantörer att ha kontroll över vilka hårdvaror som används för tillhandahållandet av sin samhällsviktiga tjänst. Brister i 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 hårdvaror utgör ett stöd för att upptäcka icke-godkända hårdvaror som inte tillhör den egna verksamheten utan kanske en hotaktör som försöker skaffa sig åtkomst till verksamhetens IT och OT-nätverk.

Det är viktigt att både processen och resultatet av tillgångsinventering är lättillgänglig och enkel att arbeta i. En tillgångsinventering för hårdvaror ska dokumenteras i en för ändamålet anpassad applikation eller 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,
- när hårdvaran planerad att tas ur bruk,
- var hårdvaran fysiskt finns,
- om det finns några hälso- eller säkerhetsrisker (*safety*) med hårdvaran som behöver tas i beaktning för att den samhällsviktiga tjänsten ska levereras (specifikt för OT-hårdvara), samt
- om hårdvaran används för leveransen av den samhällsviktiga tjänsten, direkt eller indirekt.

Vid exempelvis SaaS-lösningar kan det vara svårt att själv göra en hårdvaruinventering. Detta måste isåfall kravställas mot den leverantören att ha en sådan inventering på plats.

Hårdvaruinventeringen kan senare användas för att bestämma vilken hårdvara som är godkänd att användas, genom en så kallad vitlista. En hårdvaruvitlista är en lista över tillåtna enheter som får koppla upp sig mot, eller vara en del utav, ett OT- eller IT-system. Det är enbart de tillåtna hårdvaruenheterna som ska kunna komma åt nätverket. Hårdvaruenheter som inte är del av vitlistan ska inte kunna koppla upp sig mot, eller komma åt OT- eller IT-systemen. En hårdvaruvitlista 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-CSF: ID.AM-2

NIST SP 800-53 rev.5: CM-8

Att ha kontroll över vilka mjukvaror som används inom verksamheten är lika viktigt som att ha kontroll över vilka hårdvaror som en organisation tillåter. Att ha kontroll på vilka mjukvaror som verksamheten har ger både ekonomiska och säkerhetsmässiga fördelar. Från ett ekonomiskt perspektiv kan verksamheten spara pengar på att veta hur många licenser som verksamheten har, samt hur många licenser som används. Från ett säkerhetsperspektiv ger kontroll över vilka mjukvaror som används inom verksamheten en snabb överblick om verksamheten är påverkad när information om nya sårbarheter framkommer. Vidare kan verksamheten snabbt vidta mitigerande åtgärder för att stänga sårbarheten genom att installera en uppdaterad version, eller i allvarliga fall sluta använda mjukvaran.

En mjukvaruinventering bör innehålla:

- namn på mjukvara,
- produkt ID,
- version av mjukvara,
- vem som är ansvarig för mjukvaran,
- hur många licenser organisationen har,
- hur många användare av mjukvaran organisationen har,
- vilka användare som har mjukvaran installerad, och
- om mjukvaran används för leveransen av den samhällsviktiga tjänsten, direkt eller indirekt.

En mjukvaruinventering kan upprätthållas genom att använda en programvara, Software Asset Management-verktyg (SAM) eller genom att manuellt upprätthålla registret. Fördelen med ett SAM-verktyg är att dessa har möjligheten att söka igenom IT-miljöer efter programvaror samt ha kontroll över när licenser går ut. Att ha inventeringen i ett manuellt upprättat register kan snabbt leda till att det manuella registret blir föråldrat.

För att få ytterligare kontroll över vilka mjukvaror som används, bör en vitlista användas. En vitlista för mjukvara skapas genom att organisationen bestämmer vilka mjukvaror som får installeras och användas på de interna nätverken. En mjukvara som inte är med på vitlistan får således inte 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-CSF: 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 en organisation bedöma vilka av dessa som är mest kritiska för tillhandahållandet av den samhällsviktiga tjänsten. För OT miljöer rekommenderas det att utöka identifieringen till kritiska system som inte har som primära funktion att förarbeta information (till exempel processtyrningssystem).

