| Utfärdad: | Träder i kraft: | Giltighetstid: |
|---|---|---|
| 08.04.2025 | 08.04.2025 | tills vidare |

Rekommendationen grundar sig på följande lagstiftning:
Cybersäkerhetslagen (124/2025) 9 och 18 §
Lag om ändring av lagen om informationshantering inom den offentliga förvaltningen (125/2025) 18 c §

Ändringsuppgifter:

# Transport- och kommunikationsverket Traficoms rekommendation till NIS-övervakande myndigheter om åtgärder för riskhantering

## Innehåll

# I Rekommendationens bakgrund och syfte

## Rekommendation till myndigheter

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom (nedan ”Transport- och kommunikationsverket”) har utarbetat denna rekommendation till tillsynsmyndigheter för att övervaka åtgärder för riskhantering inom cybersäkerhet enligt NIS 2-direktivet. Rekommendationen grundar sig på cybersäkerhetslagen (124/2025) och ändringar av lagen om informationshantering inom den offentliga förvaltningen (906/2019) (125/2025) (nedan ”informationshanteringslagen”).

Rekommendationens syfte är att tillhandahålla information för myndigheter om hurdana åtgärder som kan ingå i de lagstadgade kraven. I rekommendationen beskrivs också olika metoder som den övervakande myndigheten enligt sitt övervägande och sin bedömning från fall till fall använder i sina styrnings- och tillsynsuppgifter. Myndigheten kan också anlita den egna organisationens externa bedömningsorgan för informationssäkerhet eller andra informationssäkerhetsexperter. Att anlita extern hjälp kan till exempel vara nödvändigt i en situation när granskningen förutsätter teknisk specialkompetens eller omfattande teknisk förmåga som den övervakande myndigheten inte har. Sådana är till exempel situationer där övervakande myndigheter inte har de verktyg eller den kompetens som behövs för skanningar eller konfigurationsinspektioner.

Transport- och kommunikationsverket konstaterar för tydlighetens skull att rekommendationen inte binder myndigheter eller aktörer, utan styr, bistår och stöder. Bestämmelser om juridiskt bindande skyldigheter finns i lagar, kommissionens genomförandeakter och eventuella preciserande tekniska föreskrifter som utfärdats av tillsynsmyndigheterna och som kan beakta branschspecifika särdrag. Varje övervakande myndighet är behörig att avgöra hurdana åtgärder som uppfyller föreskrivna krav inom respektive sektor. En aktör inom regleringens tillämpningsområde ska å sin sida se till att organisationens verksamhet motsvarar de föreskrivna skyldigheterna.

Transport- och kommunikationsverket konstaterar att uppfyllande av rekommendationen och de i rekommendationen nämnda standarderna eller allmänna referensramarna eller användning av Cybermätaren som utarbetats av Transport-

och kommunikationsverket inte garanterar att aktören uppfyller de föreskrivna skyldigheterna i sin helhet. De bedömningskriterier och standarder som används i rekommendationen är som sådana inte harmoniserade med kraven i cybersäkerhetslagen eller informationshanteringslagen. En punkt i standarden kan till exempel innehålla krav som inte ingår i lagen, så de kan inte direkt jämställas med varandra. Således har bedömningskriterierna och standarderna använts som källor som ger mer information och som exempel, som man inte förpliktar till att använda men som fungerar som hjälp för att påvisa överensstämmelse med kraven.

Rekommendationen har endast skapats för att konkretisera alternativ för verifiering av de åtgärder som avses i 9 § i cybersäkerhetslagen och 18 c § 1–12 punkterna i informationshanteringslagen och som beskrivs närmare i motiveringarna till dessa. Transport- och kommunikationsverket konstaterar dock att rekommendationen även bygger på andra bestämmelser som nära anknyter till riskhanteringsåtgärderna i cybersäkerhets- och informationshanteringslagarna, till exempel den riskbedömning som anknyter till respektive bransch samt aktörens övervägda riskhantering som beaktar proportionalitetsprincipen och bestämmelserna om ledningens ansvar.

Rekommendationerna kan också stödja planeringen av riskhanteringen inom cybersäkerhet för andra aktörer än de som avses i 3 § i cybersäkerhetslagen. Särskilt de rekommendationer om grundläggande praxis för informationssäkerhet som ingår i kapitel 11 har utarbetats så att även aktörer som inte hör till tillämpningsområdet för NIS-regleringen genom att följa rekommendationerna kan utvärdera cybersäkerhetens mognadsnivå och förbättra den.

Transport- och kommunikationsverket har som ett led i myndighetssamarbetet och samordningsuppgiften vid den gemensamma kontaktpunkten utarbetat denna rekommendation till myndigheter som övervakar riskhanteringsåtgärder för cybersäkerhet.

## Rättslig grund

Bakgrunden till rekommendationen är det så kallade NIS 2-direktivet, cybersäkerhetsdirektivet, dvs. Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

I artikel 21 i NIS 2-direktivet föreskrivs om riskhanteringsåtgärder för cybersäkerhet. Enligt punkt 1 i artikeln ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster. De åtgärder som avses i punkt 2 i artikeln ska baseras på en allriskansats som syftar till att skydda

nätverks- och informationssystem och dessa systems fysiska miljö från incidenter. I stycket efter punkt 2 i artikeln nämns omständigheter som minst ska beaktas i den nämnda verksamhetsmodellen.

NIS 2-direktivet har genomförts nationellt med den nya cybersäkerhetslagen samt genom ändringarna i informationshanteringslagen.

Tillämpningsområdet för cybersäkerhetslagen omfattar de i 3 § föreskrivna aktörerna inom olika sektorer. I 9 § i lagen föreskrivs om åtgärder för hantering av cybersäkerhetsrisker. Enligt 1 mom. i paragrafen ska aktörer vidta proportionella tekniska, driftsrelaterade eller organisatoriska hanteringsåtgärder i enlighet med handlingsmodellen för hantering av cybersäkerhetsrisker för att hantera sådana risker som hänför sig till säkerheten i kommunikationsnät och informationssystem och förhindra eller minimera skadliga verkningar. I 2 mom. i paragrafen föreskrivs att i handlingsmodellen för hantering av cybersäkerhetsrisker och de hanteringsåtgärder som baserar sig på den ska de frågor som räknas upp i punkterna 1–12 i momentet beaktas och uppdateras. I denna rekommendation behandlas tillämplig praxis för dessa 12 punkter som separata kapitel.

När det gäller aktörer inom den offentliga förvaltningen har kraven som hänför sig till riskhanteringsåtgärder för cybersäkerhetsäkerhet genomförts i informationshanteringslagen. I 3 § i lagen föreskrivs närmare om vad kraven för aktörer inom den offentliga förvaltningen gäller. I informationshanteringslagen finns kraven på riskhanteringsåtgärder inom cybersäkerheten i 4 a kap. 18 c §. Kraven har samma innehåll som i cybersäkerhetslagen.

Enligt 18 § i cybersäkerhetslagen är Cybersäkerhetscentret vid Transport- och kommunikationsverket den gemensamma kontaktpunkt som avses i artikel 8.3 i NIS 2-direktivet. Enligt 2 mom. är uppgiften för en gemensam kontaktpunkt att främja samarbetet och samordningen mellan tillsynsmyndigheterna vid fullgörandet av uppgifter enligt denna lag. Enligt motiveringarna i förordningen kan en gemensam kontaktpunkt främja samarbetet och informationsutbytet mellan de tillsynsmyndigheterna samt ge rekommendationer till tillsynsmyndigheterna i syfte att samordna kraven och tillsynen enligt lagen.

I den ovannämnda nationella genomförande lagstiftningen föreskrivs inte strängare krav än i NIS 2-direktivet, utan det har genomförts i enlighet med principen minimal harmonisering.

## Beredning och upprätthållande av rekommendationen

Transport- och kommunikationsverket har vid utarbetandet av denna rekommendation parallellt granskat den nationella cybersäkerhetslagen och informationshanteringslagen, NIS 2-direktivet, samt genomförandeförordning (EU) 2024/2690 och dess kompletterande dokument som har beretts i samarbete mellan medlemsstaterna, kommissionen och ENISA samt ett flertal kriterier och utvärderingsverktyg för informationssäkerhet såsom ISO/IEC 27001, IEC 62443, NIST CSF, Julkri och Cybermätaren. Med hjälp av dessa och den erfarenhet som

ackumulerats i ämbetsverkets olika informationssäkerhetsuppgifter har man försökt fastställa allmän praxis för cybersäkerhet som är lämplig för de i lagen framställda riskhanteringsåtgärderna för cybersäkerhet och tillsynen av dem.

Under beredningen av rekommendationen har man diskuterat med tillsynsmyndigheter som övervakar verksamheten enligt det s.k. NIS-direktivet (EU) 2016/1148 och med de nya tillsynsmyndigheterna enligt NIS 2-direktivet. Syftet med diskussionerna har bland annat varit att kartlägga omfattningen av de aktörer som omfattas av myndigheternas tillsyn och myndigheternas beredskap för tillsyn enligt den nya regleringen. I diskussionerna behandlades i synnerhet frågor om den kompetens och de resurser som behövs inom tillsynen samt förvärvande av extern hjälp. Myndigheterna önskade hjälp särskilt i tillsynen av teknisk cybersäkerhet både för utförande av tillsynen och utvärdering av tillsynsresultaten. Dessa frågor har man försökt besvara i denna rekommendation som har kompletterats under beredningen på basis av diskussioner med de ovannämnda myndigheterna.

Transport- och kommunikationsverket bad tillsynsmyndigheterna om utlåtanden om utkastet till rekommendation om åtgärder för riskhantering för cybersäkerhet enligt NIS 2-direktivet. Rekommendationen var på remiss i tjänsten utlåtande.fi på finska i 8 veckor under tiden 5.4.2024–31.5.2024 (diarienummer för begäran om utlåtande: Traficom/18410/09.00.02/2023). Begäran om utlåtande riktades särskilt till tillsynsmyndigheter som avses i cybersäkerhetslagen, men det var möjligt för alla intresserade att yttra sig.

Sammanlagt mottogs 16 utlåtanden om rekommendationen.

Ett sammandrag av utlåtandena har utarbetats, där den viktigaste responsen från utlåtandena beskrivs. Sammandraget finns på Transport- och kommunikationsverkets webbplats[1].

Med anledning av remissvaren har det gjorts ändringar, preciseringar och kompletteringar i rekommendationen.

Enligt remissvaren anses utkastet till rekommendation allmänt taget fungera som stöd för de övervakande myndigheterna och aktörerna. Rekommendationen upplevs konkretisera genomförandet av de riskhanteringsskyldigheter som lagstiftningen medför på praktisk nivå. Innehållet i utkastet till rekommendation anses i princip vara heltäckande och strukturen tydlig, eftersom den följer strukturen för motsvarande delar i regeringens proposition om en cybersäkerhetslag. Tabelluppställningen som hade valts som presentationssätt upplevs förbättra begripligheten. Det att varje enskild rekommendationsåtgärd är motiverad och innehåller en tydlig hänvisning till referensramarna ansågs som en bra lösning.

Å andra sidan upplever man det som problematiskt att varje riskhanteringsåtgärd granskades som en enskild åtgärd separat från de övriga kraven, eftersom det

[1] https://kyberturvallisuuskeskus.fi/sites/default/files/media/file/Sammandrag%20av%20remissvaren%20till%20Traficoms%20utkast%20till%20rekommendation%20till%20NIS_%C3%B6vervakande%20myndigheter.pdf

kan leda till att hanteringen av varje risk inleds med samma intensitet. Dessutom önskas det att den inbördes kompensationen mellan åtgärderna i rekommendationen beaktas bättre. Rekommendationen upplevdes också som lång och därför önskas ett sammandrag av hanteringsåtgärderna.

I rekommendationen har man medvetet strävat efter att presentera varje riskhanteringsåtgärd som en egen självständig helhet och beskriva innehållet i hanteringsåtgärden. Detta har lett till att exemplen delvis överlappar varandra. Motiveringstexten för varje enskild riskhanteringsåtgärd som presenteras i rekommendationen anses fungera som ett sammandrag.

Rekommendationens terminologi har förtydligats och hänvisningarna i rekommendationen preciserats. Rekommendationens inledning har kompletterats och preciserats till den del responsen gällt riskbasering, proportionalitetsprincipen, ledningens ansvar och rekommendationens förhållande till eventuella preciserande tekniska föreskrifter som myndigheterna utfärdat. Dessutom har läsanvisningen kompletterats genom att precisera definitionen av aktörer på högre mognadsnivå.

Motsvarigheten mellan riskhanteringsåtgärderna i rekommendationen och de referensramar (standarder och bedömningskriterier) som tillämpades i rekommendationen upplevs som problematisk. Ett korshänvisningsdokument som utarbetats av Transport- och kommunikationsverket har utifrån responsen fogats till rekommendationen, men rekommendationens inledning kompletterades för att undvika eventuella missförstånd om att det skulle vara fråga om harmoniserade standarder som direkt uppfyller lagens krav.

Det gavs både allmänna utlåtanden och åtgärdsspecifika utlåtanden om riskhanteringsåtgärderna i rekommendationen. Rekommendationen har i första hand uppdaterats så att den motsvarar den ändrade regeringspropositionen om cybersäkerhetslagen och därefter har remissvaren om cybersäkerhetsåtgärderna från remissrundan om möjligt beaktats genom ändringar eller preciseringar av rekommendationen. Observationer om branschspecifika standarder och anvisningar har fogats till rekommendationen i enlighet med förslagen.

Enligt remissvaren anses det vara problematiskt att remissförfarandet för utkastet till rekommendationen ordnades innan riksdagsbehandlingen av cybersäkerhetslagen avslutats, vilket även Transport- och kommunikationsverket känt till. Transport- och kommunikationsverket skickade utkastet till rekommendation på remiss trots den utmanande tidpunkten för remissförfarandet, eftersom detta ansågs konkretisera genomförandet av riskhanteringsåtgärderna även i sin halvfärdiga form och vara till hjälp särskilt för de nya tillsynsmyndigheterna och aktörerna inom lagstiftningens tillämpningsområde.

Rekommendationen gäller tills vidare från 08.04.2025. Rekommendationen uppdateras vid behov på basis av respons från intressentgrupper och praktiska erfarenheter.

## Bedömning av konsekvenser

Informationssamhälls- och säkerhetskonsekvenser

Syftet med den nya lagstiftningen om riskhantering inom cybersäkerhet och därigenom också med denna rekommendation är att förbättra säkerheten och funktionssäkerheten i ett samhälle som är beroende av kommunikationsnät och informationssystem. Genom diskussioner som förts under beredningen av rekommendationen och som förs vid användningen av rekommendationen är det möjligt att konkret utvärdera och främja cybersäkerhetens mognadsnivå och tillstånd inom olika sektorer. Syftet med rekommendationen är att öka och stärka den allmänna driftsäkerheten och säkerheten i de kommunikationsnät och tjänster som används inom olika sektorer i samhället. Rekommendationen bedöms främja och stärka samhällets cybersäkerhet.

En del av den nya lagstiftningen är grundläggande praxis för informationssäkerhet (praxis för cyberhygien i NIS 2-direktivet). Kapitel 11 i rekommendationen innehåller rekommendationer för grundläggande praxis för informationssäkerhet som alla aktörer i samhället kan använda oberoende av om aktören omfattas av de lagstadgade skyldigheterna. I det avseendet är syftet att förbättra samhällets cybersäkerhet.

Konsekvenser för myndigheter

Rekommendationens mål är att göra styrningen, rådgivningen och tillsynen på samhällelig nivå för den nationella lagstiftningen konsekventare och enhetligare. Rekommendationen ger myndigheter verktyg som kan användas för att utarbeta föregripande material för aktörerna för rådgivning, styrning och tillämpning av kraven, liksom även i utarbetandet av eventuella bestämmelser om riskhanteringsåtgärder för cybersäkerhet. Syftet med rekommendationen är att stödja myndigheterna så att de inte behöver skapa alla metoder och all praxis från början. De övervakande myndigheternas kompetens och resurser varierar bland annat för att uppgifterna enligt den nationella lagstiftningen är nya för myndigheterna. På grund av skillnaderna mellan olika branscher kan vi i rekommendationen inte ta upp sektorspecifika särdrag.

Rekommendationen torde ha positiva effekter på de övervakande myndigheterna och är ett stöd för samarbetet mellan olika tillsynsmyndigheter. Om rekommendationen tillämpas i stor utsträckning förenhetligas tillsynsmyndigheternas tillsynspraxis inom olika sektorer. Detta bidrar också till transparens i myndighetsverksamheten och förutsägbar tillsynsverksamhet samt konsekvens bland aktörerna.

I beredningen av rekommendationen har man strävat efter teknikneutrala och allmängiltiga lösningar. Det är dock svårt att förutse framtidens tekniker, vilket kan medföra att rekommendationen behöver uppdateras. Att hålla rekommendationen uppdaterad kan visa sig vara utmanande på grund av den snabba tekniska utvecklingen.

På grund av omfattningen av saker som rekommenderas och deras tekniska natur har lättare informationsstyrning inte lika omfattande inverkan som rekommendationen när det gäller myndighetsrådgivning i enskilda situationer, utbildningar som ordnas då och då eller vanliga frågor som publiceras på myndigheternas webbplatser. Med hjälp av rekommendationen är det möjligt att underlätta det aktörspecifika behovet av handledning.

Konsekvenser för aktörer

Rekommendationen bidrar till att cybersäkerhetsrisker i framtiden bedöms heltäckande som en del av aktörens riskhantering och att förändringar i verksamhetsmiljön och förändringarnas konsekvenser för verksamheten identifieras bättre. Dessutom möjliggör rekommendationen proportionell bedömning av riskhanteringsåtgärder i förhållande till risken och stöder genomförande av riskhantering. Genom att vidta åtgärder enligt rekommendationen kan aktörerna bättre återhämta sig från cyberstörningar och därmed producera säkrare och tillförlitligare tjänster för hela samhället.

I rekommendationen beaktas med tanke på riskhanteringen också upphandlingar och leveranskedjor. Genomförande av åtgärder enligt rekommendationen gör det möjligt för aktören att skapa en bättre lägesbild av eventuella risker. I synnerhet när det gäller upphandlingar syftar rekommendationen till att tillhandahålla verktyg för att identifiera och hantera cyberrisker i anslutning till upphandlingar.

Aktören kan ha flera fördelar av en bra riskhantering. Om man genom rekommendationen lär sig att hantera cybersäkerhetsrisker kan det underlätta aktörernas börda vid en möjlig certifiering som krävs inom sektorn eller som skaffas frivilligt. Ett riskhanteringssystem som upprätthålls och är bra stöder på lång sikt aktörernas affärsverksamhet och bidrar till att identifiera möjligheter att utveckla affärsverksamheten. Att följa rekommendationen kan förhindra att en cyberrisk realiseras, varvid det inte krävs ekonomiska resurser för utredning av störningen och återhämtning från den. Aktören kan med hjälp av rekommendationen också lära sig bedöma betydelsen av en kvarstående risk och förbereda sig för den. Dessutom kan aktören med hjälp av rekommendationen bättre definiera ansvarsfördelningen som hänför sig till den kvarstående risken.

## Definitioner

Definitionerna som presenteras här grundar sig till stor del på cybersäkerhetslagen och definitionerna i regeringspropositionen som hänför sig till den samt definitioner i TEPA-termbanken[2]. Vid varje definition anges en källhänvisning. Denna punkt innehåller särskilt de definitioner som presenteras i rekommendationen och som inte finns i 2 § Definitioner i cybersäkerhetslagen.

**Aktör** (entity) avser en juridisk eller fysisk person som bedriver verksamhet enligt bilaga I eller II till cybersäkerhetslagen eller tillhör en aktörstyp enligt bilaga I eller II och uppfyller eller överskrider definitionen av en medelstor aktör, eller

[2] Terminologicentralen är en samling fackordlistor och ordböcker https://termipankki.fi/tepa/sv/

är en storleksoberoende aktör, eller uppfyller särskilda kriticitetskriterier. (Cybersäkerhetslagen 3 §)

**Betydande incident** (significant incident) avser en incident som har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten, eller en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

**Riktlinjer för riskhantering** (risk management policy) avser planering på högsta nivå i organisationen i syfte att systematiskt identifiera, bedöma och hantera risker som hänför sig till organisationen eller dess verksamhet, ställa upp mål och kontrollera hur målen uppnås. För motsvarande riktlinjer kan termen riskhanteringspolicy användas. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

**Handlingsmodell för riskhantering** (risk management procedure/process) avser en riskhanteringsprocess för att regelbundet identifiera, analysera, utvärdera och hantera risker i kommunikationsnät och informationssystem och i deras fysiska miljö. Som en del av handlingsmodellen för riskhantering utvärderas riskhanteringsåtgärdernas effektivitet med lämpliga indikatorer. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

**Riskhanteringsåtgärder** (risk management measures) avser av aktören genomförda åtgärder för att hantera, förebygga och förhindra risker som hänför sig till säkerheten i kommunikationsnät och informationssystem och förhindra eller minimera skadliga verkningar. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

**Riktlinjer som gäller säkerheten** (information security policy) avser aktörens syn på informationssäkerhetens mål, principer och genomförande under hela livscykeln för kommunikationsnät och informationssystem. För motsvarande riktlinjer i anknytning till standard ISO/IEC 27001 används termen informationssäkerhetspolicy. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

**Förfaranden som gäller säkerheten** (information security procedures/processes) avser olika processer och tekniska förfaringssätt för att genomföra riktlinjerna i anknytning till säkra kommunikationsnät och informationssystem. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

Praxis **som gäller säkerheten** (information security practices) avser olika funktionssätt i anknytning till informationssäkerhet och cybersäkerhet som används i praktiken för att genomföra förfaranden som gäller säkerheten. (Cybersäkerhetslagen, motiveringarna till regeringens proposition)

**Autentisering eller verifiering** (verification) avser ett förfarande för att försäkra sig om objektets sanningsenlighet, riktighet och ursprung. Det finns olika

nivåer av autentisering. Den kan vara stark eller svag och göras på önskad tillitsnivå. (TEPA-termbanken)[3].