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.

Vidare kan verksamheten med hjälp utav sin kontinuitetsplanering bedöma vilka tjänster som är mest kritiska, se krav 9.

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-CSF: 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 en verksamhet har koll och kontroll över sina närverk är viktigt, dels för att förstå vilka förbättringar som verksamheten kan göra i sina nätverk, dels för att förstå vilka sårbarheter som deras 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, identifiering av komponenter såsom routrar, brandväggar och enheter samt visar visuellt hur dessa samverkar.

Det finns produkter på marknaden som automatiserar processen med att skapa en nätverkskarta. Om en verksamhet skulle använda någon av dessa produkter bör verksamhetsutövaren vara försiktig, 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

ITIL – Change Management

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 bör en ändringshanteringsprocess (Change Management process) införas. För OT miljöer rekommenderas det dessutom att tillämpa en sådan process även för kritiska system som inte är informationssystem (till exempel processtyrningssystem).

Anledning till att ha en ändringshanteringsprocess är för att säkerställa att en ändring inte medför en risk för personskador, drift eller informationssäkerhet 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 behöver vara tydligt definierat. När ändringar genomförs av underleverantörer (till exempel av en leverantör av en managerad tjänst) bör kraven på ändringshanteringsprocessen fastslås i tjänsteavtalet.

Vid introducering av ny IT-mjukvara i OT-miljöer bör leverantören iaktta försiktighet, då användandet av IT-mjukvara i dessa miljöer är riskfyllt.

Leverantören 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 tillgångshanteringsprocessen inkludera regelverk för hur informationshanteringssystem ska hanteras när de upphört att användas. Skälet till detta är för att dels det inte bör 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. Dessa regler bör även tillämpas på OT system som inte är informationshanteringssystem (till exempel processtyrningssystem) då även dessa kan innehålla konfigurationer som är känsliga.

När ett informationssystem når slutet av sin livscykel bör 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 bör konfiguration också uppdateras för att radera relaterade inställningar (till exempel åtkomsträttigheter, brandväggsregler, proxy-inställningar).

För vissa moderna lagringsmedium (till exempel 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 enbart data raderas på dem.

Om känslig information som finns lagrad i informationssystemet behövs efter systemets livstid så bör 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 verksamheten) 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 som ett verktyg för att hitta oönskad aktivitet i system men kräver fortlöpande säkerhetsarbete, utveckling och uppföljning. Verksamheter bör upprätta mål och rutiner för att implementera säkerhetsloggning i alla system samt regelbundet följa upp efterlevnaden av de uppsatta rutinerna.

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

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

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

För att inte bli överväldigad av information bör en verksamhet 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. Den bör undvika att skicka samtlig loggdata ett system kan generera till samma punkt, detta eftersom säkerhetsarbetet kan försvåras om man vid analys behöver ta hänsyn till och gallra bort driftrelaterade logghändelser. Se till att loggningsnivåerna är hanterbara.

Tid bör läggas på analysen i samband med implementering av nya system eller då nya funktioner tillkommer för att bedöma vilka loggar (om några) som är av relevans för säkerhetsarbetet.

Separation av rättigheter är viktigt. En systemadministratör bör inte ha rättigheter att manipulera en central lagring av säkerhetsloggar eftersom ALL användaraktivitet ska sparas och ge möjlighet till granskning av användaraktivitet.

Det är viktigt att säkerställa att loggdata inte kan manipuleras i efterhand. Det kan säkerställas exempelvis genom att lagra loggdata 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.

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 ha en process och metod för att skydda sina nätverk och informationssystem löpande. I OT miljöer bör även sådana system som inte är informationssystem men som har en viktig funktion för tjänsteleveransen omfattas av processen, till exempel processtyrningssystem.

En process och en metod för att skydda nätverk och informationssystem vid införskaffning eller upprättande, kallas ackrediteringsprocess. En ackrediteringsprocess hjälper verksamheten att utforma skyddet för ett nätverk eller ett informationssystem och processen är risk- och kravbaserad. En ackrediteringsprocess är komplement till bland annat en utvecklingsprocess, varför vissa delar från en utvecklingsprocess kan kännas igen. I en utvecklingsprocess finns andra krav, såsom funktionskrav, som måste hanteras. En ackrediteringsprocess fokuserar enbart på säkerhetsrisker och säkerhetskrav.

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 informationssäkerhetskravinsamling 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.
    a. 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 bör 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 leverantören 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 leverantören 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, bör en GAP-analys genomföras. Verifieringen bör dokumenteras. Först därefter kan nätverket eller informationssystemet driftsättas.

Ackrediteringsprocess:

Vid användande 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 deras 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 och 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 arbetet vara målriktat i stället för generellt. Vissa säkerhetsåtgärder som är vanliga i IT miljöer är inte lämpliga i samma form i OT miljöer (till exempel automatiska uppdateringar och 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 verksamheten 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 möjlig men behöver övervakas och kontrolleras (till exempel via en brandvägg) för att förhindra att information av högre klass blir överfört till ett segment av lägre klass. 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). Segmenteringen kan även upprättas baserad på informationsklassning av den information som förarbetas i olika delar av nätverket.

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 verksamheten i hur en bra nätverkssegmentering kan upprättas:

- Segmentering bör 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 bör 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-nät 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 det inte lämnar ut information som kan vara nyttigt 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 (*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-CSF: 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 som kan utföras 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).
- Undvik 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 regelbundet därefter för att säkerställa att användarna 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-CSF: 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 hot mot verksamheten. Hotaktörer har möjlighet att upptäcka sårbarheterna som icke uppdaterad programvara innebär och utnyttja sårbarheterna. Därför är det viktigt att ha en metod för att säkerhetsuppdatera de programvaror som används i verksamheten. Att regelbundet säkerhetsuppdatera 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 från MSB:s CERT-SE och ENISA:s CERT.europa.eu.
2. Rutiner för test och verifiering - för att kontrollera att uppdateringen överensstämmer med den av leverantören 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 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 är det inte möjligt att genomföra säkerhetsuppdateringar omgående, detta på grund av de konsekvenser för drift det kan medföra. Dessa system kan undantas från att omgående installera säkerhetuppdateringar. När säkerhetsuppdateringar finns tillgängliga bör en process som analyserar om säkerhetsuppdateringen kan installeras eller ej finnas. Om det inte går bör det dokumenteras att säkerhetsuppdatering ej kan göras och skälen för att säkerhetsuppdatering ej kan göras. I dessa fall blir det extra viktigt att segmentera sina 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-CSF: 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

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 användas mer allmänt där det är möjligt att använda MFA.

För applikationer brukar moderna kommunikationsprotokoll tillhandahålla möjligheten att skydda trafiken med bland annat autentisering. Denna funktion är dock sällan 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 enbart 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-CSF: 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 tid, samt uppdateras kontinuerligt mot nya hot. Antivirusprogram är vanliga i IT miljöer men deras användning i OT miljöer kräver särskilda åtgärder såsom att testa deras kompatibilitet för målsystemet, huruvida uppdateringar påverkar andra applikationer och om det blir problem med prestandan (om antivirusprogrammet till exempel skulle kunna påverka en tidskritisk process).

Det är viktigt att ha 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 processer som hanterar skydd av personer och utrustning mot fysisk skada (safety).

Många stora leverantörer av OT-system har särskilda rekommendationer för antivirusprogram, eller till och med stödjer vissa antivirusprogram. I vissa fall genomför leverantörer 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) och Remote Terminal Units (RTU)) och instrument som kör tidskritiska processer eller har speciellt anpassade operativsystem bör tillverkarens rekommendationer hämtas in, innan det övervägs att installera antivirusprogram.