I denna rekommendation kan autentisering eller verifiering (authentication) även användas som en del av åtkomsthanteringen, varvid termen definieras separat.

**Konfiguration** (configuration) avser fastställande av programvarans eller enhetens funktionsinställningar. (TEPA-termbanken)

**Härdning** (hardening) avser att funktionsinställningarna fastställs så att endast funktioner, enheter och tjänster som är väsentliga med tanke på användningskraven och behandlingen av uppgifter har tagits i bruk. (Katakri)[4]

**Zonindelning** (segmentation) avser åtskiljande av nätet genom att begränsa nätmiljön till hanterbara helheter. Zonindelning kan också kallas segmentering. (Katakri)

**Nollförtroendeprincipen** (zero trust) avser en princip där ett datanät, en enhet, en användare eller en applikation inte automatiskt garanterar vissa rättigheter eller åtkomst till information eller informationssystem. Enligt principen förutsätter varje åtgärd i informationssystemet alltid identifiering och åtgärderna övervakas kontinuerligt och automatiskt. Principen om nollförtroende kan också kallas principen om nolltillit. (Katakri)

**Säkerhetskopia** (backup) avser en kopia av data som är avsedd att användas om originalet går förlorat till exempel på grund av fel eller skada. (TEPA-termbanken)

**Reservsystem** (backup/redundant system) avser ett system som kan tas i bruk när användningen av ett normalt system störs eller förhindras. Reservsystemet behöver inte vara exakt likadant som det normala systemet, förutsatt att det ger tillräckligt likadan beredskap som det normala systemet. (TEPA-termbanken)

[3] Terminologicentralen är en samling fackordlistor och ordböcker https://termipankki.fi/tepa/sv/
[4] https://um.fi/katakri-verktyg-for-informationssakerhetsauditering-for-myndigheter

# II Läsanvisning för rekommendationen

I de följande kapitlen fokuserar var och ett på en av de riskhanteringsåtgärder för cybersäkerheten som räknas upp 9 § 2 mom. i cybersäkerhetslagen och i 18 c § 1 mom. i informationshanteringslagen. Åtgärderna presenteras i samma ordning som i lagarna. I genomförande av åtgärder och tillsyn kan det vara motiverat att framskrida i annan ordningsföljd än i denna rekommendation. I tillsynsverksamheten kan det dessutom vara motiverat att koncentrera sig särskilt på de tillsynsåtgärder som är viktigast när det gäller den sektor eller aktör som övervakas.

Alla åtgärder som presenteras för hantering av cybersäkerhetsrisker uppdelas vidare i specifikare rekommendationer som presenteras i form av en förteckning. Efter förteckningen över rekommendationer ges mer detaljerade motiveringar i tabellen för varje rekommendation.

I slutet av varje riskhanteringsåtgärd som presenteras i tabellform ingår utvidgade anvisningar för sådana aktörer av vilka tillsynsmyndigheten förväntar sig en högre mognadsnivå. Förteckningen och tabelleringen av rekommendationerna följer i övrigt samma ordning.

I anvisningarna för aktörer med högre cyberrisk har man i första hand beaktat genomförandeförordningen (EU) 2024/2690 som godkänts av kommissionen med stöd av artikel 21.5 i NIS 2-direktivet, genom vilken man har fastställt tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet för

- leverantörer av DNS-tjänster
- registreringsenheter för toppdomäner
- leverantörer av molntjänster
- leverantörer av datacentraltjänster
- leverantörer av nätverk för leverans av innehåll
- leverantörer av utlokaliserade driftstjänster
- leverantörer av utlokaliserade säkerhetstjänster
- leverantörer av marknadsplatser online
- leverantörer av sökmotorer
- leverantörer av plattformar för sociala nätverkstjänster och
- tillhandahållare av betrodda tjänster.

Kraven på en högre mognadsnivå kan också vara motiverade för andra aktörer som omfattas av tillämpningsområdet för cybersäkerhetslagen och informationshanteringslagen utifrån aktörens riskbedömning och sektorspecifika särdrag. Sådana aktörer kan till exempel vara stora organisationer som har egen programutveckling. Kommissionen kan i fortsättningen också godkänna andra genomförandeakter som gäller centrala och viktiga aktörer och som stärker kraven på riskhanteringsåtgärder.

**Exempel på genomförande**

- I exemplen på genomförande beskrivs på vilket sätt den i tabellen beskrivna rekommendationen eller delar av den kan genomföras och hurdana genomföranden myndigheten kan möta i samband med tillsyn.
- Exemplen på genomförande är inte uttömmande, utan deras syfte är att ge exempel i synnerhet för situationer där man inte har tidigare erfarenhet av att genomföra de saker som beskrivs i rekommendationen. Omfattningen av genomföranden bör dock vara i lämplig relation till risken som hänför sig till verksamheten och till verksamhetens övriga krav.
- De åtgärder som behövs kan variera betydligt beroende på aktörens storlek, sektorn och vilka hot som riktas mot aktören. I exemplen på genomförande har man dock i mån av möjlighet försökt beakta olika aktörer och deras olika behov.

**Verifiering**

I verifieringen beskrivs exempel på hur tillsynsmyndigheten kan verifiera att aktörens åtgärder för hantering av cybersäkerhetsrisker har genomförts. Verifieringsexemplen är indelade i olika kategorier på grundval av det tekniska kravet. Tillsyn enligt olika kategorier ger olika grad av tillförlighet om aktörens cybersäkerhetssituation vid tillsynsögonblicket. Åtgärder inom olika kategorier kan också väljas för att användas beroende på vilka resurser som finns tillgängliga.

1. I kategori 1 beskrivs huvudsakligen tillsyn som grundar sig på dokumentation eller självbedömning. En granskning som grundar sig på dokumentation eller självbedömning ger sällan en ingående bild av den verkliga cybersäkerhetssituationen. Därför rekommenderas att åtminstone vissa saker i kategorierna 2 och 3 tas upp till granskning. Genom att använda genomförandeexemplen i kategori 1 kan tillsynsmyndigheten dock relativt enkelt få en uppfattning om sektorns helhetssituation genom att rikta samma typ av tillsyn eller självbedömning till ett stort antal aktörer.
2. I kategori 2 beskrivs en mer ingående inspektion av nuläget för aktörens åtgärder. Kategorin fokuserar emellertid på tekniskt enkla metoder såsom intervjuer, konfigurationsinspektioner eller motsvarande bevis. I granskningen av kategori 2 är det vanligt att utnyttja tekniska bevis som aktören lämnat in.
3. I kategori 3 beskrivs tekniskt mångsidigare metoder som i allmänhet kräver beredning och olika färdigheter, såsom användning av olika program och verktyg samt förmåga att tolka tekniska data. Sådana kan till exempel vara olika skanningar som förutom av myndigheten även kan utföras av aktören eller en tredje part.

I tillsynen rekommenderas att använda metoder inom olika kategorier som till exempel också grundar sig på sårbarheter som beror på risker inom sektorn eller sektorns natur. Kommunikationsnät och informationssystem kan ha mycket olika omfattning och avvikande teknik och innehålla många detaljer som påverkar cybersäkerheten. Det är också vanligt att självbedömningen och inspektionen av dokument inte ger en realistisk bild av cybersäkerhetssituationen i kommunikationsnäten och informationssystemen. Självbedömningen beror naturligtvis även

på den erfarenhet som den som gör självbedömningen har och den tillgängliga tiden. Den bild av systemets situation som fås genom självbedömningar kan kompletteras med andra verifieringsmetoder.

Tillsynsmyndigheten överväger vilka metoder den anser vara nödvändiga att använda i sin tillsynsverksamhet. Myndigheten kan utöver utredning och bevis från aktören utföra granskningar och andra observationer själv eller anlita externa bedömningsorgan, såsom bedömningsorgan för informationssäkerhet eller andra kompetenta experter inom informationssäkerhet. I vissa situationer kan tillsynen även förutsätta samarbete med en annan tillsynsmyndighet i Finland eller i en annan medlemsstat.

**Motiveringar**

I motiveringarna ges vissa praktiska motiveringar till varför åtgärden enligt rubriken finns i lagstiftningen och varför den har inkluderats i rekommendationen samt vad den syftar till.

Motiveringarna ger verktyg för diskussion mellan tillsynsmyndigheten och aktören om grunderna för kraven. Motiveringarna hjälper tillsynsmyndigheten att tolka om de åtgärder som aktören vidtagit till exempel skyddar mot de hotaspekter som nämns i motiveringarna.

Motiveringarna har till vissa delar lämnats bort. Då har det ansetts att separata motiveringar inte ger mervärde utöver de genomförandeexempel eller tillsynsmetoder som redan anges i tabellen.

**Källor**

I källhänvisningarna ges exempel på allmänt kända standarder, referensramar och anvisningar som hänför sig till rekommendationen i fråga. I dessa kan tillsynsmyndigheten söka mer information eller beskrivningar av allmänt använda genomföranden.

Listan är exemplifierande och man har försökt framhäva specifika punkter i sådana standarder och referensramar som särskilt tjänar målen för varje rekommendation. Inom sektorn kan det även användas andra relevanta standarder och referensramar.

**Verktyg**

I verktygen nämns bedömningsverktyg och indikatorer samt verktyg och programvara som tillsynsmyndigheten kan använda i sin tillsynsverksamhet. Också aktören kan använda verktygen för att mäta sin egen mognadsnivå och för utveckling av verksamheten.

# 1 Riktlinjer för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om åtgärderna

Rekommendationerna grundar sig på artikel 21.2 f och delvis a i NIS 2-direktivet. Om nationellt genomförande av dessa föreskrivs i 9 § 2 mom. 1 punkten i cybersäkerhetslagen och 18 c § 1 mom. 1 punkten i informationshanteringslagen.

1. **Handlingsmodell för hantering av cybersäkerhetsrisker**: Aktören ska ha en handlingsmodell för hantering av cybersäkerhetsrisker för att regelbundet identifiera, analysera, utvärdera och hantera risker i kommunikationsnät och informationssystem och i deras fysiska miljö. Vid bedömningen av verksamhetsprincipernas och åtgärdernas effektivitet ska riskhanteringens karaktär som en kontinuerlig del av organisationens verksamhet beaktas, vilket förutsätter att bedömningen av verksamhetsprincipernas och åtgärdernas effektivitet inkluderas i hanteringsåtgärderna. Det rekommenderas att riktlinjerna och handlingsmodell för hantering av cybersäkerhetsrisker baserar sig på aktuella bästa praxis och standarder inom branschen. (Se punkt 1.1 och 1.1.1).

2. **Ett tillvägagångssätt som beaktar alla riskfaktorer:** Vid riskhanteringen ska man följa en allriskansats och säkerställa att företagets företagsstyrning och riskhanteringsprocesser beaktar informations- och cybersäkerhetsriskerna. (Se punkt 1.2).

3. **Identifiering av behov och funktioner:** Utgångspunkten för riskhanteringen ska vara att identifiera de behov som hänför sig till konfidentialitet, integritet, tillgänglighet och äkthet samt de tjänster, system, processer och personer som är centrala med tanke på funktionerna. Identifieringen hänför sig till punkt 5 om tillgångsförvaltning. (Se punkt 1.3).

4. **Identifiering av cyberhot**: Riskhanteringen förutsätter att hot mot aktören identifieras och att sannolikheten för och konsekvenserna av dessa bedöms. (Se punkt 1.4 och 1.4.1).

5. **Riskhantering:** Riskhanteringen bör syfta till att hantera riskerna så att sannolikheten för eller effekten av dem minimeras, elimineras eller läggs ut på entreprenad och de risker som kvarstår efter riskhanteringen kan godkännas på motiverade grunder. (Se punkt 1.5).

6. **Riskhanteringens ändamålsenlighet och indikatorer:** Riskhanteringens ändamålsenlighet ska regelbundet utvärderas med hjälp av lämpliga indikatorer så att de valda åtgärdernas ändamålsenlighet kan mätas och vid behov förbättras. Bedömningen kan göras exempelvis genom självbedömning eller med hjälp av oberoende tillhandahållare av informationssäkerhetstjänster. I riskhanteringen bör effekterna av riskhanteringsåtgärderna bedömas i förhållande till de hot som riktas mot aktören och de förutsebara konsekvenserna av dem. (Se punkt 1.6 och 1.6.1).

## 1.1 Handlingsmodell för hantering av cybersäkerhetsrisker

**Exempel på genomförande**

- Aktören ska ha en handlingsmodell för hantering av cybersäkerhetsrisker för att skydda kommunikationsnät och informationssystem och deras fysiska miljö mot incidenter och deras verkningar. Handlingsmodellen för hantering av cybersäkerhetsrisker utgör en central del av aktörens riskhanteringshelhet. Handlingsmodellen för riskhantering är i allmänhet en del av organisationens ledningssystem och stöder organisationens affärsstrategi. Den högsta ledningen har godkänt handlingsmodellen för riskhantering samt roller, ansvar och befogenheter som är viktiga med tanke på informationssäkerhet och riskhantering, se punkt 6.1 Förfaranden för personalsäkerheten.
- Aktören har dokumenterat handlingsmodellen för riskhantering och de utarbetade riskbedömningarna, och de finns tillgängliga. Av dokumentationen framgår riktlinjerna och det valda dokumenteringssättet. I handlingsmodellen beskrivs riskhanteringsprocessen, utvärderingen och utvecklingen av handlingsmodellen samt praxis för bedömning och mätning av effekterna av riskhanteringsåtgärderna samt kontinuerlig förbättring. Av dokumentationen framgår ledningens engagemang, viktiga roller och ansvar med tanke på riskhanteringen, riskägarna och ansvarspersonerna för hanteringsåtgärderna.
- Aktören har beskrivit riskhanteringsprocessen och inkluderat nödvändiga skeden i den, såsom riskidentifiering, analys och bedömning av verkningar samt förfaranden för hanteringen av riskerna inklusive förfaranden för val av hanteringsåtgärd och hantering av kvarstående risk samt ledningens syn. Se punkt 1.5 Riskhantering.
- Riskhanteringens riktlinjer och åtgärder är lämpliga för aktörens behov, och har utvecklats kontinuerligt och när verksamhetsmiljön förändras. Som en del av hanteringsåtgärderna ska man även bedöma deras effektivitet för att säkerställa att de valda riskhanteringsåtgärderna är uppdaterade. Se punkt 1.6 Bedömning av effektiviteten
- Det rekommenderas att handlingsmodellen för riskhantering baserar sig på riskhanteringsmetoder och verktyg enligt kända standarder eller bästa praxis inom sektorn.
- Det rekommenderas att handlingsmodellen för riskhantering även innefattar sektorsspecifika riktlinjer och regler, standarder och sektorsspecifik lagstiftning.
- Aktören har regelbundet utfört riskhantering och i synnerhet när det sker ändringar eller betydande incidenter i verksamheten eller verksamhetsmiljön.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har en dokumenterad handlingsmodell för riskhantering inom cybersäkerhet, riskförteckningar och anvisningar samt en eventuell bedömning av förändringseffekterna. Dokumenten är tillgängliga för personalen. Av handlingsmodellen och dokumentationen framgår

de olika faserna i riskhanteringsprocessen, såsom riskidentifiering, analys, bedömning och behandling samt genomförda riskhanteringsåtgärder. Av handlingsmodellen framgår hur riskhanteringen inom cybersäkerheten genomförs och dokumenteras som en del av organisationens verksamhet och hur man vid riskhanteringen beaktar risker i kommunikationsnät och informationssystem och i deras fysiska miljö samt hur aktören i riskhanteringsåtgärderna har inkluderat en bedömning av riktlinjernas och åtgärdernas effektivitet. Av handlingsmodellen framgår också hur ledningens ansvar realiseras i handlingsmodellen för riskhantering och eventuella roller och befullmäktiganden i anknytning till riskhantering (se 6.1). Av riskanteringsmodellen framgår hur regelbunden och kontinuerlig riskhanteringen är, vilket även kan bedömas genom inspektion av handlingsmodellens förändringshistorik. Om handlingsmodellen baserar sig på en viss standard eller referensram, ska det framgå tydligt av dokumentationen. Av dokumentationen ska framgå vilken standard eller referensram som har använts och hur den har tillämpats (till vilka delar och till vilka delar inte).

2. Tillsynsmyndigheten verifierar genom att intervjua aktörens personal om hur handlingsmodellen för hantering av cybersäkerhetsrisker upprätthålls och utvecklas. Av intervjuerna ska framgå att riskhantering genomförs för risker i kommunikationsnät och informationssystem och deras fysiska miljö. Genomförande av riskhanteringsmodellen i praktiken verifieras genom att intervjua personalen om handlingsmodellen för riskhantering och anmälningspraxis för cybersäkerhetsrisker i organisationen. Personalen har kunskap att i tillämpliga delar genomföra riskhantering som en del av det dagliga arbetet. Personalen har kunskap om att anmäla risker och incidenter de upptäcker (se 9).

**Motiveringar**

Risker som riktas mot kommunikationsnät och informationssystem som används i aktörens funktioner och tjänsteutbud ska identifieras, bedömas och hanteras regelbundet och som en etablerad del av organisationens riskhantering. Handlingsmodellen för riskhantering ska utvärderas regelbundet och alltid när det sker ändringar i verksamhetsmiljön. Med rätt dimensionerad riskhantering i förhållande till verksamheten förhindrar och minimerar man incidenters inverkan på verksamheten, verksamhetens kontinuitet, mottagarna av tjänster och andra tjänster.

**Källor**

ISO/IEC 27001:2022 (6.1, 6.2, 8.2, 8.3)

ISO/IEC 27005:2022 (5.1, 5.2, 6.3, 6.5, 7, 8, 9, 10.4)

ISO 31000:2018

IEC 62443-2-1:2010 (4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.11, 4.2.3.12, 4.2.3.13, 4.3.2.6.3, 4.3.2.6.5, 4.3.2.6.6, 4.3.3.2.6, 4.3.4.2)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4, Annex B)

| |
|---|
| IEC 62443-2-4:2015 (SP 02.01, SP 03.01) |
| IEC 62443-2-4:2024 (SP.03.01) |
| NIST CSF 1.1 (ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.GV-4, ID.RM-1, ID.RM-2, ID.RM-3) |
| NIST CSF 2.0 (ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, GV.RM-01, GV.RM-02, GV.RM-03, GV.PO-01, GV.PO-02) |
| NIST SP 800-30 rev 1 (2.1, 2.2, 2.4, 3.1, 3.2, 3.3) |
| NIST SP 800-37 rev 2 (2.1, 2.2, 3.1, E) |
| COSO Enterprise Risk Management Framework |
| Handbok för riskhantering för aktörer inom statsförvaltningen (på finska) |
| NIS CG Reference document (3.3.1 Risk management framework) |
| NIS CG Implementing guidance (2.1 Risk management framework) |
| **Verktyg** |
| Julkri (HAL-06) |
| Cybermätaren (CRITICAL-2, RISK-1, RISK-2, RISK-3, RISK-4, RISK-5, THIRD-PARTIES-2, ARCHITECTURE-1, PROGRAM-1, PROGRAM-2) |

### 1.1.1 Handlingsmodell för riskhantering – utökade anvisningar

| |
|---|
| **Exempel på genomförande** |
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br>• Förutom punkt 1.1 har aktören skapat och upprätthållit för sig lämpliga hanteringskriterier. I hanteringskriterierna har man bestämt för aktören lämpliga förfaranden för fastställande av risknivåer och hanteringen av dem.<br>• Riskhanteringskriterierna kan innefatta förfaringssätt för val av riskhanteringsmetoder som till exempel kan vara att behålla risken, minimering av konsekvenserna, eliminering och att lägga ut på entreprenad.<br>• Av riskhanteringskriterierna ska framgå aktörens risktolerans och praxis för godkännande av kvarstående risker. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har bestämt och på tillräcklig nivå dokumenterat riskhanteringskriterierna. |

| |
|---|
| 2. Tillsynsmyndigheten försäkrar sig om att riskhanteringskriterierna uppfylls genom inspektion av riskhanteringen och dokumenteringen av kvarstående risker. Dessutom kan tillämpningen av kriterierna verifieras genom att intervjua personalen. |
| **Motiveringar** |
| De fastställda kriterierna för handlingsmodellen för riskhantering hjälper organisationen att ta fram riskbedömningar som är jämförbara sinsemellan. |
| **Källor** |
| ISO/IEC 27001:2022 (6.1.2)<br>ISO/IEC 27005:2022 (6.4, 8.1)<br>ISO 31000:2018 (6.3.2, 6.3.4)<br>IEC 62443-2-1:2024 (ORG 2.1)<br>NIST CSF 1.1 (ID.RM-2, ID.RM-3)<br>NIST CSF 2.0 (GV.RM-02, GV.RM-03, GV.RM-06)<br>NIS CG Reference document (3.3.1 Risk management framework)<br>NIS CG Implementing guidance (2.1 Risk management framework) |
| **Verktyg** |
| Julkri (HAL-06)<br>Cybermätaren (CRITICAL-2, RISK-3, RISK-4) |

## 1.2 Ett tillvägagångssätt som beaktar alla riskfaktorer

| **Exempel på genomförande** |
|---|
| • Som en del av aktörens förvaltningsstyrning och handlingsmodellen för riskhantering har aktören bedömt risker i kommunikationsnät och informationssystem och i deras fysiska miljö med ett tillvägagångssätt som beaktar alla riskfaktorer.<br>• Aktören har bedömt hur internt hot, externt hot eller fysiskt hot påverkar informations eller tjänsternas konfidentialitet, riktighet, autenticitet och tillgänglighet och beaktat dem i sin handlingsmodell för riskhantering. Andra sådana hot kan till exempel vara avbrott i telekommunikationen, elavbrott, stöld, skadegörelse, brand, svåra väderförhållanden, naturkatastrofer och katastrofer. |

- Dessutom kan man i bedömningarna beakta utvecklings- och underhållsåtgärdernas inverkan, till exempel avbrott som orsakas av applikations- och systemuppdateringar. Se punkt 3.
- Aktören har i riskbedömningen beaktat risker orsakade av andra parter, som till exempel byte av leverantörer och störningar i leveranskedjorna. Se punkterna 3.2 Säkerhet vid upphandling och 4.2 Riskhantering i leveranskedjan.
- Riskbedömningen innefattar också risker i anknytning till personalen och åtkomsthantering. Se punkterna 6 Personalsäkerhet och utbildning i cybersäkerhet samt 7 Förfaranden för åtkomsthantering och autentisering.
- I punkt 12 preciseras åtgärder för att säkerställa den fysiska miljön, lokalsäkerheten och nödvändiga resurser. Till exempel i fråga om den fysiska miljön kan man beakta hur eventuella byggarbeten påverkar kommunikationsnätens och informationssystemens funktion.