Eftersom anpassningsåtgärder för antivirusprogram i OT miljöer kan vara resurskrävande så rekommenderas att prioritera vissa utvalda strategiska system i första hand och se till att dessa fungerar väl innan man gör utrullningar på mindre kritiska system.

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-CSF: PR.AC-2

NIST SP 800-53 Rev. 5: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8

ISA/IEC 62443-2-1 4.3.3.3

NIST SP 800-82r2 6.2.11

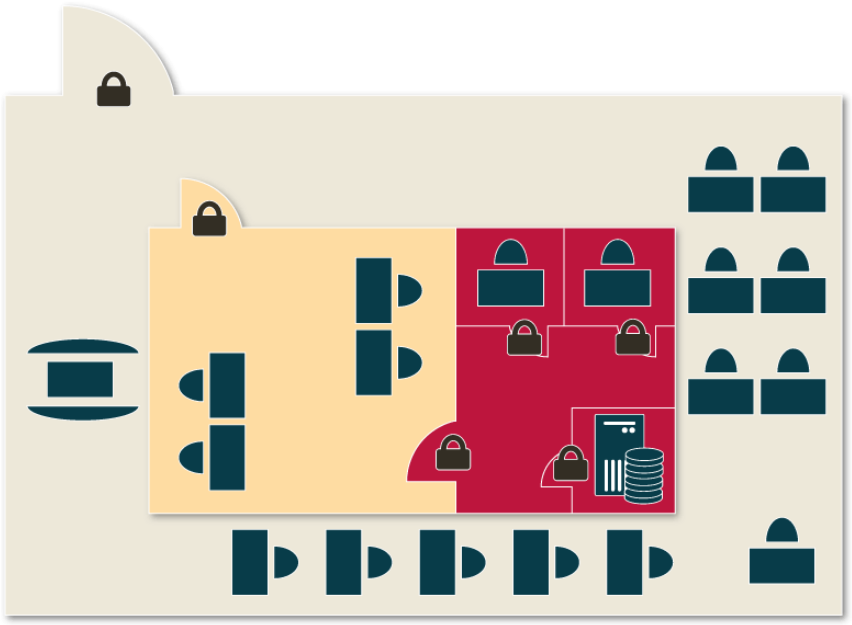
Vägledning I Säkerhetsskydd - Fysisk Säkerhet, SÄPO, september 2020

Det är lätt att glömma bort att fysisk säkerhet också är viktigt för att kunna ha ett systematiskt informationssäkerhetsarbete. 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 begränsa åtkomsten till viktig och känslig utrustning från obehöriga, där enbart behörig personal bör ha fysisk åtkomst. Servrar och nätverksutrustning är intressanta måltavlor 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 även åtkomst begränsas 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, samt så bör loggning avseende tillträde ske.

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, för att uppfylla kravet om begränsning av åtkomst till IT och OT.

Bilden beskriver att det mest skyddsvärde finns inom det röda området, med behörighets-begränsade låsanordningar. Det kan vara med nyckel som tilldelas behöriga, men det rekommenderas att smart kort tillsammans med kod används. Detta för att kunna logga tillträde till utrymmet. Inom det röda området finns exempel på hur IT- och OT-utrustning låses in men också behörighetsbegränsade arbetsutrymmen.

Inom det gula området finns arbetsstationer där de som har behörighet till det gula utrymmet kan arbeta men också de med behörighet till det röda utrymmet. Alla som har behörighet till det gula utrymmet har inte access till det röda utrymmet.

Lökprincipen för OT-nätverk kan appliceras på samma sätt där enbart de som ska ha åtkomst till kritiska OT-system ska kunna komma åt dessa.

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 sin utrustning eller när personer behöver arbeta på distans. Fjärråtkomst öppnar emellertid också nya vägar in för hotaktörer att komma åt kritiska system. Därför är det viktigt att bara använda fjärråtkomstlösningar där så är nödvändigt och som har följande säkerhetsegenskaper:

- Lösningen bör autentisera användaren med multifaktorsautentisering (MFA) för att minimera risken att stulna användarkontouppgifter kan användas för att få åtkomst till informationssystemet.
- Lösningen bör logga all åtkomst till informationssystemet, inklusive inloggningsförsök. Det behöver 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 bör stödja åtkomstkontroll på detaljerad nivå, så att användare kan tilldelas begränsad fjärråtkomst till vissa informationssystem baserad på olika förutsättningar. Mer specifikt:
  - Det bör 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 bör vara möjligt att konfigurera åtkomst baserad på grupper (till exempel baserad på roller som användarna innehar).
- Brandväggskonfigurationer som behöver implementeras för att tillåta fjärråtkomst till ett informationssystem bör dokumenteras i detalj och sparas i Asset Management systemet.
- Lösningen bör 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 bör 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-CSF: PR.DS-3,5,

NIST SP 800-53r5 CM-6, CM-7

Säkerhetshärdning av ett system, en hårdvara eller en mjukvara beskriver en process där konfigurationen väljs på ett sätt 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 behöver fortsätta fungera. Detta kan innebära att till exempel osäkra protokoll eller inställningar behöver köras vidare. Ett sådant beslut bör baseras på risk- och konsekvensanalysen.

Verksamheten bör 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 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. Verksamheten bör upprätta mål och rutiner för att implementera säkerhetsloggning i alla system samt regelbundet följa upp efterlevnaden av de uppsatta rutinerna.

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

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

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän bör synkroniseras mot en och samma säker och robust referenskälla för tid.

För att inte bli överväldigad av information bör en verksamhet 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. Den bör undvika att skicka samtlig loggdata som ett system kan generera till samma punkt, detta eftersom säkerhetsarbetet kan försvåras om det vid analys behövs ta hänsyn till och gallras bort driftrelaterade logghändelser. Se till att loggningsnivåerna är hanterbara.

Tid bör läggas på analysen i samband med implementering av nya system eller då nya funktioner tillkommer för att bedöma 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 eftersom *all* användaraktivitet ska sparas och ge möjlighet till granskning av användaraktivitet.

Det är viktigt att säkerställa att loggdata inte kan manipuleras i efterhand. Det kan undvikas exempelvis genom att lagra loggdata på lagringsytor som inte möjliggör radering eller manipulering 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.

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 (till exempel 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-CSF: 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 en organisation ha en process för att hantera kontinuiteten i verksamheten, en kontinuitethanteringsprocess. Att planera för oönskade händelser minimerar konsekvensen eftersom det kortar ner tiden för att kunna arbeta på alternativa sätt samt att kunna återgå till normaltillstånd snabbare.

Kontinuitethanteringsprocessen ska innehålla en bedömning av hur kritisk en verksamhetsprocess är för verksamheten, konsekvensbedömning (se konsekvensbedömning i riskanalys i krav 2) samt val av strategier för att kunna hantera verksamhetens kontinuitet.

Exempel på kontinuitetsstrategier kan vara:

- att ta säkerhetskopior på system som kan återläsas ifall något oönskat inträffar,
- att planera för manuell hantering eller alternativ hantering ifall huvudsystem slås ut, och
- att planera för att ha redundans i system.

När kontinuitetsstrategier har valts ska en kontinuitetsplan upprättas som ska uppdateras regelbundet eller om förändring sker i verksamheten. Kontinuitetsplanen ska testas årligen för att säkerställa att planen fungerar om en oönskad händelse inträffar, se krav 9.2.

I OT miljöer bör beaktas att prioriteringar som påverkar kontinuitetsplanen oftast inte är detsamma 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)" > Tillgänglighet > Effektivitet. Kontinuitetsplanering bör därför se olika ut i IT respektive OT miljöerna.