**Verifiering**

1. Tillsynsmyndigheten inspekterar att aktören har beaktat alla väsentliga riskfaktorer i sin handlingsmodell för hantering av cybersäkerhetsrisker och i sin riskbedömning. Av handlingsmodellen framgår att cybersäkerhetsrisker beaktas i företagets företagsstyrning och riskhanteringsprocesser. Av aktörens riskbedömning ska framgå att risker i kommunikationsnät och informationssystem är täckande och inbegriper bland annat fysiska, tekniska och personbaserade risker.

**Motiveringar**

Med ett tillvägagångssätt som beaktar alla riskfaktorer är avsikten att beakta alla skäligen förutsebara riskfaktorer i kommunikationsnät och informationssystem. Ju mer betydande kommunikationsnätet eller informationssystemet är för aktören i desto större omfattning ska hoten bedömas. Med detta tillvägagångssätt kan man främja aktörens beredskap för olika typer av hot och säkerställa till exempel att hot i anknytning till vissa kategorier inte bortses i alltför stor grad.

**Källor**

ISO/IEC 27001:2022 (6.1.1)

ISO/IEC 27005:2022 (7.2)

ISO 31000:2018 (6.3.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1)

IEC/TR 62443-3-1:2013 (4.2.3.7)

NIST CSF 1.1 (ID.RA-5)

NIST CSF 2.0 (ID.RA-05)

NIS CG Reference document (2.2 All Hazard approach)

| NIS CG Implementing guidance (2.1 Risk management framework) |
|---|
| **Verktyg** |
| Julkri (FYY-01)<br>Cybermätaren (CRITICAL-2, RISK-1, RISK-2) |

## 1.3 Identifiering av behov och funktioner

| **Exempel på genomförande** |
|---|
| • Aktören har identifierat funktioner som är centrala med tanke på tjänster, system, processer och personer samt inkluderat deras informationssäkerhetsbehov som en del av riskhanteringen. Denna punkt specificeras i punkt 5 Tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på säkerheten.<br>• Aktören har identifierat, dokumenterat och gjort en riskbedömning av kommunikationsnät och informationssystem inklusive enskilda enheter, tjänster eller informationssystem vars störningar skulle avbryta hela verksamheten (single point of failure, SPOF).<br>• Som stöd för bedömningen av riskens konsekvenser kan riskhanteringskriterier användas (se 1.1.1).<br>• Aktören har identifierat sin verksamhetsmiljö och de behov av informationssäkerhet som hänför sig till konfidentialiteten, riktigheten och tillgängligheten i fråga om uppgifter och tjänster. Se punkt 2.3 Val av säkerhetsförfaranden.<br>• Det rekommenderas att aktören har beskrivningar av den externa och interna verksamhetsmiljön som visar krav på riskhantering som utgår från väsentliga intressentgrupper och aktören själv. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har identifierat de mest kritiska tillgångarna för sin verksamhet (centrala tjänster, system, processer och personer) och inkluderat deras särdrag och behov i sin handlingsmodell för riskhantering när det gäller informationens och tjänstens konfidentialitet, riktighet och tillgänglighet. Identifierade kritiska funktioner och tillgångar och deras informationssäkerhetsbehov ska framgå av handlingsmodellen för riskhantering och tillgångshanteringen. |
| **Motiveringar** |
| Identifiering av kritiska behov och funktioner och hur de påverkas av risken hjälper vid valet av proportionerliga informationssäkerhetsåtgärder och i godkännandet av en kvarstående risk. |

| Källor |
|---|
| ISO/IEC 27001:2022 (4.1, 4.2, 6.2) |
| ISO/IEC 27002:2022 (5.9, 5.12) |
| ISO/IEC 27005:2022 (6.1, 6.2, 6.4, 7.2, 10.1) |
| ISO 31000:2018 (6.3.2) |
| IEC 62443-2-1:2010 (4.2.3.4, 4.2.3.6) |
| IEC 62443-2-1:2024 (ORG 1.1, ORG 2.4) |
| NIST CSF 1.1 (ID.RA-1) |
| NIST CSF 2.0 (ID.RA-01, GV.OC-02, GV.OC-03) |
| NIST SP 800-30 rev 1 (2.3, 3.1, 3.2) |
| NIST SP 800-37 rev 2 (2.3, 2.5, 3.2) |
| NIS CG Reference document (3.4.1 Asset classification) |
| NIS CG Implementing guidance (2.1 Risk management framework) |
| NIS CG Implementing guidance (12.1 Asset Classification) |
| **Verktyg** |
| Julkri (HAL-04) |
| Cybermätaren (CRITICAL-1, CRITICAL-2, ASSET-1, ASSET-2, THIRD-PARTIES-1, ARCHITECTURE-1) |

## 1.4 Identifiering av cyberhot

| Exempel på genomförande |
|---|
| • Som en del i hanteringen av cybersäkerhetsrisker har aktören följt upp de i punkt 1.3 identifierade hoten mot kommunikationsnät och informationssystem inklusive uppgifter om cyberhot och sårbarheter samt bedömt deras sannolikhet och konsekvens som en del av riskbedömningen. Aktören ska i sin hotanalys inkludera interna och externa hot, avsiktliga gärningar och skador.<br>• Aktören har bedömt cyberhotets sannolikhet och konsekvenser. I bedömningen av sannolikheten har man beaktat till exempel hur ofta hotet i fråga händer, om hotet har förekommit tidigare i organisationen och om motsvarande hot har förekommit inom sektorn. I bedömningen av sannolikheten är det också bra att inkludera en hotpotential, såsom angriparens vilja, motiv, förmåga och tillgången till automatiserade skadeprogram. |

- För att bedöma konsekvenser kan aktören ordna simuleringar och övningar med scenarier i olika fiktiva situationer om hot mot sin verksamhet för att bedöma den egna beredskapen och riskhanteringsförmågan.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören kan uppvisa dokumentation av identifierade cyberhot mot kommunikationsnät och informationssystem och att de har beaktats i hanteringen av cybersäkerhetsrisker. Av aktörens hotanalys framgår bedömning av hotens konsekvenser och sannolikhet.

**Motiveringar**

Identifiering av hot och en systematisk hotanalys ger möjlighet att identifiera de vanligaste hoten och sårbarheterna mot systemet, som utgör en risk för kommunikationsnätets eller informationssystemets tillförlitlighet, integritet och tillgänglighet. Genom hotanalysen samlar man in förståelse om hotets konsekvenser och sannolikheten för att eventuella sårbarheter utnyttjas.

**Källor**

ISO/IEC 27002:2022 (5.7)

ISO/IEC 27005:2022 (7.2, 7.3, 9.1)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, Annex B)

NIST CSF 1.1 (ID.RA-2, ID.RA-3)

NIST CSF 2.0 (ID.RA-02, ID.RA-03)

NIST SP 800-30 rev 1 (3.2, D, E, G)

NIS CG Implementing guidance (2.1 Risk management framework)

NIS CG Implementing guidance (2.2 Compliance monitoring)

**Verktyg**

Cybermätaren (THREAT-1, THREAT-2)

Cybersäkerhetscentrets lägesbildsprodukter, till exempel Cybersäkerhetscentrets veckoöversikt och cyberväder

Cyberövningar och simuleringar

### 1.4.1 Hotanalys – utökade anvisningar

**Exempel på genomförande**

Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.

- Utöver punkt 1.4 har aktören för hotanalysen samlat in uppgifter om hot och sårbarhet från flera olika källor samt analyserat cyberhotens sannolikhet och konsekvenser i den egna verksamheten. Aktören har i riskbedömningen inkluderat risker för kommunikationsnät och informationssystem som identifierats med hjälp av en hotanalys.
- Aktören har följt den senaste tekniska utvecklingen (state of the art) för funktioner som hänför sig till hotmiljön och cybersäkerheten samt utvecklat och upprätthållit egna kommunikationsnät och informationssystem i enlighet med riskbedömningen.
- Med hjälp av hotmodelleringen har man identifierat och dokumenterat kritisk information, gränssnitt, externa beroenden och informationsflöden i kommunikationsnät och informationssystem. Hotmodelleringen har kunnat göras med lämpliga hotmodelleringsmetoder, såsom STRIDE och DREAD.

## Verifiering

1. Tillsynsmyndigheten inspekterar hotanalyser gjorda av aktören. Av dem ska framgå att analysen baserar sig på en systematisk metod och är kontinuerlig, regelbunden och konsekvent. Hotanalysen har innefattat insamling och analys av hotinformation samt kartläggning och analys av den egna hotmiljön. Aktören kan använda en allmänt känd hotmodelleringsmetod såsom STRIDE eller DREAD för att identifiera hot mot systemet.
2. Tillsynsmyndigheten verifierar att hotanalysen är systematisk genom att intervjua personalen om tillvägagångssätt vid hotanalys. Genom intervjuerna kontrolleras att omfattningen av insamlingen av hotinformation, analysfrekvens, identifierade potentiella hot i den egna hotmiljön samt de åtgärder som man kommit överens om utifrån hotanalyserna är tillräckliga med hänsyn till aktörens behov.

## Motiveringar

Hotanalysen är ett verktyg för beredskapen. Med regelbunden hotanalys kan man upptäcka förändringar i hotmiljön och identifiera nya hot mot systemet. Hotbedömningen kan å andra sidan även utesluta hot vars möjliga konsekvens för verksamhetsmiljön är liten.

## Källor

ISO/IEC 27002:2022 (5.7)

ISO/IEC 27005:2022 (7.2, 7.3, 9.1)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1)

NIST CSF 1.1 (ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6)

| |
|---|
| NIST CSF 2.0 (ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, DE.AE-04, DE.AE-07) |
| NIST SP 800-30 rev 1 (3.2, D, E, G) |
| NIS CG Implementing guidance (2.1 Risk management framework) |
| NIS CG Implementing guidance (2.2 Compliance monitoring) |
| **Verktyg** |
| Cybermätaren (THREAT-1, THREAT-2, SITUATION-3) |
| Hotmodelleringsmetoder: STRIDE[5], DREAD[6] |

## 1.5 Riskhantering

| **Exempel på genomförande** |
|---|
| • Aktören har hanterat identifierade risker och på basis av riskspecifik betydelse. Riskhanteringen kan inbegripa olika sätt att reagera, till exempel att behålla risken, godkänna risken, minimera konsekvenserna, eliminering och att lägga ut på entreprenad. Aktören kan som stöd för riskhanteringen använda riskhanteringskriterier (se 1.1.1).<br>• Aktören har bestämt en ägare för risken som ansvarar för genomförandet av de beslutade riskhanteringsåtgärderna. Ägaren av risken kan vid behov bestämma vilken åtgärd som ska genomföras, följa upp genomförandet av hanteringsåtgärderna och åtgärdernas effektivitet.<br>• Aktören har identifierat och prioriterat lämpliga riskhanteringsåtgärder för cybersäkerhet genom att beakta resultaten av riskbedömningen och hanteringsåtgärdernas effektivitet. Aktören har enligt situationen även bedömt effektiviteten av riskhanteringsåtgärden och förändringen den medför för verksamheten samt vid behov genomföra en preciserande riskbedömning.<br>• Aktören har även dokumenterat åtgärder för riskhantering och tydligt motiverat orsakerna till en kvarstående risk.<br>• Aktörens högsta ledning eller riskägaren har godkänt riskbedömningens och riskhanteringens resultat och kvarstående risker.<br>• Det rekommenderas att regelbundet inspektera och kontrollera åtgärder för riskbedömning och riskhantering samt när det har gjorts betydande ändringar eller inträffat betydande incidenter.<br>• Riskhanteringsåtgärder är en del av verksamheten och personalen har utbildats. Detta preciseras i punkterna 2.2 Engagerande av personalen och 6 Personalsäkerhet och utbildning i cybersäkerhet. |

[5] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
[6] https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers

## Verifiering

1. Tillsynsmyndigheten verifierar hanteringen av cybersäkerhetsrisker genom att inspektera riskbedömningen. Aktören ska förevisa resultat av bedömning och hantering av cybersäkerhetsrisker. I dokumenten ska framgå riskbedömningens resultat, riskhantering och överenskomna hanteringsåtgärder samt eventuella roller och ansvar. Syftet med riskhanteringen har varit att hantera riskerna så att deras sannolikhet eller konsekvenser till exempel har minimerats, eliminerats eller lagts ut på entreprenad. Av dokumenten ska framgå även kvarstående risker, hantering av en kvarstående risk och motiveringar som hänför sig till godkännandet.

   För att få bevis på att riskhanteringen är regelbunden ska tillsynsmyndigheten verifiera händelseuppgifterna i anknytning till riskhanteringen. Tillsynsmyndigheten kan verifiera aktörens riskhanteringshistoria till exempel genom att följa upp antalet risker och deras effektivitet över en viss tidsperiod. Om förhindrande åtgärder speciellt har riktats mot centrala risker (key risk) kan antalet risker eller deras effektivitet minska med tiden. Om riskerna eller deras konsekvenser inte förändras ens under en lång tid är det bra att granska hur handlingsmodellen för riskhantering fungerar och om rätt kriterier används för att mäta riskerna.

## Motiveringar

Vid riskhantering bedöms förhållandet mellan riskhanteringsåtgärdernas effektivitet och en kvarstående risk: ska nivån på den kvarstående risken tolereras eller ska ytterligare lindrande åtgärder vidtas. Syftet med riskhantering är att genomföra en sådan kombination av riskhanteringsåtgärder som ger en tillfredsställande balans mellan kraven, kostnaderna och den kvarstående risken för säkerheten. Aktörens risktoleransförmåga och -vilja bestämmer en godtagbar nivå för den kvarstående risken.

## Källor

ISO/IEC 27001:2022 (6.1.3, 8.1, 8.2, 8.3, 9.3)

ISO/IEC 27005:2022 (8)

ISO 31000:2018 (6.5)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4, Annex B)

NIST CSF 1.1 (ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-2, ID.RM-3)

NIST CSF 2.0 (ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-2, GV.RM-3)

NIST SP 800-30 rev 1 (3.4, H)

NIST SP 800-37 rev 2 (3.3, 3.4, 3.5, 3.6)

NIS CG Reference document (3.3.1 Risk management framework)

| |
|---|
| NIS CG Implementing guidance (2.1 Risk management framework) |
| **Verktyg** |
| Julkri (HAL-06)<br>Cybermätaren (CRITICAL-2, RISK-3, RISK-4, RISK-5, WORKFORCE-4) |

## 1.6 Riskhanteringens ändamålsenlighet och indikatorer

| **Exempel på genomförande** |
|---|
| • Som en del av riskhanteringen har aktören bedömt effektiviteten hos riskhanteringsåtgärderna med lämpliga indikatorer och utvecklat indikatorerna när aktörens affärsverksamhet och verksamhetsmiljö förändras och utvecklas.<br>• Indikatorerna kan basera sig på affärsstrategins verksamhetsprincip och på de åtgärder och förfaranden som används i organisationen.<br>• I bedömningen av åtgärdernas effektivitet för riskhanteringen i kommunikationsnät och informationssystem har man även beaktat sektorsspecifika riktlinjer, regler, standarder och sektorsspecifik lagstiftning.<br>• Med hjälp av indikatorerna har aktören bedömt om de listade riskerna fortfarande är betydelsefulla, om riskens effekt eller sannolikhet fortfarande är på samma nivå och om de inriktade åtgärderna är uppdaterade. Vid bedömning av åtgärdernas effektivitet har man beaktat hot som riktats mot aktören och de förväntade konsekvenserna av dem, såsom de vanligaste följderna av hoten och vanliga konsekvenser av dem.<br>• Riskhanteringens effektivitet har bedömts regelbundet och i samband med betydande incidenter eller förändringar.<br>• Som ett resultat av bedömningen av riskhanteringens effektivitet och indikatorernas resultat har aktören anpassat riskhanteringsåtgärderna så att de motsvarar den förändrade situationen.<br>• Aktörens hantering av informationssäkerheten i kommunikationsnät och informationssystem och dess genomförande har inspekterats och bedömts på ett oberoende sätt. Aktören har skapat processer för oberoende inspektioner och ledningen ska planera och genomföra dem regelbundet.<br>• Personerna som utför inspektionen är oberoende av aktörens verksamhet och de har tillräcklig kompetens och erfarenhet för att utföra inspektionen. Inspektionen kan göras som självbedömning eller genom en tillhandahållare av informationssäkerhetstjänster.<br>• Resultatet av bedömningen har rapporterats till ledningen. Korrigerande åtgärder har genomförts och kvarstående risker har godkänts i enlighet med aktörens riskkriterier. |
| **Verifiering** |

1. Tillsynsmyndigheten inspekterar aktörens indikatorer. Indikatorerna ska vara lämpliga för utvärdering av riskhanteringsåtgärdernas effektivitet så att de valda åtgärdernas ändamålsenlighet kan mätas och vid behov förbättras. Av planerna ska framgå aktörens processer och planer för inspektionerna. Aktören kan uppvisa rapporter över inspektionerna och utvärderingarna.
2. Tillsynsmyndigheten intervjuar aktörens anställda och utvärderar hur indikatorerna används och fungerar i praktiken. Indikatorerna ska vid behov fungera som ledningens verktyg i fråga om hantering av cybersäkerhetsrisker. Tillsynsmyndigheten intervjuar aktören om riskhanteringen. Av intervjuerna ska framgå hur riskhanteringsåtgärder inleds på basis av indikatorerna. Aktören kan också uppmanas att även uppvisa ett riskhanteringsdokument av vilket ska framgå åtgärdshistoriken.

**Motiveringar**

Riskhanteringsåtgärder bör ge ett mervärde och därför ska de utvärderas regelbundet. En hotmiljö och teknik som ständigt utvecklas medför de största utmaningarna för att de valda åtgärderna ska hållas uppdaterade. Därför ska riskhantering och utvärdering av effektiviteten göras under riskens hela livscykel. Oberoende bedömare säkerställer riskhanteringens effektivitet och att den är uppdaterad.

**Källor**

ISO/IEC 27001:2022 (6.1.1, 6.1.3, 6.2, 9.1, 9.2, 9.3, 10.1)

ISO/IEC 27002:2022 (5.31, 5.35, 5.36, 8.34)

ISO/IEC 27005:2022 (8.3, 8.6, 9.2, 10.1, 10.5 10.6, 10.8)

ISO 31000:2018 (6.6)

IEC 62443-2-1:2010 (4.4.2.3, 4.4.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4, Annex B)

IEC 62443-3-3:2013 (SR 3.9)

NIST CSF 1.1 (ID.RM-1)

NIST CSF 2.0 (ID.IM-01)

NIST SP 800-30 rev 1 (3.4)

NIST SP 800-37 rev 2 (3.6, 3.7)

NIS CG Reference document (3.3.2 Policies and procedures to assess the effectiveness of security measures)

NIS CG Reference document (3.3.4 Independent review of information and network security)

NIS CG Implementing guidance (2.2 Compliance monitoring)

| |
|---|
| NIS CG Implementing guidance (2.3 Independent review of information and network security)<br><br>NIS CG Implementing guidance (7. Policies and procedures to assess the effectiveness of security measures) |
| **Verktyg** |
| Cybermätaren (CRITICAL-2, RISK-4, RISK-5, PROGRAM-2) |

1.6.1 Riskhanteringens effektivitet och indikatorer – utökade anvisningar

| **Exempel på genomförande** |
|---|
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br><br>• Utöver punkt 1.6 har aktören utarbetat riktlinjer för att bedöma effekterna av riskhanteringsåtgärderna inom cybersäkerheten.<br>• Aktören har tagit i bruk ett rapporteringssystem för att följa upp genomförandet av åtgärderna för riskhantering inom cybersäkerheten enligt NIS 2-direktivet och deras effektivitet. Rapporteringssystemet har utarbetats så att det lämpar sig för aktörens storlek och organisationsstruktur, verksamhetsmiljö och hotmiljö.<br>• För att få indikatorer på riskhanteringsåtgärdernas effektivitet har aktören kunnat fastställa till exempel följande:<br>  ○ riskhanteringsåtgärder som ska följas upp och mätas och målen för dem på högre nivå<br>  ○ processer och metoder för tillsyn<br>  ○ när uppföljning och mätning ska utföras<br>  ○ vem övervakar och mäter<br>  ○ när resultateten av uppföljning och mätning ska analyseras och utvärderas samt<br>  ○ vem som analyserar och utvärderar resultaten.<br>• Aktören har inkluderat informationssäkerhetsrevisioner i förfaranden för riskhanteringens effektivitet samt informationssäkerhetstest av datanätverk och informationssystem.<br>• Aktören har bedömt hur handlingsmodellen för riskhantering verkställs i organisationen. |
| **Verifiering** |

1. Tillsynsmyndigheten inspekterar aktörens riktlinjer och för bedömningen av effektiviteten av riskhanteringsåtgärderna för rapporteringssystemets cybersäkerhet. Av rapporteringssystemet ska framgå den riskhanteringsplan som organisationen genomför och möjliga ansvarspersoner. Här kan också framgå hur riskhanteringsåtgärderna för cybersäkerhet verkställs, deras effektivitet och att de är uppdaterade.

**Motiveringar**

Rapporteringssystemet kan hjälpa aktören att följa upp att riskhanteringsåtgärderna för cybersäkerhet i NIS 2-direktivet verkställs i organisationen.

**Källor**

ISO/IEC 27001:2022 (6.1.1, 6.2, 9.1, 9.2)

ISO/IEC 27002:2022 (5.31, 5.35, 5.36)

ISO/IEC 27005:2022 (8.3, 8.6, 9.2, 10.1, 10.5 10.6, 10.8)

IEC 62443-2-1:2010 (4.4.2.3, 4.4.4)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4)

IEC/TR 62443-3-1:2013

NIST CSF 1.1 (PR.IP-8)

NIST CSF 2.0 (ID.IM-03)

NIS CG Reference document (3.3.2 Policies and procedures to assess the effectiveness of security measures)

NIS CG Reference document (3.3.3 Compliance monitoring)

NIS CG Implementing guidance (2.2 Compliance monitoring)

NIS CG Implementing guidance (7. Policies and procedures to assess the effectiveness of security measures)

**Verktyg**

Cybermätaren (CRITICAL-2, RISK-4, RISK-5, PROGRAM-1, PROGRAM-2)

# 2 Riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem

Rekommendationerna grundar sig på artikel 21.2 a i NIS 2-direktivet. Om nationellt genomförande av denna föreskrivs i 9 § 2 mom. 2 punkten i cybersäkerhetslagen och 18 c § 1 mom. 2 punkten i informationshanteringslagen.

1. **Riktlinjer och förfaranden som gäller säkerheten**: Dessa kan gälla administrativ säkerhet, personal-, maskinvaru-, programvaru-, kommunikationsnäts- och datamaterialsäkerhet samt operativ säkerhet och säkerhet för den fysiska miljön. I standarden ISO 27001 används termen ”informationssäkerhetspolicy” för motsvarande riktlinjer. Aktören bör till exempel ha skriftliga riktlinjer och förfaranden för säkerheten i kommunikationsnät och informationssystem. Om sådana finns ska dessa stå i rätt proportion till aktörens behov och de ska vara uppdaterade. (Se punkt 2.1 och 2.1.1).

2. **Personalengagemang:** Dessutom kan man i riskhanteringen sträva efter att aktörens personal bör känna till de säkerhetsförfaranden som används och förbinda sig att iaktta dem. (Se punkt 2.2).

3. **Val av säkerhetsförfaranden:** Vid valet av lämpliga förfaranden kan de affärsmässiga behoven och identifierade cybersäkerhetsriskerna beaktas. (Se punkt 2.3).

## 2.1 Riktlinjer och förfaranden som gäller säkerheten

| **Exempel på genomförande** |
|---|
| • Aktören har utarbetat skriftliga riktlinjer och förfaranden för säkerheten i kommunikationsnät och informationssystem. I standarder används ibland termen informationssäkerhetspolicy för dessa. Aktörens högsta ledning har godkänt riktlinjerna och förfarandena som gäller säkerheten samt övervakar att dessa förverkligas.<br>• Av riktlinjer och förfaranden som gäller säkerheten framgår målen för säkerheten i kommunikationsnät och informationssystem, aktörens åtagande att uppfylla de krav som tillämpas på informationssäkerhet och åtagande att kontinuerligt förbättra riktlinjer och förfaranden.<br>• Riktlinjer och förfaranden som gäller säkerheten förankras hos personalen och eventuellt också tredje parter, såsom underleverantörer, leverantörer och tjänsteleverantörer (se 2.2).<br>• Aktören kan använda allmänt vedertagna standarder, referensramar för cybersäkerheten eller bästa praxis inom sektorn för informationssäkerhetspolicyn som stöd för utarbetandet av riktlinjer och metoder som gäller säkerheten.<br>• Riktlinjer och förfaranden för säkerheten kan gälla administrativ säkerhet, personal-, maskinvaru-, programvaru-, kommunikationsnäts- och datamaterialsäkerhet samt operativ säkerhet och säkerhet för den fysiska miljön. |

- Aktören har i riktlinjerna som gäller säkerhet i kommunikationsnät och informationssystem i tillämpliga delar inkluderat cybersäkerhetsåtgärder som hänför sig till NIS 2-direktivet, såsom åtkomsthantering, tillgångsförvaltning, konfiguration av terminalutrustning, nätverkssäkerhet, säkerhetskopiering, kryptering, hantering av störningssituationer, hantering av sårbarheter och den fysiska miljöns säkerhet.
- Som en del av riktlinjer och förfaranden för säkerheten har aktören angett roller, ansvar och befogenheter i anknytning till säkerheten (se 6.1).
- I valet av riktlinjer och förfaranden som gäller säkerheten har aktören beaktat affärsmässiga behov och identifierade cybersäkerhetsrisker. Riktlinjer och förfaranden lämpar sig för aktörens användning och står i rätt proportion i förhållande till risken i verksamheten.
- Riktlinjer och förfaranden som gäller säkerheten i kommunikationsnät och informationssystem har hållits uppdaterade genom regelbundna inspektioner. Regelbundna inspektioner har hållits vid på förhand bestämda tidpunkter (till exempel en gång om året) och när betydande ändringar har gjorts eller betydande incidenter har inträffat.
- Lämpligheten för riktlinjer och förfaranden har bedömts vid inspektionerna och har anpassats för att motsvara aktörens behov. Aktören kan också ha beaktat en förändring i verksamhetsmiljön och hotmiljön samt en utveckling av informationssäkerhetsfunktioner.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören kan uppvisa dokumentation för riktlinjer och förfaranden som gäller säkerheten i kommunikationsnät och informationssystem. Riktlinjer och förfaranden som gäller säkerheten är tillräckligt täckande och delområden som är lämpliga för aktörens verksamhet har inkluderats. Av dokumenten framgår tydligt målen, principerna och genomförandet av aktörens informationssäkerhet.

   För att kontrollera att riktlinjer och förfaranden står i rätt proportion ska det av dokumenten framgå att riktlinjerna är kopplade till affärsverksamheten och till aktörens verkställda riskhantering av cybersäkerhet.

   Riktlinjer och förfaranden är uppdaterade och har upprätthållits. Detta kan verifieras genom att kontrollera dokumentens uppdateringshistorik. Av uppdateringshistoriken framgår att dokumenten har granskats regelbundet och uppdaterats vid behov och vid betydande förändringar eller incidenter. Aktören kan uppvisa planer och dokumentation över inspektioner av riktlinjer och förfaranden.
2. Tillsynsmyndigheten bedömer om riktlinjer och förfaranden gällande aktörens säkerhet står i rätt proportion och är uppdaterade genom att intervjua personalen om hur medvetna de är om de utarbetade riktlinjerna och förfarandena samt hur de verkställs och iakttas i praktiken.

**Motiveringar**

| |
|---|
| Riktlinjer och förfaranden som gäller säkerheten utgör grunden för organisationens informationssäkerhetskultur och hanteringen av säkerheten i kommunikationsnät och informationssystem, inbegripet människor, processer och teknologier eller tekniker. Riktlinjer och förfaranden som står i rätt proportion stöder arbetet i vardagen och gör det möjligt att uppnå organisationens säkerhetsmål. |
| **Källor** |
| ISO/IEC 27001:2022 (4.1, 4.2, 5.2, 5.3)<br>ISO/IEC 27002:2022 (5.1, 5.36)<br>IEC 62443-2-1:2010 (4.3.2.2.1, 4.3.2.2.2, 4.3.2.6)<br>IEC 62443-2-1:2024 (ORG 1.1, ORG 1.3, ORG 1.6, ORG 2.4)<br>IEC 62443-2-4:2015 (SP 01)<br>IEC 62443-2-4:2024 (SP.01.05, SP.01.06, SP.01.07, SP.03.01)<br>NIST SP 800-53 Rev. 5<br>NIST CSF 1.1 (ID.GV-1, ID.GV-3, ID.BE-3)<br>NIST CSF 2.0 (GV.OC-01, GV.OC-03, GV.PO-01, GV.PO-02)<br>NIS CG Reference document (3.2.1 Network and information security policy)<br>NIS CG Implementing guidance (1.1 Policy on the security of network and information systems) |
| **Verktyg** |
| Julkri (HAL-01)<br>Cybermätaren (CRITICAL-2, PROGRAM-1 PROGRAM-2, Allmänna förvaltningsåtgärder) |

### 2.1.1 Riktlinjer och förfaranden som gäller säkerheten – utökade anvisningar

| |
|---|
| **Exempel på genomförande** |
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br>• Utöver punkt 2.1 har aktören vid behov utarbetat separata riktlinjer (policy) per delområde. Riktlinjer har kunnat utarbetas till exempel för hantering av sårbarheter, säkerhet i leveranskedjorna, säkerhetstestning, bedömning av |

| |
|---|
| effekterna av riskhanteringsåtgärderna, kryptering, åtkomsthantering, användning av huvudanvändarnamn och förhöjda rättigheter, hantering av information och tillgångar samt användning av externa lagringsmedier.<br>• Som en del av riktlinjer och förfaranden som gäller säkerhet har aktören kunnat utarbeta specifikare förfaranden och anvisningar för olika delområden såsom åtkomsthantering, tillgångsförvaltning, säker konfiguration av terminalutrustning, nätverkssäkerhet, säkerhetskopiering, kryptering, hantering av störningssituationer, hantering av sårbarheter och säkerheten i den fysiska miljön.<br>• Behovet av specifikare förfaranden och anvisningar kan till exempel bero på delområdets storlek eller uppdateringsbehovets frekvens. Aktören kan till exempel som en del av tillgångsförvaltningen ha behov att utfärda instruktioner för kritiska tillgångar i fråga om säker överföring av enheter, programvara och information till externa lokaler. |
| **Verifiering** |
| 1. Tillsynsmyndigheten inspekterar av aktören utarbetade branschspecifika riktlinjer och preciserande anvisningar om säkerheten. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (5.1, 5.37)<br>IEC 62443-2-1:2024 (ORG 1.1, ORG 1.3, ORG 1.6, ORG 2.4)<br>NIST CSF 1.1 (ID.GV-4)<br>NIST CSF 2.0 (GV.OC-4)<br>NIS CG Implementing guidance (1.1 Policy on the security of network and information systems) |
| **Verktyg** |
| Cybermätaren (CRITICAL-2, PROGRAM-1, Allmänna förvaltningsåtgärder) |

## 2.2 Engagerande av personalen:

| |
|---|
| **Exempel på genomförande** |
| • Aktörens ledning har sett till att hela personalen och möjliga tredje parter följer riktlinjer och förfarande som gäller säkerheten i kommunikationsnät och |

informationssystem (se 2.1) samt andra olika förfaranden och närmare anvisningar som utarbetats för olika delområden (se 2.1.1).

- Aktören har regelbundet informerat personalen och tredje parter om riktlinjer och förfaranden som gäller säkerheten.
- Riktlinjer och förfaranden som gäller säkerheten har inkluderats i utbildningar som aktören ordnar. Närmare information om utbildning finns i punkt 6.5 Personalutbildning och 11.1 Grundläggande praxis för informationssäkerhet.
- Aktören har handlingsmodeller för eventuell verksamhet som strider mot riktlinjerna och förfarandena för säkerheten. Denna punkt specificeras i punkt 6.1 Personalens säkerhet.

**Verifiering**

1. Tillsynsmyndigheten inspekterar praxisen för att informera eller utbilda personalen om riktlinjer och förfaranden i anknytning till säkerheten. Det kan till exempel vara en webbplats, utbildningsmaterial eller annat motsvarande som hela personalen har tillgång till. Tillsynsmyndigheten kan också kontrollera aktörens handlingsmodell för att engagera personalen i att iaktta riktlinjerna för cybersäkerhet. Detta kan till exempel vara uppföljning av utbildning som gäller riktlinjerna för säkerheten.
2. Tillsynsmyndigheten verifierar genom intervjuer att personalen är förtrogen med riktlinjer och förfaranden som gäller säkerheten. Av intervjuerna framgår personalens funktion i enlighet med gemensamma riktlinjer och förfaranden. Personalen vet var skriftligt material finns.

**Motiveringar**

Tillägnandet av riktlinjer och förfaranden som gäller säkerheten är beroende av en kompetent personal. Med hjälp av utbildning förstår varje anställd betydelsen av sin uppgift som en del av den övergripande säkerheten i organisationen.

**Källor**

ISO/IEC 27001:2022 (5.2, 7.3, 7.4)

ISO/IEC 27002:2022 (5.4, 6.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 1.4, ORG 1.5, ORG 1.6)

NIST CSF 1.1 (ID.GV-2, ID.AM-6, DE.DP-1, PR.AT-5)

NIST CSF 2.0 (GV.RR-02, PR.AT-02)

NIS CG Reference document (3.2.2 Roles, responsibilities and authorities)

NIS CG Implementing guidance (1.2 Roles, responsibilities and authorities)

**Verktyg**

| |
|---|
| Julkri (HAL-02, HAL-03, HAL-12, HAL-13)<br><br>Cybermätaren (CRITICAL-2, WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, WORKFORCE-4, Allmänna förvaltningsåtgärder) |

## 2.3 Val av säkerhetsförfaranden

| **Exempel på genomförande** |
|---|
| • Aktören har i valet av förfaranden i anknytning till kommunikationsnät och informationssystem beaktat aktörens affärsmässiga behov och identifierade cybersäkerhetsrisker (se 2.1). Affärsverksamhetens behov har omfattat till exempel kraven från centrala intressentgrupper, sektorns reglering och aktörens standarder och certifikat.<br>• Säkerhetsförfarandena har valts på basis av identifierade säkerhetsbehov. För att välja säkerhetsförfaranden som står i rätt proportion har aktören gjort en förteckning över sina tillgångar, gjort en riskbedömning och klassificerat tillgångarna i enlighet med informationssäkerhetsbehovet (till exempel konfidentialitet, integritet, äkthet och tillgänglighet). Vid behov har aktören även kunnat inkludera äkthet, ostridighet och autentisering. Tillgångsförteckningen och tillgångsklassificeringen preciseras i punkt 5.2.<br>• Aktören har uppdaterat och utvecklat säkerhetsförfarandena regelbundet och i samband med betydande ändringar, såsom när verksamhetsmiljön eller hotmiljön förändras eller när det inträffat incidenter. |
| **Verifiering** |
| 1. Tillsynsmyndigheten inspekterar dokumenterade riktlinjer och förfaranden som gäller säkerheten. I dokumenten har angetts bland annat krav som uppkommer av reglering i aktörens affärsverksamhet eller reglering i fråga om sektorn. Av valet av förfaranden som gäller säkerheten framgår affärsverksamhetens behov, standarder och certifieringar som är en del av ledningssystemet, sektorns reglering och centrala intressentgruppers behov. Av valet av förfaranden framgår också identifierade cybersäkerhetsrisker och de har en tydlig koppling till riskbedömningen, valet av riskhanteringsåtgärder, deras effektivitet och indikatorer samt tillgångsförvaltningen och dess förteckning och klassificering. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (5.12, 5.36) |

| |
|---|
| IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1) |
| NIST CSF 1.1 (ID.GV-1, ID.GV-3, ID.GV-4) |
| NIST CSF 2.0 (GV.OC-01, GV.PO-01) |
| NIS CG Reference document (3.2.1 Network and information security policy) |
| NIS CG Implementing guidance (1.1 Policy on the security of network and information systems) |
| **Verktyg** |
| Julkri (HAL-05) |
| Cybermätaren (ASSET-1, ASSET-2, PROGRAM-1, PROGRAM-2, ARCHITECTURE-1) |

# 3 Säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter

Rekommendationerna grundar sig på artikel 21.2 e i NIS 2-direktivet. Om nationellt genomförande av denna föreskrivs i 9 § 2 mom. 3 punkten i cybersäkerhetslagen och 18 c § 1 mom. 3 punkten i informationshanteringslagen.

1. **Skydd av kommunikationsnät och informationssystem under hela livscykeln:** Aktören ska sträva efter att upprätthålla en tillräcklig säkerhetsnivå i kommunikationsnät och informationssystem under hela deras livscykel. (Se punkt 3.1 och 3.1.1).

2. **Säkerheten hos föremålet för förvärvet:** Till exempel ska upphandlade system vara tillräckligt säkra, med hänsyn till verksamhetens behov, bland annat i fråga om integritet, tillgänglighet och konfidentialitet. Vid upphandling av system kan man till exempel fästa uppmärksamhet vid deras förmåga att avvärja de vanligaste attackerna. (Se punkt 3.2).

3. **Systemhärdningar:** En säker konfiguration av systemen, dvs. inställningarna, kan definieras, dokumenteras och upprätthållas under hela livscykeln, och detta kan särskilt beaktas vid uppdateringar. (Se punkt 3.3 och 3.3.1).

4. **Hantering av ändringar och uppdateringar**: I fråga om konfigurations- och programuppdateringar kan man exempelvis sträva efter att de dokumenteras, är utformade i enlighet med ändringshanteringsprocesserna och detaljerade samt att de görs i rätt tid med tanke på objektets särdrag och uppdateringarnas kritiska natur. Otillåtna eller skadliga ändringar kan till exempel förhindras. (Se punkt 3.4 och 3.4.1).

5. **Testning av säkerheten**: De objekt som är mest kritiska med tanke på säkerheten kan identifieras separat och deras säkerhet tryggas till exempel genom regelbundna inspektioner av processer eller genom tekniska tester. (Se punkt 3.5).

6. **Hantering av sårbarheter och delgivning av information om sårbarheter:** Aktören kan till exempel se till att det för upptäckta sårbarheter finns en rapporteringskanal samt på förhand fastställda förfaranden och praxis för behandling av anmälningar. (Se punkt 3.6).

7. **Säkerheten i tjänster som tillhandahålls:** Aktören kan till exempel säkerställa att det över huvud taget är möjligt att på ett säkert sätt konfigurera dessa kommunikationsnät och informationssystem och att det produceras lämpliga säkerhetsuppdateringar för dem. (Se punkt 3.7).

8. **Strukturell säkerhet i kommunikationsnäten:** När det gäller kommunikationsnät ska aktören se till att dess struktur är säker. Till exempel objekt som är kritiska för funktionerna ska identifieras och vid behov skyddas genom uppdaterade tekniska metoder, såsom genom zonindelning. (Se punkt 3.8).

9. **Skydd mot skadlig trafik**: Eventuell skadlig trafik ska kunna upptäckas och förhindras. (Se punkt 3.9).