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-CSF: 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 tillgång till verksamhetens information eller åtminstone kritisk information för att få i gång verksamheten.

Regler och policyer avseende hur säkerhetskopiering ska göras samt vilken data som ska omfattas bör tas fram för varje system som bedömts som viktigt för tillhandahållande av samhällsviktiga tjänster. Bedömningen av vilka system som är viktiga bör göras 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 behöver beaktas. Beroenden mellan system behöver kartläggas och väsentliga kringliggande system behöver inkluderas i säkerhetskopieringsplanen för aktuell tjänst, se krav 7.1.

En bedömning av hur ofta säkerhetskopior behöver tas bör även göras. Det kan till exempel vara så att enbart en delmängd av ett systems data är föränderlig eller föränderlig i högre takt än övrig data. Säkerhetskopieringsrutiner bör anpassas efter detta. Konsekvensbedömningen i krav 9 bör användas för att bedöma hur ofta säkerhetskopior behöver tas.

Det är också av vikt att bedöma hur länge information bör eller ska sparas beroende på dess beskaffenhet. Verksamhetsutövare måste ha i åtanke när den bestämmer hur länge säkerhetskopian ska sparas, att ett intrång kan ha funnits långt tillbaka innan intrånget eventuellt resulterar i ett förstörande angrepp. Att läsa tillbaka en säkerhetskopia som eventuellt har skadliga koder, men ej exekverad, riskerar att ej ha större nytta då koden kan exekveras igen i framtiden.

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

En rekommendation är att verksamheten arbetar utefter ”3-2-1”-principen vad gäller säkerhetskopior. Det bör finnas tre kopior av informationen: en kopia är den information leverantören arbetar med till vardags samt två säkerhetskopior på två olika medier, varav en säkerhetskopia lagras utanför verksamhetsstället.

Rutiner för återställning av säkerhetskopior behöver finnas tillgängliga för de som eventuellt behöver verkställa återläsningen. Dessa rutiner bör också finnas tillgängliga på något annat medium än där rutiner normalt lagras eftersom rutinerna riskerar att bli otillgängliga vid en incident. Det rekommenderas att lagra dessa rutiner utskrivna tillsammans där säkerhetskopian finns.

Tänk på att säkerhetskopior som eventuellt innehåller känslig information kan behöva särskilt skydd, 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-CSF: 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 ska regelbundet återläsas och valideras. Det är viktigt att säkerställa att det finns tillräcklig information kring hur system återställs samt att återläsning fungerar. Detta bör göras i en isolerad miljö i vilken 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-CSF: 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 verksamheten har redundanta system.

Vid bedömning av lämplig redundansnivå på infrastruktur för 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 och OT-system samt i så fall hur länge. Anpassa design på redundansen 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 verksamheten via regelbundna tester undersöka systemens riktighet, det vill säga att informationen på systemen faktiskt är aktuell. Exempelvis bör tester utföras där verksamheten regelbundet växlar mellan primärdrift och DR-drift.

Om system inte har stöd för flera nätverkskopplingar för att dra nytta av en redundant nätverksinfrastruktur bör säkerställas att andra åtgärdsplaner finns etablerade (till exempel möjlighet till omgående byte av hårdvara).

Redundans kan även vara en önskvärd egenskap för system som inte är informationssystem i OT-miljöer men som har en viktig funktion i tjänsteleveranser, till exempel processtyrningssystem.

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 och kräver fortlöpande säkerhetsarbete, utveckling och uppföljning. Verksamheten bör upprätta mål och rutiner för att implementera säkerhetsloggning i alla system samt regelbundet följa upp efterlevnaden av de uppsatta rutinerna.

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

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

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän bör synkroniseras mot en och samma säker och robust referenskälla för tid.

För att inte bli överväldigad av information bör en verksamhet 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, detta eftersom säkerhetsarbetet kan försvåras om man vid analys behöver ta hänsyn till och gallra bort driftrelaterade logghändelser. Se till att loggningsnivåerna är hanterbara.