## 3.1 Skydd av kommunikationsnät och informationssystem under hela livscykeln

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkt 11.3 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har förfaranden för att skydda kommunikationsnät och informationssystem under hela deras livscykel. I livscykeltänkande ska man beakta planering, ibruktagande, drift och avveckling. Egendomens livscykel preciseras i punkt 5.3 Användning av tillgångsförteckningen. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar dokumentationen genom inspektion att aktören skyddar sina kommunikationsnät och informationssystem. Av dokumentationen framgår hur de skyddas under hela deras livscykel. När det gäller livscykeln har man beaktat planering, ibruktagande, drift och avveckling. Att skyddet har tagits i bruk kan verifieras till exempel genom att använda tillgångskatalogen och ändringar som hänför sig till den samt annat bevis som aktören lämnat in, såsom skärmdumpar samt intervjuer. Skyddsåtgärder som ska granskas är bland annat punkterna 3.3 Systemhärdningar, 3.4 Hantering av ändringar och uppdateringar, 3.8 Strukturell säkerhet i kommunikationsnäten samt 11 Grundläggande praxis för informationssäkerhet i tillämpliga delar.<br>2. Genom att granska konfigurationer och lägesinformation som aktören lämnat in (till exempel DNS, DHCP-logguppgifter och dokumentering, övriga enhetsbestånd, konfigurationshantering eller versionering av nätverksutrustning) och jämföra dem med dokumentationen kan tillsynsmyndigheten verifiera att förfarandena har verkställts. Av uppgifterna ska framgå att det till exempel inte finns avvecklade enheter eller enheter i miljön vars process för ibruktagande inte har genomförts utan grundad anledning. Särskild uppmärksamhet ska fästas vid enheter som nödvändigtvis inte direkt är synliga i kommunikationsnätets och informationssystemets uppgifter. Sådana kan vanligen till exempel vara virtuella datorer i molntjänster och tjänster, såsom gränssnitt som kanske ska kontrolleras i användargränssnitten för tjänsten i fråga. Om aktören använder molntjänster eller andra virtuella plattformar ska inspektionen även omfatta dessa. |

| |
|---|
| 3. Tillsynsmyndigheten kan utvidga den föregående inspektionen med skanningar eller datainspelningar. |
| **Motiveringar** |
| En försämring av säkerheten med tiden kan medföra sårbarheter som inte identifieras. Det är vanligt att en enhet, virtuella datorer och applikationer inte avvecklas när användningsbehovet har upphört. I allmänhet orsakar objekt som inte underhålls ofta allvarliga sårbarheter. |
| **Källor** |
| IEC 62443-2-1:2024 (NET 1.1, NET 1.2, COMP 1.1, CM 1.1, CM 1.3, CM 1.4, ORG 2.3)<br>NIST CSF 1.1 (PR.AC-5, PR.DS-3)<br>NIST CSF 2.0 (PR.IR-01)<br>NIST SP 800-30 rev 1 (F)<br>NIST SP 800-37 rev 2<br>NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products) |
| **Verktyg** |
| Julkri (HAL-05.1, TEK-17.2)<br>Cybermätaren (ASSET-1, ASSET-2, ASSET-3, ASSET-4) |

### 3.1.1 Säker produktutveckling – utvidgade anvisningar

| |
|---|
| **Exempel på genomförande** |
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br>• Aktören har producerat applikationer och system i enlighet med säker utvecklingspraxis, till exempel med hjälp av praxis som fastställts av SDLC (secure/software development life cycle) eller SSDLC (secure software development life cycle). Praxisen gäller alla faser i utvecklingscykeln (definition, planering, utveckling, genomförande, testning, ibruktagande och underhåll).<br>• Cybersäkerhetskraven har analyserats i definitions- och planeringsskedena.<br>• Åtgärder för säker produktutveckling har fastställts. Detta omfattar till exempel säkra arkitekturval (till exempel zero-trust), säker programmeringspraxis, användning av säkra leveranskedjor, val av säkra komponenter. |

- Aktören har fastställt säkerhetskraven för utvecklingsmiljön.
- Säkerhetstestningsprocesserna har definierats och tagits i bruk. I säkerhetstestningen kan man till exempel utnyttja den automatiska arbetsgången (DevSecOps), som innehåller olika säkerhetstest, såsom statisk och dynamisk säkerhetstestning (static application security testing SAST, dynamic application security testing DAST), inspektionspraxis (review), säkerhetsskanning och intrångstestning (penetration testing).
- Säkerhetskraven för de data som används i testningen har beaktats i verksamheten. Eventuella konfidentiella data är skyddade på minst motsvarande sätt som i produktionssystemen eller så har de sanerats, anonymiserats eller pseudonymiserats.

**Verifiering**

1. Tillsynsmyndigheten inspekterar aktörens dokumentation om hur aktören genomför säker produktutveckling. Åtgärderna för säker produktutveckling beror i hög grad på produktens egenskaper och verifieringen ställs i relation till dessa egenskaper. I produktutvecklingen utnyttjas ofta allmänt kända goda funktionssätt, såsom SDLC eller SSDLC. Av dokumentationen framgår hur aktören försäkrar sig om de levererade produkternas informationssäkerhet till exempel i definitions-, planerings-, utvecklings-, genomförande- och testningsskedena.
2. Tillsynsmyndigheten verifierar utvecklingspraxisen till exempel genom att inspektera aktörens utvecklingsinfrastruktur. Utvecklingsinfrastrukturen innehåller i allmänhet olika plattformar för till exempel utveckling, testning, kvalitetssäkring och förproduktion. Under utvecklingen är det dessutom vanligt med säkerhetstest på produkten. Eventuella källkoder och konfigurationer har skapats på ett säkert sätt till exempel så att importen av externa bibliotek sker enligt fastställda funktionssätt, att man vid skapandet av källkoden har använt funktionssätt med vilka ändringar endast kan göras av identifierade och auktoriserade användare. Om utvecklingen också omfattar utrustningen är det skäl att inspektera leveranskedjorna i anslutning till detta och även testa utrustningens säkerhet.

**Motiveringar**

Testning av produkten är ett sätt att säkerställa att produkten är så säker som möjligt. På så sätt levereras inte svaga genomföranden vidare och de produkter som levereras är kompatibla med cybersäkerhetslagen. Testning är också ett sätt att hitta sårbarheter före angripare. Dessutom kan en omfattande testning och behandling av testresultaten ge en realistisk bild av säkerheten och synliggöra eventuella svagheter, varvid man kan förbereda sig på dem med kompenserande åtgärder.

**Källor**

ISO/IEC 27002:2022 (8.25, 8.28, 8.31)

| |
|---|
| IEC 62443-2-1:2010 (4.3.4.3) |
| IEC 62443-2-1:2024 (ORG 2.3) |
| IEC 62443-4-1:2018 |
| NIST CSF 1.1 (PR.IP-2) |
| NIST CSF 2.0 (ID.AM-08) |
| OWASP Application Security Verification Standard |
| OWASP Top Ten |
| NIS CG Reference document (3.9.7 Secure development life cycle) |
| NIS CG Implementing guidance (6.2. Secure development life cycle) |
| **Verktyg** |
| Julkri (TEK-14) |
| Cybermätaren (ARCHITECTURE-4, THIRD-PARTIES-2) |

## 3.2 Säkerheten hos föremålet för upphandlingen

| **Exempel på genomförande** |
|---|
| • Aktören ska försäkra sig om att de tjänster, system, produkter och resurser som upphandlas av en tredje part på basis av verksamhetens behov är tillräckligt säkra bland annat i fråga om integritet, tillgänglighet och konfidentialitet och att de har förmåga att avvärja de vanligaste attackerna.<br>• Aktören ska säkerställa att en produkt eller tjänst kan konfigureras säkert och att det finns informationssäkerhetsuppdateringar för föremålet under hela den planerade livscykeln och att uppdateringar är väsentliga för föremålet.<br>• Om föremålet för upphandlingen till exempel är en tjänst eller resurs ska man se till föremålets säkerhet, kvalitet och tillgänglighet under hela livscykeln. Man ska i synnerhet förbereda sig på eventuella ändringar när det gäller tjänsteleverantören, så att tjänsten eller resursen vid behov kan överföras eller återställas i egen besittning. Vid behov ska man också förbereda sig för ändringar i ägarförhållanden.<br>• Man kan försöka säkerställa säkerheten hos upphandlingen till exempel med avtal, genom att undersöka produktens egenskaper, genom att till exempel förutsätta certifieringar, genom att försäkra sig om leverantörens tillförlitlighet och ha beredskap för risker. Säkerhetskraven ska bestämmas redan i det inledande skedet av upphandlingen och kraven har tillställts leverantören och fogats till avtalet.<br>• Aktören har försäkrat sig om att det finns dokumentation över det upphandlade föremålet som inbegriper dess innehåll, säker konfiguration och användning. |

- Säkerheten hos det upphandlade föremålet har säkerställts under hela livscykeln. Detta kan innefatta till exempel uppdateringar i avtalet, uppdateringar av underhåll och regelbundna säkerhetskontroller.
- Förutom upphandlingsprocessen kan man dessutom försäkra sig om anskaffningsföremålet med godkännandetestning (factory acceptance test, site acceptance test).
- Aktören har beaktat säkerhetsaspekterna även under upphandlingsprocessen. Mer om säker hantering av information i punkt 11.8.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har praxis för att försäkra sig om säkerheten hos upphandlade föremål (se ovan nämnda genomförandeexempel). Man ska försäkra sig om säkerheten hos föremålen för upphandlingen när det gäller föremål med svagheter i informationssäkerheten som kan medföra risker för aktörens verksamhet. Att försäkra sig om säkerheten hos upphandlingsföremålet kräver i allmänhet en omfattande upphandlingsprocess där alla säkerhetsaspekter beaktas. Aktören har försäkrat sig om att en säker konfiguration av föremålen som upphandlas är möjlig och att det produceras säkerhetsuppdateringar för föremålen under tillräckligt lång tid. Föremålen för upphandlingen ska dessutom ha en förmåga att avvärja åtminstone de vanligaste attackerna.

   Säkerheten hos föremålen för upphandlingen kan man ta upp till exempel genom upphandlingsprocessen. Föremålet som anskaffas kan till exempel vara en enhet, tjänst eller resurs. Ett typiskt sätt att försäkra sig om säkerheten kan till exempel vara olika testnings- och undersökningsmetoder i samband med upphandlingarna, åtgärder i anknytning till föremålets livscykel samt beredskap för olika hot och förändringar i hotmiljön genom säkerhetsavtal. Man ska alltså försäkra sig om att aktörens upphandlingsprocess stöder säkerhetsbehoven och att upphandlingsprocessen iakttas och beaktas i riskbedömningen. Hur upphandlingsprocessen genomförs kan till exempel verifieras genom att bekanta sig med upphandlingsdokumenten, intervjuer och genom att undersöka de upphandlade föremålens nuläge. Vid upphandlingar ska man särskilt beakta aktörens specialbehov. Sådana kan till exempel vara geografiska krav, behov i anknytning till resurser och tjänstelöften, möjlighet att överföra tjänsterna, säkerhetsegenskaper hos produkter och tjänster samt uppdatering av tjänsterna och livscykel.

**Motiveringar**

Misslyckade upphandlingar kan förutom ekonomisk risk vara förenade med cybersäkerhetsrisker. Till exempel en produkt eller tjänst som inte är säker kan äventyra andra informationssystem och kommunikationsnät. Om upphandlingen inte har gjorts med tillräckliga arrangemang ökar sannolikheten för många hot, såsom beroende av enhetstillverkaren (vendor lock-in), hot som orsakas av ändringar i ägarförhållandena, förlust av kompetensen och föremålet för upphandlingen.

| Källor |
|---|
| ISO/IEC 27002:2022 (5.21, 5.23) |
| IEC 62443-2-1:2010 (4.3.4.3.1, 4.3.4.3.4) |
| IEC 62443-2-1:2024 (ORG 1.6, ORG 2.3) |
| IEC 62443-2-4:2015 |
| IEC 62443-3-3:2013 (SR 3.4, 3.5) |
| NIST CSF 1.1 (ID.SC-1, ID.SC-3, ID.SC-4) |
| NIST CSF 2.0 (GV.SC-01, GV.SC-05, GV.SC-07) |
| NIST SP 800-161 rev 1 (3.1) |
| NIS CG Reference document (3.9.6 Security in acquisition of ICT services, ICT systems or ICT products) |
| NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products) |
| **Verktyg** |
| Julkri (HAL-16, HAL-16.1) |
| CYBERMÄTAREN (THIRD-PARTIES-1, THIRD-PARTIES-2, ARCHITECTURE-3, ARCHITECTURE-4) |
| Informationshanteringsnämndens rekommendation om informationssäkerhet vid upphandling, målgrupp informationshanteringsenheter och myndigheter: http://urn.fi/URN:ISBN:978-952-367-647-3 |

## 3.3 Systemhärdningar

| Exempel på genomförande |
|---|
| Denna punkt kompletterar punkt 11.10 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har bestämt processer och verktyg för att skapa en säker konfiguration för enheter, applikationer, tjänster och kommunikationsnät som underhålls under hela livscykeln.<br>• Som en del av riskbedömningen har man bestämt minst de objekt vars drift är väsentlig med tanke på säkerhet, försörjningsberedskap eller andra riskhanteringsorsaker.<br>• För dessa objekt har man skapat en konfiguration som främjar föremålets informationssäkerhet. En säker konfiguration avser till exempel eliminering av |

tydligt riskfyllda egenskaper, avstängning eller eliminering av extra tjänster, komponenter och portar, byte av standardlösenord och att säkerhetsfunktioner tas i bruk.

- Om en säker konfiguration inte kan produceras för föremålet och det utgör en förhöjd säkerhetsrisk för kommunikationsnät eller informationssystem ska det vara skyddat med andra riskhanteringsmetoder.
- Säkerhetsparametrar i anknytning till konfigurationen, exempelvis lösenord, ska förvaras säkert och tillgängliga och vara lätta att ändra.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören fastställer, dokumenterar och underhåller en säker konfiguration av systemen. För kontroll av säker konfiguration kan man utnyttja befintlig dokumentation och konfigurationsfiler. Av dessa ska framgå att aktören tar bort extra inställningar, byter standardinställningar som inte är säkra och tar i bruk eventuella säkerhetsegenskaper. Tillsynsmyndigheten inspekterar dessutom aktörens konfigurationspraxis vid ändringar, exempelvis i anknytning till uppdateringar. Typiska saker som kan skärpas är till exempel att byta standardlösenord, borttagning av extra tjänster och egenskaper (till exempel extra hanteringsförbindelser), borttagning av extra enheter och komponenter, att byta kommunikationsprotokollen till säkra (till exempel okrypterad till krypterad), säkerhetsinställningar tas i bruk (till exempel brandvägg, skadeprogramskontroll, automatiska uppdateringar).
2. Tillsynsmyndigheten inspekterar tillvägagångssätt för härdning genom att med aktörens hjälp bekanta sig med konfigurationen av olika enheter, program och tjänster. Man kan be att få skärmdumpar av konfigurationerna och använda intervjuer. Om antalet objekt är stort lönar det sig att använda ett täckande urval som även inbegriper olika typer av objekt. Det lönar sig att välja de objekt som är mest betydande med tanke på verksamheten och säkerheten.

**Motiveringar**

**Källor**

ISO/IEC 27002:2022 (8.9, 8.20, 8.21)

IEC 62443-2-1:2024 (NET 1.1, ORG 1.1, CM 1.1, CM 1.2, CM 1.3, CM 1.4, COMP 1.1)

IEC 62443-2-4:2015 (SP 06.02)

IEC 62443-2-4:2024 (SP.03.02, SP.03.05, SP.03.08, SP.03.09, SP.06.03, SP.07.04, SP.08.02, SP.09.02 RE(4), SP.09.03, SP.09.04, SP.09.07, SP.09.09, SP.10.02)

IEC 62443-3-3:2013 (SR 7.6)

| |
|---|
| NIST CSF 1.1 (PR.IP-1, PR.IP-3) |
| NIST CSF 2.0 (ID.RA-07, PR.PS-01) |
| NIS CG Reference document (3.9.1 Configuration management) |
| NIS CG Implementing guidance (6.3. configuration management) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi |
| Julkri (TEK-10) |
| Cybermätaren: ASSET-1, ASSET-3, ASSET-4, ARCHITECTURE-3 |

3.3.1 Systemhärdningar i kommunikationsnät och informationssystem genomförs systematiskt och i stor omfattning – utökade anvisningar

| |
|---|
| **Exempel på genomförande** |
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br><br>• En säker konfiguration följer till exempel kända konfigurations- eller härdningsreferenser. Konfigurationerna har bestämts på ett täckande sätt för de olika föremålen i informationssystemet.<br>• Säkra konfigurationer har införts kontrollerat i systemen. Detta kan till exempel innebära ett centraliserat konfigurationshanteringssystem. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören vid behov har valt härdningsreferenser för härdningar av sina enheter och tjänster. Aktören har dessutom dokumenterat eventuella incidenter i dessa. Härdningsreferenser tillhandahålls till exempel av CIS, DISA och programvaruleverantörer. Ofta ska man avvika från referensgenomföranden på grund av egenskaper som används. Referensvalen och gjorda avvikelser kan vara skriftliga konfigurationer som kan inspekteras. Genomförandet av härdningar kan inspekteras till exempel genom att undersöka konfigurationen hos enheter, applikationer och tjänster. Om ett centraliserat konfigurationssystem används kan konfigurationer till objekten kontrolleras i det. I konfigurationshanteringssystemets loggar kan man kontrollera konfigurationssystemets funktion och omfattning. |
| **Motiveringar** |
| Härdningar är ett av de effektivaste sätten för att minska angreppsytan för en enskild applikation eller enhet. Redan enkla härdningar kan ge synliga resultat, men i verkligheten har i synnerhet stora produkter enorma mängder egenskaper |

som man kan ha nytta av att eliminera eller ändra konfigurationen för. Att utnyttja färdiga härdnings- och konfigurationsanvisningar för detta kan vara ändamålsenligt.

**Källor**

ISO/IEC 27002:2022 (8.9, 8.20, 8.21)

IEC 62443-2-1:2024 (NET 1.1, ORG 1.1, CM 1.1, CM 1.2, CM 1.3, CM 1.4)

IEC 62443-2-4:2015 (SP 06.02)

IEC 62443-2-4:2024 (SP.03.02, SP.03.05, SP.03.08, SP.03.09, SP.06.03, SP.07.04, SP.08.02, SP.09.02 RE(4), SP.09.03, SP.09.04, SP.09.07, SP.09.09, SP.10.02)

IEC 62443-3-3:2013 (SR 7.6)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (ID.RA-07, PR.PS-01, PR.PS-03)

NIS CG Reference document (3.9.1 Configuration management)

NIS CG Implementing guidance (6.3. configuration management)

**Verktyg**

CIS benchmark

DISA STIG

Kartläggning av angreppsytan Hyöky.fi

Julkri (TEK-10)

Cybermätaren (ASSET-3, ASSET-4, ARCHITECTURE-3)

## 3.4 Hantering av ändringar och uppdateringar

**Exempel på genomförande**

Denna punkt kompletterar punkt 11.9 om grundläggande praxis för informationssäkerhet.

- Aktören har dokumenterat förfarandet för hantering av ändringar och processen i anknytning till det. Processen för hantering av ändringar kan inbegripa till exempel en beskrivning av ändringens godkännande, hur snabbt ändringen ska göras för att säkerställa att den görs vid rätt tidpunkt och en beskrivning av ersättande åtgärder om ändringen inte kan verkställas.

- Ändringar, korrigeringar och underhåll i kommunikationsnät och informationssystem har genomförts i enlighet med förfarandet för hantering av ändringar. Förfarandet för hantering av ändringar grundar sig på aktörens riktlinjer för säkerheten.
- I förfarandet för hantering av ändringar har beskrivits tillvägagångssätt och skyldigheter i anknytning till genomförande av nödändringar, av vilka framgår till exempel dokumentationskrav och åtgärder för att trygga säkerheten.
- För ändringar som gjorts genom underhåll på distans har använts godkända förfaranden som förhindrar otillåtna ändringar.

**Verifiering**

1. Tillsynsmyndigheten verifierar aktörens dokumentation i fråga om hantering av ändringar. Aktören har en skriftlig beskrivning av hur till exempel konfigurations- och applikationsuppdateringar införs på ett täckande sätt i olika delar av systemet och vid rätt tidpunkt på basis av hur kritisk uppdateringen är och systemets egenskaper. Processen för hantering av ändringar ska innehålla en beskrivning av till exempel hur eventuella ändringar godkänns, hur de i efterhand kan spåras och hur snabbt ändringen ska införas i målsystemen. Eventuella ersättande åtgärder ska också beskrivas om en ändring inte kan verkställas. Hanteringen av ändringar kan vara genomförd på ett enkelt sätt utifrån riskhanteringen, och även beroende av storleken på aktörens kommunikationsnät och informationssystem. Vid behov finns även en beskrivning av hanteringen av ändringar om hur man säkerställer att ändringarna fungerar och deras säkerhet, i synnerhet om systemet har speciellt höga tillgänglighets- och konfidentialitetskrav. I hanteringen av ändringar ska man även beskriva handlingssätt, som följs upp i samband med nödändringar.
2. Tillsynsmyndigheten verifierar att hantering av ändringar verkställs genom att utnyttja till exempel händelser, tickets och loggregistreringar som hänför sig till ändringarna. Dessutom kan man använda sig av intervjuer. Genomförandet av förfaranden för hantering av ändringar kan också verifieras genom att jämföra konfigurations- och versionsuppgifter samt ändringsloggen med konfigurationen som körs och versionen i olika objekt.

   Tillsynsmyndigheten verifierar hur uppdateringspraxis verkställs till exempel genom att be om uppgifter om gjorda uppdateringar (händelselogg, skärmdumpar och motsvarande).
3. Tillsynsmyndigheten verifierar att uppdateringspraxis verkställs till exempel genom skanning. Eventuella incidenter utreds med hjälp av aktören eller i dokumentationen.

**Motiveringar**

Genom hantering av ändringar och uppdateringar kan utnyttjandet av många sårbarheter förhindras. En viktig försvarsmetod är att snabbt reagera på uppdateringsbehov särskilt i kommunikationsnätens och informationssystemens yttre omgivning. Uppdateringar i sig ger dock inte alltid ett perfekt slutresultat. Det kan finnas en annan produkt till exempel i kommunikationsnät och informations-

| |
|---|
| system där samma sårbarhet inte är uppdaterad (patch). I dessa fall kan kännedom om produkterna och kompenserande åtgärder utifrån det, såsom olika begränsningar och övervakning, vara till hjälp. Även upphandling av en produkt och hantering av leveranskedjorna kan vara viktiga. Ibland känner leverantören av en eller annan orsak inte till en sårbarhet till exempel i ett bibliotek som används, varvid leverantören inte reagerar på korrigeringsbehovet. Sådana situationer är bra att beakta i synnerhet när det gäller säkerhetskritiska produkter. Organisationen kan till exempel föra bok över beroenden av sina kritiska produkter (software bill of materials, SBOM) och vid behov reagera på brister som upptäcks genom att uppdatera slutprodukterna. |
| **Källor** |
| ISO/IEC 27001:2022 (6.2, 6.3, 8.1)<br>ISO/IEC 27002:2022 (7.13, 8.19, 8.32)<br>IEC 62443-2-1:2010 (4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5)<br>IEC 62443-2-1:2024 (ORG 1.1, ORG 2.4, AVAIL 1.2, CM 1.4)<br>IEC 62443-2-4:2024 (SP.11.01, SP.11.02, SP.11.06)<br>IEC 62443-3-3:2013 (SR 3.4)<br>NIST CSF 1.1 (PR.AC-3)<br>NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01)<br>NIS CG Reference document (3.9.2 Change management and maintenance)<br>NIS CG Implementing guidance (6.4. Change management, repairs and maintenance) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-17)<br>Cybermätaren (ASSET-3, ASSET-4, ARCHITECTURE -3l,<br>ARCHITECTURE-5h) |

3.4.1 Hanteringen av ändringar och uppdateringar är systematiskt – utökade anvisningar

| |
|---|
| **Exempel på genomförande** |
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad. |

- Aktören har förfaranden för ändringar i kommunikationsnät och informationssystem. Förfarandena beaktar livscykelns faser ända från planeringen till elimineringen.
- Om möjligt, omfattar förfarandena planerade och oplanerade ändringar samt utveckling.
- Aktören har kanaler för att övervaka sårbarheter i kommunikationsnät och informationssystem. En kanal kan till exempel vara den internationella CSIRT-funktionen (CERT-FI) och tjänste- eller utrustningsleverantörernas anmälningskanaler.
- Informationssäkerhetsuppdateringar som är kritiska för cybersäkerheten i aktörens kommunikationsnät och informationssystem har installerats utan dröjsmål. Om det inte är möjligt har ersättande åtgärder tagits i bruk utan dröjsmål.
- Nödändringar har registrerats så att orsaken till att man frångått det normala förfarandet framgår. Om den testning som i normala fall krävs i samband med en nödändring har förbigåtts, så har testningen genomförts i efterhand till den del som det varit möjligt.
- Ändringar har när det varit möjligt testats och kontrollerats innan de införs i produktionssystemen.
- Vid behov har en analys om säkerhetseffektivitet gjorts för ändringen som även kan genomföras i ett separat testningssystem.
- Införandet av ändringar i systemen är organiserat. Ändringarna kan till exempel införas med RFC-processen (request for change), där ansvar och förfaranden har bestämts.
- Förfarandena för hantering av ändringar kan inbegripa till exempel följande faser: riskanalys, klassificering och prioritering samt fastställande av tester för dem, återkallande av ändringar (roll-back), dokumentering och godkännande av ändringar.
- Ändringar, underhåll och korrigeringar har genomförts och registrerats med bestämda verktyg.

**Verifiering**

1. Tillsynsmyndigheten inspekterar i aktörens dokumentation som beskriver hanteringen av ändringar att hanteringen av ändringar och uppdateringar som helhet är kontrollerad, systematisk och organiserad. Aktören har bestämt kanaler som följs för att upptäcka nödvändiga informationssäkerhetsuppdateringar och ändringsbehov samt handlingssätt för att analysera dessa uppdateringar och förändringar och vid behov införa dem utan dröjsmål i nödvändiga objekt. I synnerhet de ändringar som påverkar cybersäkerheten testas vid behov till exempel i testsystem eller på annat sätt när det gäller funktionaliteten och cybersäkerheten innan de införs i objektet. Tillsynsmyndigheten inspekterar att det finns ett systematiskt sätt för att godkänna, genomföra och registrera ändringar. Av dokumentationen om hantering av förändringar framgår även hur man hanterar ändringar och uppdateringar som görs genom fjärrhantering, särskilt när det gäller ändringar gjorda av tredje parter.

| |
|---|
| 2. I inspektionen av hur hanteringen av ändringar genomförs kan tillsynsmyndigheten använda de metoder som beskrivs i punkt 3.4.2 i större omfattning så att hanteringen av ändringar är förenlig med vad som beskrivs i dokumentationen. Det ska även finnas ansvarspersoner för olika åtgärder som känner till och följer processen. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27001:2022 (6.2, 6.3, 8.1)<br>ISO/IEC 27002:2022 (7.13, 8.31, 8.32)<br>IEC 62443-2-1:2010 (4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5, 4.3.4.3.7)<br>IEC 62443-2-1:2024 (ORG 1.1, ORG 2.3, ORG 2.4, AVAIL 1.2, CM 1.4)<br>IEC 62443-2-4:2015 (SP 11)<br>IEC 62443-2-4:2024 (SP.02.01, SP.03.01, SP.03.02, SP.03.05, SP.03.09, SP.07.04, SP.08.02, SP.08.04, SP.09.09. SP.10.02, SP.11.02, SP.11.06)<br>IEC 62443-3-3:2013 (SR 3.4)<br>NIST CSF 1.1 (PR.AC-3, ID.AM-1)<br>NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01, PR.PS-03, ID.IM-01, ID.IM-02)<br>NIS CG Reference document (3.9.2 Change management and maintenance)<br>NIS CG Reference document (3.9.5 Security patch management)<br>NIS CG Implementing guidance (6.4. Change management, repairs and maintenance)<br>NIS CG Implementing guidance (6.6. Security patch management) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-17)<br>Cybermätaren (ASSET-4, THREAT-1, THREAT-2) |

## 3.5 Testning av säkerheten

| |
|---|
| **Exempel på genomförande** |

- Aktören ska ha riktlinjer, förfaranden och handlingssätt för att testa sin informationssäkerhet i den omfattning som behövs med tanke på verksamheten, behoven och det riskbaserade behovet, se 1.6 Riskhanteringens effektivitet och indikatorer. Detta omfattar enligt behovet teknisk testning och till exempel testning av processer och förfaringssätt. Testerna kan gälla enskilda system eller hela organisationen.
- Säkerhetstesterna kan till exempel innehålla sårbarhetsskanningar och informationssäkerhetsrevisioner.
- Säkerhetstestningen är organiserad, ansvarspersoner har utsetts för den och den är regelbunden. Testning genomförs till exempel med vissa intervaller, i samband med att nya system tas i bruk, i samband med betydande ändringar och efter incidenter.
- Innehållet i säkerhetstestningen är definierad. Definitionerna kan till exempel inbegripa en beskrivning av testmetoder, objekt som ska testas och periferikomponenter. Av testningen sammanställs en täckande dokumentation av vilken framgår till exempel använda metoder, tidsstämpel och bevisning (evidens).
- Fynd som gjorts under testningen har hanterats. Från fall till fall kan detta innebära till exempel en ändring av processen, hantering av sårbarhetens konsekvens, omvärdering eller godkännande av den kvarstående risken.

**Verifiering**

1. Tillsynsmyndigheten inspekterar aktörens riktlinjer och praxis för att testa sin säkerhet i enlighet med hur nödvändig testningsverksamheten är med tanke på aktörens verksamhet, behov och riskbedömning. För vissa aktörer är det tillräckligt att genomföra punkt 1.6, i synnerhet om kommunikationsnätets och informationssystemens roll i verksamheten är mycket liten och måttfull när det gäller dess risknivån. Testningsåtgärderna kan till exempel vara regelbundna händelser där bestämda åtgärder genomförs. Sådana är till exempel tester i vissa processer eller i en teknisk miljö. I fråga om tekniska tester kan man till exempel inspektera utarbetade testningsrapporter.
2. Dessutom kan tillsynsmyndigheten kontrollera testningens effektivitet genom att inspektera metoder som används för att hantera i testningen hittade incidenter.

**Motiveringar**

De säkerhetstestningar som aktören genomför bidrar till att identifiera eventuella svagheter i kommunikationsnät, informationssystem och processer. Regelbundna testningar kan hindra en angripare från att utnyttja svagheter om aktören hittar och korrigerar dem först. Det är typiskt att det ibland till exempel inträffar fel i processen och att till exempel tjänster som inte är uppdaterade blir kvar i systemet eller att det finns öppna portar. Då kan säkerhetstestning ha en processkorrigerande effekt.

| Källor |
|---|
| ISO/IEC 27002:2022 (8.29, 8.33, 8.34) |
| IEC 62443-2-1:2010 (4.3.4.3.1) |
| IEC 62443-2-1:2024 (ORG 2.3, ORG 2.4, CM 1.4, DATA 1.1, EVENT 1.4) |
| IEC 62443-2-4:2015 (SP 02.02, RE 3) |
| IEC 62443-2-4:2024 (SP.02.01, SP.02.02, SP.03.02, SP.03.05, SP.03.09, SP.03.10, SP.06.03, SP.07.04, SP.08.02, SP.08.03, SP.09.09, SP.10.02, SP.11.02, SP.11.06) |
| IEC 62443-3-3:2013 (SR 3.5, 3.6, 3.7) |
| NIST CSF 1.1 (DE.CM-8, DE.DP-3, RS.MI-3) |
| NIST CSF 2.0 (ID.IM-02, ID.RA-01, ID.RA-06) |
| NIS CG Reference document (3.9.4 Security testing) |
| NIS CG Implementing guidance (6.5. Security testing) |
| **Verktyg** |
| Julkri (TEK-03.3, TEK-17) |
| Cybermätaren (THREAT-1, THIRD-PARTIES-2, ARCHITECTURE-4) |

## 3.6 Behandling och offentliggörande av sårbarheter

| Exempel på genomförande |
|---|
| • Aktören har rapporteringskanaler för att anmäla sårbarheter hos de tjänster som aktören tillhandahåller. Aktören har förfaringssätt och praxis för behandling av sårbarhetsanmälningar som gäller de tjänster som aktören tillhandahåller.<br>• Aktören har också förfaringssätt och praxis för att vid behov på interna och externa kommunikationskanaler informera om sårbarheten och eventuella metoder för att hantera den.<br>• Aktören har förfaringssätt och praxis för behandling av sårbarhetsuppgifter om de tjänster som används. (se 3.4.1)<br>• Aktören har inkluderat anmälning av sårbarheter till CSIRT i förfaringssätten och praxisen i enlighet med den nationella processen för samordnad publicering av sårbarhetsinformation[7] (CVD, coordinated vulnerability disclosure). |

[7] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/process-samordnad-publicering-av

| |
|---|
| **Verifiering** |
| 1. Tillsynsmyndigheten inspekterar aktörens dokumentation om hur upptäckta sårbarheter i produkter kan anmälas till aktören och hur sårbarheterna hanteras. Av dokumentationen ska också framgå hur upptäckta sårbarheter vid behov anmäls vidare till exempel till den nationella CSIRT och tjänstens användare. Av detta framgår till exempel kommunikationskanal, kommunikationssätt och ansvarsperson. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (8.8)<br>IEC 62443-2-1:2024 (EVENT 1.9, ORG 2.4)<br>IEC 62443-2-4:2015 (SP 02.02 RE(2), SP 03.03)<br>IEC 62443-2-4:2024 (SP.03.01, SP.03.03, SP.08.01)<br>NIST CSF 1.1 (ID.RA-1, ID.RA-5, PR.IP-12, RS.AN-5, RS.MI-3)<br>NIST CSF 2.0 (ID.RA-01, ID.RA-05, ID.RA-06, ID.RA-08, PR.PS-02)<br>NIS CG Reference document (3.9.3 Vulnerability handling and disclosure)<br>NIS CG Implementing guidance (6.10. Vulnerability handling and disclosure) |
| **Verktyg** |
| Cybermätaren (THREAT-2, THIRD-PARTIES-2)<br>Traficoms nyheter: Sårbarheter – att anmäla sårbarheter på korrekt sätt[8] |

## 3.7 Säkerhet vid utveckling

| |
|---|
| **Exempel på genomförande** |
| • Om aktören producerar tjänster eller system för kommunikationsnät och informationssystem ska man vid behov försäkra sig om att dessa tjänster i |

[8] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/sarbarheter-att-anmala-sarbarheter-pa-korrekt-satt

fråga om informationssäkerhet är i enlighet med punkt 3.2 Säkerheten hos föremålet för upphandlingen. Se även punkt 4.2 Riskhantering för leveranskedjor.

- Aktören ska ha en kanal för att anmäla om upptäckta sårbarheter i tjänster och system som aktören producerar. Se punkt 3.6 Hantering och offentliggörande av sårbarheter.
- Aktören har upprätthållit en materialförteckning över sina tjänster och system (till exempel SBOM, software bill of materials; HWBOM, hardware bill of materials) för att beroenden och sårbarheter i dessa kan identifieras.

**Verifiering**

1. Tillsynsmyndigheten inspekterar aktörens beskrivningar av hur säkerheten hos de tjänster som aktören producerar har säkerställts så att de särskilt uppfyller de krav som beskrivs i punkt 3.2 och beaktar dessutom punkt 4.2. Innehållet i beskrivningen beror i hög grad på tjänsternas och systemens karaktär och kraven på beskrivningarna ska stå i rätt proportion till detta. Aktören ska ha en lättillgänglig kanal för att rapportera om eventuella informationssäkerhetsproblem samt förfaranden för att hantera dessa rapporter och vid behov införa dem i slutprodukten (se 3.6). Aktören ska ha tillräcklig dokumentation i anknytning till tjänster och system, av vilken framgår bland annat beroenden till exempel av externa leverantörer eller tjänsteproducenter som en del av genomförandet av 4.2 och 3.2. Detta kan genomföras så att aktören upprätthåller innehållsinformation, såsom materialförteckningar (SBOM, HWBOM), om tjänster och system.
2. Tillsynsmyndigheten kompletterar inspektionen till exempel genom intervjuer och genom att med hjälp av aktören testa rapporteringskanalen för sårbarheter. Tillsynsmyndigheten kan dessutom använda eventuella skanningar eller testning av tjänster och system och material som producerats av dessa.

**Motiveringar**

**Källor**

ISO/IEC 27002:2022 (8.25, 8.31)

IEC 62443-2-1:2010 (4.3.4.3)

IEC 62443-2-1:2024 (ORG 2.3)

IEC 62443-2-4:2024 (SP 02.01)

NIST CSF 1.1 (PR.IP-2)

NIST CSF 2.0 (ID.AM-08)

| |
|---|
| NIS CG Reference document (3.9.6 Security in acquisition of ICT services, ICT systems or ICT products)<br>NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products)<br>NIS CG Implementing guidance (6.10. Vulnerability handling and disclosure) |
| **Verktyg** |
| Julkri (TEK-14)<br>Cybermätaren (THREAT-1, THIRD-PARTIES-2, ARCHITECTURE-4) |

## 3.8 Strukturell säkerhet i kommunikationsnät

**Exempel på genomförande**

Denna punkt kompletterar punkterna 11.3 och 11.4 om grundläggande praxis för informationssäkerhet.

- Aktörens kommunikationsnät är skyddat från otillåten åtkomst. Trafik är tillåten endast med protokoll som behövs för behövliga adresser och portar.
- Aktören har begränsat åtkomsten till sina tjänster enligt principen om lägsta behörighet till exempel genom att begränsa åtkomsten till tjänster i offentliga kommunikationsnät (gränssnitt, taltjänster, fildelning, hanteringstjänster) på basis av identitet, användargrupper, IP-adresser, portar eller protokoll. Principen om lägsta behörighet uppdateras under hela kommunikationsnätets livscykel med hjälp av ändringshantering.
- Även tjänsteleverantörernas distansförbindelser är skyddade. Särskild uppmärksamhet iakttas vid underhåll på distans och användningen av förbindelser för fjärråtkomstunderhåll har definierats noggrant.
- Dessutom kan aktören vid behov begränsa tjänsteleverantörens åtkomst behovs- och tidsbaserat.
- I kommunikationsnäten har använts endast enheter som hanteras av aktören och anslutning av andra enheter till kommunikationsnätet är förbjuden.
- Kommunikationskanalerna mellan systemet kan vid behov skyddas med metoder som baserar sig på till exempel logisk eller fysisk differentiering eller kryptering.
- Aktören har zonindelat (segmenterat) sina kommunikationsnät så att olika tjänster och system differentieras i egna områden. Detta kan grunda sig till exempel på kritiska tjänsterna eller systemen är och deras sårbarhet, konfidentialitet, användningsbehov eller -sätt. De system och motsvarande som använts har i mån av möjlighet differentierats i olika zoner. Vid zonindel-

ningen har man särskilt beaktat industriautomationsutrustningen (OT, operational technology och ICS, industrial control systems) och differentieringen av dessa från IT-systemen.

- Aktören har differentierat de system som är mycket sårbara eller kritiska eller som i händelse av att de blir utsatta för risker kan leda till att hela nätet eller systemet äventyras. Sådana system är till exempel hanteringsnät och hanteringsarbetsstationer.
- Trafiken mellan zonerna har begränsats så att endast nödvändig trafik är tillåten.
- Aktören har differentierat sina system och kommunikationsnät från de system och kommunikationsnät som leverantörer och tjänsteleverantörer tillhandahåller.
- Differentieringen kan genomföras med många olika tekniker såsom fysisk eller logisk differentiering genom att använda till exempel följande eller kombinationer av dem: virtuellt lokalt nätverk (virtual local area network VLAN, virtual extensible local area network VXLAN), brandvägg, network access control NAC, system för detektion av intrång/system för att förhindra intrång IDS/IPS, virtuellt privat nätverk (virtual private network VPN).
- Aktören har också kunnat utnyttja mikrosegmentering och nollförtroendeprincipen (zero trust) vid differentieringen av nätet.
- Det finns aktuella nätverksbilder och nätverksscheman om aktörens kommunikationsnät och informationssystem.

**Verifiering**

1. Vid inspektionen av den strukturella säkerheten i kommunikationsnät utnyttjar tillsynsmyndigheten dokumentation, till exempel nätverksbilder, beskrivningar av informationssystemen, funktionssätt och andra anvisningar. Till exempel av nätverksbilder framgår hur förbindelser till olika icke-tillförlitliga kommunikationsnät har begränsats till exempel att förbindelserna går via enskilda punkter. Punkterna är i allmänhet till exempel brandväggar, krypteringsenheter och fjärråtkomstpunkter. Aktören har dessutom kunnat dela sina informationssystem och kommunikationsnät i separata delar, till exempel i enlighet med olika roller, behovet av informationssäkerhet, användningsbehovet eller hur kritiska de är.
2. Tillsynsmyndigheten verifierar nätverkets struktur genom intervjuer och konfigurationsinspektioner. I randenheter och olika delar av det interna nätverket är endast nödvändig trafik tillåten. Detta kan kontrolleras till exempel i brandväggs- eller routerreglerna, vid behov i samarbete med aktören. I vissa fall kan filtrering även göras på enhets- eller applikationsnivå i själva objektet (till exempel en tjänst eller terminalutrustning). Brandväggens och fjärråtkomstpunkternas standardvärden förbjuder all trafik som inte behövs. Motsvarande funktion kan även uppnås på andra sätt, såsom statisk routing och kryptering. En zonindelning kan ofta kontrolleras på det ovannämnda sättet eller genom att undersöka konfigurationen hos nätverkets aktiva enheter. En av de vanligaste metoderna är att dela in olika zoner i virtuella nätverk (virtual local

area network VLAN), men även andra tekniker kan vara i användning. Vid inspektion av dessa konfigurationer är det särskilt bra att använda aktörens personal.

Tillsynsmyndigheten ber aktören att verifiera kommunikationsnätets skydd till exempel genom att visa de delar av konfigurationen som till exempel anger hur principen om lägsta behörighet verkställs.

3. Nätverkets strukturella skydd kan också kontrolleras med olika skanningsapplikationer och genom att utnyttja telekommunikationsinspelningar av aktören. Aktören kan göra skanningarna själv eller använda en tredje part, vars resultat tillsynsmyndigheten inspekterar.

   Skanningsverktyg kan utnyttjas till exempel genom att kartlägga synligheten av olika delar i kommunikationsnäten från andra delar av nätverket. Det lönar sig att se till att skanningar inte genomförs kors och tvärs mellan olika delar i nätverket. Det lönar sig dessutom att vara särskilt omsorgsfull vid skanningar där man i icke-tillförlitliga kommunikationsnät verifierar synligheten i aktörens kommunikationsnät. Förutom skanningar kan man även utnyttja generering av olika telekommunikationspaket. Man göra åtkomstförsök från olika källor till tjänster i objektet som testat genom att till exempel använda webbläsare och andra program. I kontrollen av nätverkets säkerhet kan man också utnyttja telekommunikationsinspelningar som kan användas för att inspektera kommunikationen mellan olika enheter och att icke-tillåtna enheter inte kommunicerar mellan varandra.

## Motiveringar

Att skydda kommunikationsnäten förhindrar en stor del av den skadliga trafiken från osäkra nätverk. Zonindelning av informationssystem och kommunikationsnät är en central metod för att fördröja en angripare från att avancera i kommunikationsnät och informationssystem efter att hen har fått fotfäste i objektet som angrips.