Tid bör läggas på analysen i samband med implementering av nya system eller då nya funktioner tillkommer för att bedöma 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 eftersom *all* användaraktivitet ska sparas och ge möjlighet till granskning av användaraktivitet.

Det är viktigt att säkerställa att loggdata inte kan manipuleras i efterhand. Det kan säkerställas exempelvis genom att lagra loggdata 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.

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 §

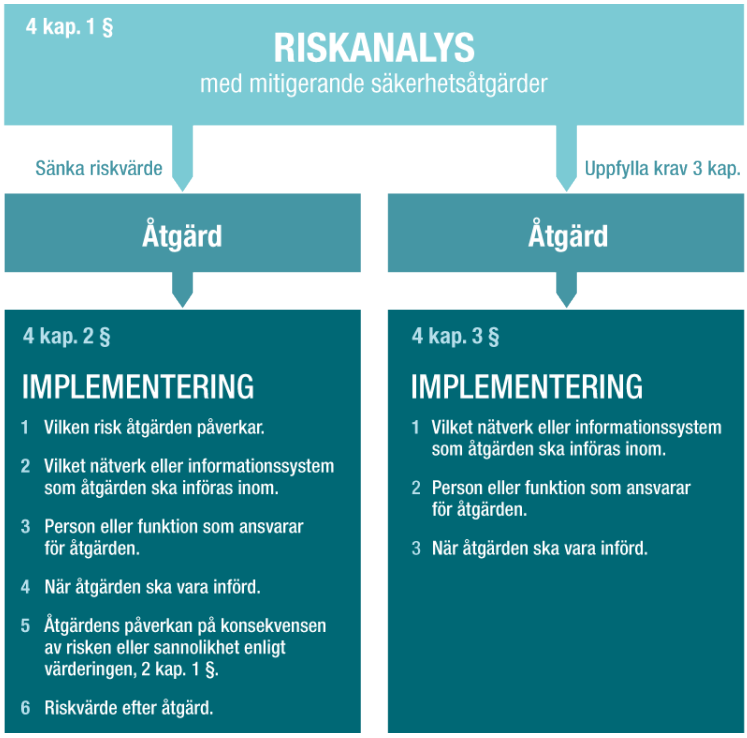
Allmänt råd:

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.

Det är viktigt att notera att kraven för införande av informationssäkerhetskraven, enligt 3 kap. STEMFS 2021:3, skiljer sig ifrån införandet av åtgärder som kommer från riskanalysen i krav 3 samma föreskrift. Bilden nedan beskriver hur de olika informationssäkerhetskraven och riskanalysåtgärderna ska hanteras. Se bilden nedan:



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. se 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 det sammanhang som leverantören verkar i. Vissa åtgärder kan vara irrelevanta för en leverantör varför den då kan avstå från att 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.

Hållbar energi för alla

Energimyndigheten leder samhällets omställning till ett hållbart energisystem.

Vi bidrar med fakta, kunskap och analyser om tillförsel och användning av energi i samhället, och arbetar för en trygg energiförsörjning.

Forskning om framtidens fordon och bränslen, förnybara energikällor och smarta elnät får stöd av oss. Vi stöttar också affärsutveckling som gör det möjligt att kommersialisera innovationer och ny teknik, och ser till att goda lösningar kan exporteras.

Vi ansvarar för Sveriges officiella statistik på energiområdet, och hanterar elcertifikatsystemet och handeln med utsläppsrätter.

Dessutom deltar vi i internationella klimatsamarbeten, och förmedlar fakta om effektivare energianvändning till hushåll, företag och myndigheter.

Energimyndigheten

Energimyndigheten, Box 310, 631 04 Eskilstuna
Telefon 016-544 20 00, Fax 016-544 20 99
E-post registrator@energimyndigheten.se
www.energimyndigheten.se