## Källor

ISO/IEC 27002:2022 (8.16, 8.20, 8.22)

IEC 62443-2-1:2010 (4.2.3.5, 4.3.3.4)

IEC 62443-2-1:2024 (NET 1.1, NET 1.3, NET 1.5, NET 1.6, NET 2.2, NET 3.2, NET 3.3, USER 1.16)

IEC 62443-2-4:2015 (SP 02.03)

IEC 62443-2-4:2024 (SP.03.02, SP.03.03, SP.03.07, SP.05.05, SP.07.03, SP.07.04)

IEC 62443-3-3:2013 (SR 1.11, 1.12, 1.13, 2.5, 2.6, 2.7, 3.1, 3.8, 5.1, 5.2, 5.4, 7.7)

NIST CSF 1.1 (PR.AC-3, PR.AC-5)

NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01)

| |
|---|
| NIS CG Reference document (3.9.8 Network security) |
| NIS CG Reference document (3.9.9 Network segmentation) |
| NIS CG Implementing guidance (6.7. Network security) |
| NIS CG Implementing guidance (6.8. Network segmentation) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi |
| Julkri (TEK-01) |
| Cybermätaren (ARCHITECTURE-2) |
| För skanning: nmap, Nessus, OpenVAS, Rapid7 |
| För telekommunikationsinspelning: Wireshark, tcpdump, netflow, sFlow |
| För åtkomstförsök: ping, hping3, nc, ssh, Pythonin scapy-kirjasto |

## 3.9 Skydd mot skadlig trafik

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkterna 11.3 och 11.5 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har sätt för att upptäcka skadlig trafik och förhindra otillåtna applikationer och genomförande av dem om det är möjligt.<br>• Aktören har en lösning som förhindrar skadlig eller oönskad trafik från icke-tillförlitliga kommunikationsnät, till exempel brandvägg (som separat utrustning eller programvara) eller åtkomstlista (access control list, ACL).<br>• På basis av aktörens riskhantering kan det också finnas till exempel system för detektion eller förhindrande av intrång (system för detektion av intrång/intrusion detection system IDS, system för förhindrande av intrång/intrusion prevention system IPS, endpoint detection and response EDR, extended detection and response XDR) och tjänster som begränsar överbelastningsangrepp (t.ex. pakettvättar).<br>• Aktören har tekniska kontroller eller åtminstone skriftlig praxis för installation av programvara och skydd mot skadliga program (t.ex. e-postnätfiskemeddelanden, okända externa lagringsmedier, piratapplikationer, skadlig roaming).<br>• Aktören ska automatiskt administrera installation och genomförande av programvara samt användning av lagringsmedier (till exempel Windows Defender Application Control WDAC, AppLocker, AppArmor, SELinux). |

- Aktören använder skydd mot skadliga program, såsom antivirusprogram på terminaler (t.ex. Anti-Virus AV, EDR, XDR), IDS/IPS eller mellanserver. Skyddet mot skadliga program kan även till exempel vara centraliserad i e-posttjänsten (förhindrande av nästfiskemeddelanden/anti-phishing, förhindrande av skadliga program/anti-malware, DomainKeys Identified Mail DKIM, Domain-based Message Authentication, Reporting and Conformance DMARC osv.)
- Applikationer som observerar skadlig trafik har uppdaterats tillräckligt ofta för att de ska kunna identifiera nya skadliga program. Det kan till exempel innebära en gång per dag eller annan regelbunden uppdatering av certifikat eller heuristisk information.
- Dessutom är anslutning av externa medier i systemen förhindrad.
- Observation och förhindrade av skadliga program kan även till exempel göras för e-posttrafiken och nättrafiken.
- Observationen av skadliga program och blockering av otillåtna applikationer ska gälla alla enheter, inklusive mobila enheter. Om detta inte kan verkställas ska man använda andra ersättande lösningar.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören observerar och heltäckande förhindrar skadlig trafik. Skadlig trafik av skadliga program eller angripare har förhindrats i synnerhet i anslutningspunkter där aktörens kommunikationsnät och informationssystem förenas med icke-tillförlitliga nätverk eller nätverkets centrala delar för verksamheten. Väsentliga objekt är i allmänhet till exempel brandväggar, fjärråtkomstpunkter (till exempel VPN-nätsluss), infrastruktur för trådlöst nät, kommunikationssystem såsom e-post och SMS samt ofta även externa tjänster såsom nättjänster och gränssnitt. Man har också förhindrat skadlig trafik från att avancera genom att förhindra att otillåtna och skadliga applikationer körs och installeras. Detta kan göras till exempel med applikationer som identifierar och förhindrar skadliga program, applikationer som förhindrar okända externa enheter samt applikationer och regler som förhindrar körning och installation av otillåtna program. I vissa fall kan man också använda lösningar som baserar sig på förfaranden och tillvägagångssätt, om till exempel systemets risknivå är särskilt liten, tekniska lösningar inte är möjliga eller annars proportionerliga.
2. Tillsynsmyndigheten verifierar genom konfigurationen att skydd för att upptäcka och förhindra skadlig trafik används. Dessutom är det bra att inspektera systemens funktion genom att till exempel utnyttja logguppgifter. Om skadlig trafik avvärjas med förfaranden och tillvägagångssätt som grundar sig på organisatoriska lösningar kan medvetenheten och kompetensen i anknytning till dessa kontrolleras till exempel med intervjuer.
3. Tillsynsmyndigheten testar med hjälp av aktören och tjänsteleverantören funktionen hos skydd som upptäcker och förhindrar skadlig trafik. Dessa tester får dock inte äventyra aktörens eller tjänsteleverantörens kommunikationsnät eller informationssystem. Testning kan göras till exempel genom att kringgå e-postskyddet på olika sätt såsom att använda förfalskade adresser,

försöka köra ett ofarligt men otillåtet program i olika objekt och inrikta ofarliga men förbjudna inmatningar i tjänsterna.

**Motiveringar**

Största delen av lyckade angrepp grundar sig på skadliga program som kan till exempel vara virus, maskar och trojaner. Programmen kan också innehålla skadliga egenskaper, såsom bakdörrar som gör det möjligt för en angripare att komma in i systemet. Det är viktigt att program installeras från säkra källor och att man försöker förhindra skadliga applikationer. Det kan också fungera genom att begränsa applikationernas förmågor. Då kan en del av den skadliga applikationens funktion förhindras.

**Källor**

ISO/IEC 27002:2022 (5.32, 8.7, 8.19)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.2, COMP 2.1, COMP 2.2, COMP 2.3, CM 1.4, NET 1.8)

IEC 62443-2-4:2024 (SP.10.01, SP.10.02, SP.10.03, SP.10.05)

IEC 62443-3-3:2013 (SR 3.2, 3.3)

NIST CSF 1.1 (DE.CM-4, DE.CM-5, DE.CM-7)

NIST CSF 2.0 (DE.CM-01, DE.CM-03, DE.CM-09)

NIS CG Reference document (3.9.10 Protection against malicious and unauthorized software)

NIS CG Implementing guidance (6.9. Protection against malicious and unauthorized software)

NIS CG Implementing guidance (12.3. Removable media policy)

**Verktyg**

Kartläggning av angreppsytan Hyöky.fi

Julkri (TEK-11)

Cybermätaren (SITUATION-2, ARCHITECTURE-3)

Förhindrande av skadlig trafik: för e-post m.m. Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) och Sender Policy Framework (SPF), brandvägg för nätapplikation (web application firewall WAF), mellanserver, system för att upptäcka angripare/system för att förhindra intrång (intrusion detection/prevention system IDS/IPS).

Förhindrande av otillåtna applikationer: SELinux, AppArmor, Windows Defender Application Control WDAC, AppLocker.

# 4 Den övergripande kvaliteten och resiliensen hos leveranskedjan för direkta leverantörers produkter och tjänsteleverantörers tjänster och de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem samt cybersäkerhetspraxis hos leverantörer och tjänsteleverantörer

Rekommendationerna grundar sig på artikel 21.2 d och artikel 21.3 i NIS 2-direktivet. Om nationellt genomförande av dessa punkter föreskrivs i 9 § 2 mom. 4 punkten i cybersäkerhetslagen och 18 c § 1 mom. 4 punkten i informationshanteringslagen.

1. **Förteckning över leverantörer och tjänsteleverantörer:** Aktören ska ha aktuell information om alla direkta leverantörer och tjänsteleverantörer som påverkar verksamheten och tjänsteutbudet. (Se punkt 4.1).

2. **Riskhantering för leveranskedjor:** I sin riskhantering bör aktören beakta konsekvensen av en störning i leveranskedjan i den egna verksamheten och ha beredskap för en eventuell leveransstörning. Aktören bör beakta säkerhetsaspekter i förhållande till direkta enhets- eller tjänsteleverantörer i sin leveranskedja. Vid bedömningen av riskhanteringsåtgärder bör man beakta de sårbarheter som är typiska för till exempel den direkta leverantören och tjänsteleverantören, den övergripande kvaliteten och resiliensen i fråga om produkter och tjänster som aktören använder, de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem samt praxis för cybersäkerhet hos leverantörer och tjänsteleverantörer. Dessa kunde inbegripa till exempel olika krav i anknytning till säkerheten till exempel när det gäller tillgänglighet, underhåll och avtal. NIS-samarbetsgruppen, Europeiska kommissionen och Enisa utarbetar i enlighet med artikel 22 i NIS 2-direktivet riskbedömningar av vissa leveranskedjor tillsammans. Till den del sådana riskbedömningar har gjorts kan tillsynsmyndigheten genom en föreskrift kräva att aktörerna beaktar resultaten av riskbedömningen. (Se punkt 4.2).

## 4.1 Förteckning över leverantörer och tjänsteleverantörer

| **Exempel på genomförande** |
|---|
| • Aktören har upprätthållit en förteckning över alla direkta enhets- och tjänsteleverantörer samt vid behov över andra leverantörer som påverkar cybersäkerheten.<br>• Förteckningen ska innehålla leverantörernas kontaktuppgifter. Aktören har särskilt sett till upprätthållandet av uppgifter på de leverantörer som har tillgång till kritiska funktioner eller underhåller kritiska funktioner.<br>• Förteckningen beskriver tjänster, system och produkter som produceras av leverantören. Dessutom är det bra att i förteckningen ha frågor som gäller avtalet, såsom avtalsperiodens längd och frågor i anknytning till hela livscykeln. |

| **Verifiering** |
|---|
| 1. Tillsynsmyndigheten inspekterar att aktören har en heltäckande förteckning över sina direkta enhets- och tjänsteleverantörer. Av förteckningen framgår till exempel kontaktuppgifter och av leverantören levererade tjänster, system och produkter. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (5.22)<br>IEC 62443-2-1:2024 (ORG 1.6, CM 1.1)<br>IEC 62443-2-4:2024 (SP.06.02)<br>NIST CSF 1.1 (ID.SC-2, ID.SC-3)<br>NIST CSF 2.0 (GV.SC-03, GV.SC-05, GV.SC-07)<br>NIS CG Reference document (8.2 Directory of suppliers and service providers)<br>NIS CG Implementing guidance (5.2 Directory of suppliers and service providers) |
| **Verktyg** |
| Cybermätaren (CRITICAL-1, THIRD-PARTIES-1) |

## 4.2 Riskhantering för leveranskedjor

| **Exempel på genomförande** |
|---|
| • I fråga om de leverantörer som identifierats i punkt 4.1 har aktören identifierat konsekvensen av en eventuell störning i leveranskedjan i den egna verksamheten. Aktören har bestämt behövliga beredskapsåtgärder vid eventuella leveransstörningar och utarbetat riktlinjer för leveranskedjornas säkerhet. Kontinuitets- och återhämtningsplaneringen preciseras i punkt 10.1.<br>• Aktören har inkluderat direkta enhets- och tjänsteleverantörer i handlingsmodellen för riskhantering, gör en riskbedömning av dem och hanterar risker som är förenade med dem. Aktören har valt åtgärder som står i rätt proportion i anknytning till leveranskedjorna och vidtagit åtgärder för sådana leverantörer där riskhanteringsåtgärderna främjar cybersäkerheten. Se punkt 1.1 Handlingsmodell för hantering av cybersäkerhetsrisker. |

- Vid övervägande av riskhanteringsåtgärder har aktören beaktat för direkta leverantörer och tjänsteleverantörer säregna
  - sårbarheter som beror på läge, produkturval eller sektorns karaktär,
  - den övergripande kvaliteten och resiliensen i fråga om produkter och tjänster,
  - de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i produkter och tjänster samt praxis för cybersäkerhet hos leverantörer och tjänsteleverantörer som kan basera sig på praxis, certifieringar eller andra bevis som leverantören använder.
- Leverantören har vid behov inbegripit olika cybersäkerhetskrav i sina leveranskedjor till exempel när det gäller tillgänglighet, underhåll och avtal. Aktören bör identifiera för dem viktiga egenskaper i anknytning till cybersäkerhet och ställa krav som står i rätt proportion. Sådana kan till exempel vara servicenivåavtal som ställs på avtal.
- Aktören har hanterat cybersäkerhetsrisken i leveranskedjorna till exempel genom att inkludera hanteringsåtgärder för cybersäkerhetsrisker i avtalen som aktören ingår med sina direkta leverantörer och tjänsteleverantörer. Dessa kan till exempel vara bedömning av cybersäkerhetsegenskaper under avtalsperioden, krav på personalens utbildning och certifiering, anmälningspraxis av sårbarheter och granskning av tjänstens tillvägagångssätt för underhåll. Se även punkt 3.2 Säkerheten hos föremålet för upphandlingen.
- Aktören har vid valet av leverantörer och tjänsteleverantörer även beaktat möjliga bestämmelser av tillsynsmyndigheten om riskbedömningsresultaten av leveranskedjor enligt artikel 22 i NIS 2-direktivet.
- Aktören kan även vid behov be om materialförteckningar över kritiska produkter och tjänster (till exempel SBOM, software bill of materials; HWBOM, hardware bill of materials) för att beroenden och sårbarheter i dessa kan identifieras och hanteras.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har utarbetat riktlinjer för säkerheten i leveranskedjorna. Tillsynsmyndigheten verifierar att aktören har genomfört säkerhetsaspekter i leveranskedjorna. Aktören har vidtagit följande åtgärder:
   - Aktören har beaktat eventuella störningar i leveranskedjan i den egna verksamheten. Aktören har beredskap för störningar i leveranskedjorna till exempel genom reservarrangemang, avtalstekniskt eller som en del av kontinuitetshanteringen (se 10.1).
   - Aktören har beaktat säkerhetsaspekter i förhållande till direkta enhets- eller tjänsteleverantörer. Tillsynsmyndigheten verifierar till exempel i dokumentationen hur säkerhetsaspekterna har beaktats. Detta kan till exempel framgå av säkerhetskrav som ställs på enhets- och tjänsteleverantörer, begränsningar i förhållande till aktörens kommunikationsnät och informationssystem samt i de förfaranden och praxis som krävs (se till exempel 11, grundläggande praxis för informationssäkerhet).

- Aktören har inkluderat de risker som leveranskedjorna medför i riskhanteringsåtgärderna i den mån aktören har bedömt att det är nödvändigt för att säkerställa cybersäkerheten. Detta kan till exempel innebära att man beaktar sårbarheter som är typiska för leverantören eller tjänsteleverantören. Aktören har identifierat den övergripande kvaliteten och resiliensen i fråga om produkter och tjänster och beaktat dessa frågor till exempel som en del av kontinuitetshanteringen genom att inrikta riskhanteringsmetoder på produkter och tjänster och skydda sina viktigaste funktioner.
- Aktören har i sin leveranskedja beaktat hanteringsåtgärder för cybersäkerhetsrisker som ingår i produkter och tjänster. Detta innebär till exempel att aktören utreder cybersäkerheten i leveranskedjorna i den mån det är möjligt och hanterar risker som orsakas av detta som en del av sin riskhantering. Aktören har kunnat utreda cybersäkerhetens nivå till exempel genom enhets- och tjänsteleverantörens rykte, informationssäkerhetscertifikat, avtal eller som en del av upphandlingen (se 3.2) och genom att begära dokumentation eller annat material. Aktören har kunnat hantera kvarstående risker av enhets- och tjänsteleverantören genom att identifiera riskerna och inkludera dem i den egna riskhanteringen.
- Aktören har i sin leveranskedja beaktat leverantörernas och tjänsteleverantörernas praxis för cybersäkerhet. Dessa kan beaktas till exempel på de sätt som nämns i punkt d ovan. Dessutom har aktören i allmänhet bestämt med vilken praxis leverantörer och tjänsteleverantörer tillhandahåller sina tjänster i aktörens kommunikationsnät och informationssystem. Praktiska exempel är att aktören har kunnat bestämma till exempel med vilka enheter eller praxis för fjärråtkomst som leverantören eller tjänsteleverantören tillhandahåller sin tjänst i aktörens kommunikationsnät eller informationssystem. Aktören har även kunnat bestämma anvisningar, skyldigheter och utbildningar (se 6) som krävs av leverantören eller tjänsteleverantören (personalen).

**Motiveringar**

Allvarliga sårbarheter och angrepp som utnyttjar leveranskedjor har blivit betydligt vanligare under de senaste åren. Sårbarheten i leveranskedjor har även utnyttjas i attacker mot grundläggande infrastruktur.

**Källor**

ISO/IEC 27002:2022 (5.19, 5.20, 5.21, 5.37, 7.9, 8.30)

ISO 28000:2022 (4.1, 4.2, 5.2, 6.1, 6.2, 7.5, 8)

IEC 62443-2-1:2024 (USER 1.4, ORG 1.1, ORG 1.6)

IEC 62443-2-4:2024 (SP.02.01)

NIST CSF 1.1 (ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4)

| |
|---|
| NIST CSF 2.0 (GV.OC-05, GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-09)<br>NIST SP 800-37 rev 2 (2.8)<br>NIST SP 800-161 rev 1 (2.2, 2.3.4, 3.2, 3.4.2, A, B)<br>NIS CG Reference document (3.8.1 Supply chain policy)<br>NIS CG Implementing guidance (5.1. Supply chain security policy) |
| **Verktyg** |
| Julkri (HAL-06, TEK-16, TSU-16)<br>Cybermätaren (CRITICAL-2, CRITICAL-3, THIRD-PARTIES-1, THIRD-PARTIES-2) |

# 5 Tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på dess säkerhet

Rekommendationerna grundar sig delvis på artikel 21.2 i i NIS 2-direktivet. Om nationellt genomförande av denna föreskrivs i 9 § 2 mom. 5 punkten i cybersäkerhetslagen och 18 c § 1 mom. 5 punkten i informationshanteringslagen.

1. **Förfaranden och anvisningar för tillgångsförvaltning**: Aktören ska för tillgångsförvaltningen ha regelbundna och dokumenterade förfaranden och anvisningar som kan inbegripa till exempel identifiering av funktioner, processer och information. (Se punkt 5.1).

2. **Tillgångsförteckning och tillgångsklassificering**: Med tillgångar avses t.ex. lokaler, maskinvara, programvara, tjänster, personer, immateriella tillgångar och resurser såsom immateriella rättigheter eller IP-adresser. Tillgångar i anknytning till kommunikationsnät och informationssystem kan till exempel identifieras och klassificeras utifrån skyddsbehoven. Man kunde till exempel föra en uppdaterad förteckning över tillgångarna. (Se punkt 5.2).

3. **Användning av tillgångsförteckningen**: Tillgångsförvaltningen ska i princip vara en väsentlig del av hanteringen av förändringar i fråga om personal, externa aktörer och informationssystem samt livscykelhanteringen i fråga om utrustning från det att den tagits i bruk till det att den tas ur bruk på ett säkert sätt. (Se punkt 5.3).

## 5.1 Förfaranden och anvisningar för tillgångsförvaltning

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkt 11.2 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har utarbetat riktlinjer för tillgångsförvaltningen samt förfaranden och anvisningar för tillgångsförvaltning och tillgångarnas användning, och de är i allmänhet i linje med organisationens riktlinjer och förfaranden för säkerheten. Närmare bestämmelser om riktlinjer och förfaranden som gäller säkerheten finns i punkterna 2.1 och 2.1.1 Riktlinjer och förfaranden som gäller säkerheten.<br>• Aktören har inkluderat systematisk identifiering av funktioner, processer och uppgifter i förfarandena och anvisningarna för tillgångsförvaltning.<br>• I förfarandena och anvisningarna för tillgångsförvaltning har man beaktat den utrustning och de program som hyrs ut. De är till behövliga delar i linje med förteckningen i 4.1.<br>• Riktlinjerna, förfarandena och anvisningarna omfattar tillgångarnas hela livscykel från upphandling, säker transport, lagring och användning till säker eliminering samt radering och förstöring av data. Aktören har i riktlinjerna, |

förfarandena och anvisningarna beaktat till exempel en säker användning av externa lagringsmedier.

- Förfaranden och anvisningar har hållits uppdaterade genom regelbundna inspektioner (t.ex. en gång per år och i samband med betydande ändringar eller incidenter).

**Verifiering**

1. Tillsynsmyndigheten inspekterar av aktören utarbetade dokument om riktlinjer, förfaranden och anvisningar för tillgångarnas förvaltning och användning. Förfaranden och anvisningar är uppdaterade och av dem framgår aktörens funktioner, processer och systematisk identifiering av information samt förfaranden för upprätthållande av tillgångsförteckningen som har gjorts till exempel med planerade intervaller och vid betydande ändringar eller incidenter.

**Motiveringar**

Tillgångsförvaltning är ett effektivt verktyg i hanteringen av cybersäkerhetsrisker och omsorgsfull hantering av tillgångar förebygger risker och hjälper i riskhanteringen. Den är också en av de billigaste och enklaste metoderna för hantering av säkerheten.

**Källor**

ISO/IEC 27002:2022 (5.9, 5.10, 5.14, 5.37, 5.34, 7.10)

IEC 62443-2-1:2010 (4.3.4.4.6)

IEC 62443-2-1:2024 (CM 1.1, CM 1.3, DATA 1.1, DATA 1.2, DATA 1.4, ORG 1.1, COMP 1.2)

IEC 62443-2-4:2024 (SP.06.02)

IEC 62443-3-3:2013 (SR 2.4)

NIST CSF 1.1 (ID.AM-1, ID.AM-2)

NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-04, ID.AM-08)

NIS CG Reference document (3.4.2 Asset Handling)

NIS CG Implementing guidance (12.2. Handling of assets)

NIS CG Implementing guidance (12.3. Removable media policy)

**Verktyg**

Julkri (HAL-04)

Cybermätaren (ASSET-1, ASSET-2, ASSET-5)

## 5.2 Tillgångsförteckning och klassificering

**Exempel på genomförande**

Denna punkt kompletterar punkt 11.2 om grundläggande praxis för informationssäkerhet.

- Aktören har utarbetat en tillgångsförteckning som lämpar sig för aktörens verksamhet och ändamål över funktioner, processer och information som även kan inbegripa aktörens lokaler, enheter, program, tjänster, personer, immateriella tillgångar och resurser såsom immateriella rättigheter eller IP-adresser. I tillgångsförteckningen ingår utrustning, programvaror och lokaler som aktören förfogar över genom avtal. Tillgångsförteckningen är uppdaterad.
- Tillgångsförteckningen kan innehålla till exempel följande uppgifter:
  - Tillgången och en unik identifierare av den
  - Ägare, förvaltare och användare
  - Beskrivning
  - Placering
  - Typ av tillgång (program inklusive virtuella datorer, enheter samt deras operativsystem och programvara, tjänster, lokaler, VVS-system, personal, fysiska lagringar)
  - Klassificering av tillgångar
  - Riskklassificering baserad på riskbedömning (och vid behov klassificeringens effektivitet, jämför punkt 5.3)
  - Enhetens programvaruversion, programvarans SBOM (software bill of materials)
  - Slutdatum för användarstödet
  - Säkerhetskopiering
- Tillgångsförvaltningen har baserat sig på tillgångarnas informationssäkerhetsbehov, såsom konfidentialitet, riktighet och tillgänglighet. Aktören har även kunnat inkludera autenticitet och obestridlighet i informationssäkerhetskraven.
- Med tillgångsklassificeringen kan man bestämma tillgångarnas skyddsbehov enligt hur kritiska de är, risken och affärsvärdet. Aktören har bedömt risker som hänför sig till tillgångarna som en del av åtgärderna för hantering av cybersäkerhetsrisker. Aktören kan i sin tillgångsförteckning inkludera sannolikheten eller riskklassificeringen för externt hot mot tillgångarna.
- Det är bra om kraven i anknytning till tillgångarnas tillgänglighet är i linje med affärsverksamhetens kontinuitet och återhämtningsplaner (se 10).
- Aktören har bestämt klassificering för den information som ska skyddas och den utgör till exempel en del av personalens utbildning. Aktören har informerat personalen och centrala intressentgrupper om det (se 6.5).
- Aktören kan i klassificeringen använda till exempel nationell lagstiftning, nationellt eller internationellt kända rekommendationer och anvisningar för informationsklassificering.

| **Verifiering** |
|---|
| 1. Tillsynsmyndigheten inspekterar aktörens tillgångsförteckning. Tillgångsförteckningen innehåller aktörens funktioner, processer och uppgifter som nämns i genomförandeexemplet. Aktören har i bruk tillgångsklassificering på basis av tillgångarnas skyddsbehov. Aktören har inspekterat och uppdaterat tillgångsförteckningen regelbundet. Tillgångsförteckningens riktighet kan verifieras med dokumentinspektion så att tillgångsförteckningens innehåll jämförs med annan tillgänglig dokumentation såsom nätverksbilder, upphandlingsuppgifter, tillsynsvyer och observationer i tillsynen.<br>2. Tillsynsmyndigheten kan inspektera tillgångsförteckningens riktighet med en fysisk granskning. Tillsynsmyndigheten kan till exempel gå igenom aktörens lokaler och jämföra enheter som finns där med tillgångsförteckningen.<br>Tillgångsförteckningens riktighet kan också granskas med tekniska metoder. Alternativen är bland annat konfigurationsgranskning till exempel innehållet i ARP-tavlor (endast Ipv4) dock genom att beakta att alla enheter, i synnerhet ICS/OT (industrial control system/operational technology), inte nödvändigtvis gör ARP-förfrågningar automatiskt samt DHCP-databas (leases database) och DNS-uppgifter.<br>3. Tillsynsmyndigheten bekräftar tillgångsförteckningens riktighet med passiva och aktiva skanningar. Vid passiv skanning utnyttjas till exempel nätverksinspelning där man söker aktörens enheter som deltagit i trafiken. Vid aktiv skanning går man igenom aktörens IP-adressrymd (IPv4, IPv6). |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (5.9, 5.12, 5.13, 5.34)<br>ISO/IEC 27005:2022 (7.2, 8.6, 10.5)<br>IEC 62443-2-1:2010 (4.2.3.4, 4.2.3.6, 4.3.4.4.2, 4.3.4.4.3, 4.3.4.4.6, A.2.3.3.8.3)<br>IEC 62443-2-1:2024 (CM 1.1, CM 1.3, DATA 1.1, DATA 1.2)<br>IEC 62443-2-4:2024 (SP.03.08 RE(2), SP.06.01, SP.06.02)<br>IEC 62443-3-3:2013 (SR 7.8)<br>NIST CSF 1.1 (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, PR.IP-1)<br>NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, PR.PS-01)<br>NIS CG Reference document (3.4.1 Asset classification)<br>NIS CG Reference document (3.4.4 Asset inventory) |

| |
|---|
| NIS CG Implementing guidance (12.1. Asset classification)<br>NIS CG Implementing guidance (12.4. Asset inventory) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (HAL-04.2)<br>Cybermätaren (ASSET-1, ASSET-2, THIRD-PARTIES-1, ARCHITECTURE-3, ARCHITECTURE-5)<br>Skanningsprogram: arp scan, nmap, Nessus, hping3 |

## 5.3 Användning av tillgångsförteckningen

| |
|---|
| **Exempel på genomförande** |
| Denna punkt kompletterar punkt 11.9 om grundläggande praxis för informationssäkerhet.<br>• Aktören har säkerställt att tillgångsförteckningen är uppdaterad och att tillgångsförteckningen vid behov betjänar annan verksamhet, såsom riskhantering, uppdateringshantering, kontinuitet i affärsverksamheten och hantering av tillgångarnas livscykel.<br>• Tillgångsförteckningen har uppdaterats regelbundet och till exempel i samband med betydande ändringar, ändringar i kommunikationsnät och informationssystem inklusive teknikval, verktyg och konton.<br>• Det är bra om ändringshistoriken i tillgångsförteckningen kan spåras.<br>• Tillgångsförteckningen stöder hanteringen av enheternas livscykel från säkert ibruktagande av en enhet till att den tas ur bruk. Säkert ibruktagande av en enhet har preciserats i punkt 3.4 Hantering av ändringar och uppdateringar.<br>• Aktören har beaktat återställning av enheter och radering av uppgifter, avslutande av konton och användarnamn som aktören besitter när ett anställningsförhållande eller underleverantörsavtal upphört. Mer om detta i punkt 6.1 Förfaranden för personalsäkerheten och 6.2 Förfaringssätt för personalsäkerheten. |
| **Verifiering** |
| 1. Tillsynsmyndigheten inspekterar tillgångsförteckningen i enlighet med punkt 5.2. Aktören har uppdaterat tillgångsförteckningen regelbundet eller i samband med ändringar.<br>Tillsynsmyndigheten inspekterar tillgångsförvaltning till exempel som en del i inspektionen av verksamhetsmodellen för riskhantering i punkt 1. Detta inne- |

bär till exempel att aktörens riskhantering är i linje med de identifierade tillgångarna. Aktören har även i sin tillgångsförteckning kunnat inkludera till exempel konsekvensen av en risk i tillgångarna och klassificeringen.

**Motiveringar**

**Källor**

ISO/IEC 27002:2022 (5.9, 5.11, 5.18, 5.24, 5.34, 7.9, 8.10)

ISO/IEC 27005:2022 (7.2, 8.6, 10.5)

IEC 62443-2-1:2010 (4.2.3.4, 4.3.3.2, A.2.3.3.8.3)

IEC 62443-2-1:2024 (4.2.3.4, 4.3.3.2, A.2.3.3.8.3)

IEC 62443-2-4:2024 (SP.06.01, SP.06.02)

IEC 62443-3-3:2013 (SR 7.8)

NIST CSF 1.1 (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5 PR.IP-1)

NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, PR.PS-01)

NIS CG Reference document (3.4.4 Asset inventory)

NIS CG Reference document (3.4.5 Return or deletion of assets upon termination of employment)

NIS CG Implementing guidance (12.4. Asset inventory)

NIS CG Implementing guidance (12.5. Return or deletion of assets upon termination of employment)

**Verktyg**

Julkri (HAL-04)

Kybermittari (ASSET-1, ASSET-2, ASSET-3, ACCESS-1, ACCESS-2)

# 6 Personalsäkerhet och utbildning i cybersäkerhet

Rekommendationerna grundar sig delvis på artikel 21.2 i och g i NIS 2-direktivet. Nationellt genomförande av dessa föreskrivs i 9 § 2 mom. 6 punkten i cybersäkerhetslagen och 18 c § 1 mom. 6 punkten i informationshanteringslagen.

1. Förfaranden för personalsäkerheten: Med personalsäkerhet avses förfaranden som säkerställer personalens ansvar och skyldigheter i fråga om IT-säkerhet, deras IT-säkerhetskompetens samt bakgrundskontroller och hanteringen av nyckelpersonrisker. Dessutom omfattar dessa förfaranden förebyggande av missbruk, vilket bland annat innebär identifiering och undvikande av farliga arbetskombinationer, arbetsrotation samt upphörande av ett anställningsförhållande eller ett avtal. (Se punkt 6.1).

2. **Förfaringssätt för personalsäkerheten:** Aktören ska till exempel ha personalrelaterade förfaranden där också externa aktörer, såsom underleverantörer, beaktas. Förfaringssätten kan exempelvis också beakta ansvar och skyldigheter efter det att anställningsförhållandet upphört och arbetsuppgifterna ändrats. (Se punkt 6.2).

3. **Sekretess och skyldigheter**: Personalen och externa aktörer kan vid behov informeras till exempel om ansvar och skyldigheter i anslutning till säkerheten i deras arbetsuppgifter och tjänster, till exempel i fråga om sekretess. (Se punkt 6.3).

4. **Bakgrundskontroller:** Om arbetsuppgifterna och ansvaren anses kräva särskild tillförlitlighet, kan personen i mån av möjlighet bli föremål för en ändamålsenlig bakgrundskontroll. (Se punkt 6.4).

5. **Personalutbildning**: Aktören ska se till att personalen har förmåga att agera på ett sätt som motsvarar handlingsmodellen och åtgärderna för hantering av cybersäkerhetsrisker. För att uppnå detta kan personalen exempelvis få utbildning som ökar medvetenheten om cybersäkerhet i allmänhet, kunskaper om aktuella förfaranden och aktuell praxis samt om kända cybersäkerhetsrisker. Genom utbildning eller på något annat motsvarande sätt bör det säkerställas att personalen med hänsyn till arbetsuppgifterna har tillräcklig kompetens i fråga om skydd av kommunikationsnät och informationssystem, identifiering av cybersäkerhetsrisker, riskhanteringspraxis och bedömning av deras konsekvenser för de tjänster som aktören tillhandahåller och att denna kompetens också upprätthålls på en tillräcklig nivå. (Se punkt 6.5 och 6.5.1).

6. **Ledningens förtrogenhet**: Bestämmelser om skyldigheten för en aktörs ledning att upprätthålla tillräcklig förtrogenhet med riskhantering inom cybersäkerhet finns i 10 § i cybersäkerhetslagen och 18 b § i informationshanteringslagen. (Se punkt 6.6).

## 6.1 Förfaranden för personalsäkerheten

| **Exempel på genomförande** |
|---|
| • Aktören har skriftliga förfaranden som beskriver personers ansvar och skyldigheter i fråga om informationssäkerheten.<br>• I aktörens förfaranden för personalsäkerheten beskrivs även tredje parter, såsom externa aktörer och underleverantörer (se 6.2).<br>• Aktörens förfaranden för personalsäkerheten beskriver hur personalens informationssäkerhetskompetens säkerställs (se 6.5).<br>• Aktörens förfaranden för personalsäkerheten täcker också behov som hänför sig till bakgrundskontroller (se 6.4) och nyckelpersoner (se 6.6).<br>• Förfarandena för personalsäkerheten beaktar vid behov personalens olika roller. Detta kan framkomma till exempel i beaktande av ledningens ansvar som en del av förfarandena. Aktören kan till exempel definiera, namnge och befullmäktiga roller i anslutning till kommunikationsnätens och informationssystemens säkerhet och riskhantering enligt aktörens behov.<br>• Aktören kan fastställa roller, ansvar och befogenheter som gäller skyldigheterna i cybersäkerhetslagen, såsom till exempel genomförande av riskhanteringsåtgärder inom cybersäkerhet enligt 9 § och anmälan om incidenter till behörig myndighet enligt 11 § (se 9.1 och 9.7).<br>• Aktören har informerat personalen och tredje parter om förfaranden som gäller personalsäkerheten och om viktiga säkerhetsrelaterade roller.<br>• Aktören har sett till att personer som utsetts till rollerna har tillräcklig kompetens för att utföra sina uppgifter (se 6.5).<br>• Aktörens förfaranden främjar förhindrande av missbruk. Aktören har identifierat farliga arbetskombinationer och sett till att uppgifterna differentieras. Med differentiering av uppgifter undviks situationer då det uppstår arbetskombinationer som medför risker eller som har motstridiga skyldigheter och ansvarsområden. En typisk farlig arbetskombination är till exempel att en person både begär och godkänner en åtgärd eller att en person har tillgång både till ett objekt som övervakas och uppgifter som fås vid övervakningen.<br>• Aktörens förfaranden i anknytning till personalsäkerheten beskriver de förfaranden genom vilka missbruk kan förhindras. Dessa förfaringssätt kan omfatta till exempel ändringar i anställningsförhållanden, uppgiftsrotation, ändring eller upphörande av ett anställningsförhållande. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har skriftliga förfaranden när det gäller personalsäkerheten. I dessa förfaranden beskrivs ansvar och skyldigheter i fråga om informationssäkerheten som personalen ska iaktta för att uppnå säkerheten. Förfaranden beskriver utbildningar i informationssäkerhet, bakgrundskontroller och nyckelpersoner. Förfarandena gäller vid behov även tredje parter, såsom underleverantörspartner, åtminstone i fråga om funktionssätt (se 6.2). Förfarandena innehåller frågor i anknytning till missbruk, |

| |
|---|
| såsom identifiering av farliga arbetskombinationer och differentiering av uppgifter samt ändringar i och upphörande av anställningsförhållanden och avtal.<br>2. Tillsynsmyndigheten bekräftar kännedomen om och genomförandet av förfaranden för personalsäkerheten, till exempel genom intervjuer. Av intervjuerna ska framgå till exempel funktionen för nyckelpersonsrollerna i praktiken, så att tillräckliga resurser och befogenheter har reserverats för genomförande av uppgiften. Dessutom intervjuas personalen om farliga arbetskombinationer och differentieringen av dem på praktisk nivå. |
| **Motiveringar** |
| Informationssäkerheten är en helhet där personalen är den viktigaste faktorn. Personalen är ofta också den svagaste länken i fråga om informationssäkerhet, så personalens medvetenhet om informationssäkerheten, personalrelaterade förfaranden och funktionssätt är ytterst viktiga.<br><br>Personalen är det viktigaste elementet i organisationernas riskhantering. Det är viktigt att informera personalen så att de efter förmåga kan identifiera risker som är förenade med det egna arbetet. Genom samarbete åstadkoms i allmänhet bättre riskhantering än genom arbete som utförs av en begränsad grupp. |
| **Källor** |
| ISO 27001:2022 (5.3, 7.1, 7.2, 7.4)<br>ISO 27002:2022 (5.2, 5.3, 5.5, 6.2, 6.3, 6.4, 6.5)<br>IEC 62443-2-1:2010 (4.3.3.2)<br>IEC 62443-2-1:2024 (ORG 1.1, ORG 1.2, ORG 1.3, ORG 1.4, ORG 1.5, ORG 1.6, ORG 2.1, ORG 2.2)<br>IEC 62443-2-4:2015 (SP 01.07)<br>IEC 62443-2-4:2024 (SP.01.01, SP.01.02, SP.01.03, SP.01.04, SP.01.05, SP.01.06, SP.01.07)<br>NIST CSF 1.1 (PR.AT-5, PR.IP-11)<br>NIST CSF 2.0 (PR.AT-02, GV.RR-04)<br>NIS CG Reference document (3.2.2 Roles, responsibilities and authorities)<br>NIS CG Reference document (3.5.1 Human resources security)<br>NIS CG Reference document (3.5.4 Disciplinary process)<br>NIS CG Implementing guidance (1.2 Roles, responsibilities and authorities)<br>NIS CG Implementing guidance (10.1. Human resources)<br>NIS CG Implementing guidance (10.4. Disciplinary process) |
| **Verktyg** |

| |
|---|
| Julkri (HAL-02)<br><br>Cybermätaren (THIRD-PARTIES-1, THIRD-PARTIES-2, WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, Allmänna förvaltningsåtgärder) |

## 6.2 Förfaringssätt för personalsäkerheten

| **Exempel på genomförande** |
|---|
| • Aktörens förfaringssätt för personalsäkerheten verkställer förfaranden i anknytning till ändringar i och upphörande av anställningsförhållanden.<br>• Åtgärder i anslutning till ändringar kan inbegripa till exempel ändringar i åtkomsträttigheter i utrustning som en person använder när arbetsuppgifterna ändras.<br>• Förfaringssätten beskriver också åtgärder som görs när arbetsuppgifter upphör. Dessa kan bland annat vara borttagning av åtkomsträttigheter och enheter, förstörande av data samt åtgärder som hänför sig till överföring av tillgångar, kompetens och ansvar. Personalen har också informerats om dessa åtgärder.<br>• Förfaringssätten för personalsäkerheten gäller även tredje parter, såsom externa aktörer och underleverantörer. |
| **Verifiering** |
| 1. Tillsynsmyndigheten bekräftar i dokumentationen att aktören har förfaringssätt för åtgärder som vidtas i samband med ändringar i och upphörande av arbetsuppgifter. Dessa förfaringssätt gäller även tredje parter, såsom externa aktörer och underleverantörer.<br>2. Tillsynsmyndigheten kan till exempel i system och konfigurationer bekräfta att ansvar och skyldigheter har genomförts i enlighet med förfaringssätten. Detta kan innebära till exempel att onödiga åtkomsträttigheter har ändrats eller slopats, enheter har återställts, onödigt data har tagits bort och ansvar vid behov överförts till annan personal. |
| **Motiveringar** |
| En förändring i arbetsuppgifterna utgör en stor risk för att till exempel onödiga rättigheter, information eller utrustning blir kvar hos en person som inte längre är berättigad till dem. I synnerhet fall när en persons arbetsuppgifter upphör kan i vissa fall medföra till och med en stor risk för organisations informationssäkerhet om tillgången till resurserna inte förhindras. |
| **Källor** |

| |
|---|
| ISO/IEC 27002:2022 (6.5, 8.10)<br>IEC 62443-2-1:2010 (4.3.3.2)<br>IEC 62443-2-1:2024 (ORG 1.2, ORG 1.3, USER 1.1, USER 1.2, USER 1.4)<br>IEC 62443-2-4:2015 (SP 01.07)<br>IEC 62443-2-4:2024 (SP.01.07, SP.09.02, SP.09.03, SP.09.04)<br>NIST CSF 1.1 (PR.IP-11)<br>NIST CSF 2.0 (GV.RR-04)<br>NIS CG Reference document (3.5.3 Termination or change of employment procedures)<br>NIS CG Implementing guidance (10.3 Termination or change of employment procedures) |
| **Verktyg** |
| Cybermätaren (ACCESS-1, ACCESS-2, ACCESS-3, THIRD-PARTIES-1, THIRD-PARTIES-2, WORKFORCE-1) |

## 6.3 Sekretess och skyldigheter

| **Exempel på genomförande** |
|---|
| • Aktören säkerställer att de förfaranden som beskrivs i punkt 6.1 Förfaranden för personalsäkerheten inbegriper till exempel anvisningar och skyldigheter i hantering av utrustningen, användningen av användarnamn, hantering och underhåll, internetbeteende, sociala medier, användning av egen utrustning, programsäkerhet och externa lagringsmedier.<br>• Aktören säkerställer speciellt att skyldigheter som hänför sig till sekretess har beskrivits och meddelats till personalen och vid behov till tredje parter. Aktören har bestämt sekretessbelagda saker på ett tydligt sätt. Detta kan genomföras till exempel genom att märka sekretessbelagd information eller informationssystem. Dessutom ska aktören försäkra sig om att information behandlas korrekt när den överlåts och mottas.<br>• Personalen och personalen hos tredje parter ska förstå, verkställa och iaktta skyldigheterna som hänför sig till personalsäkerheten. Aktören har även beskrivit hur personalen informeras om skyldigheterna i fråga om informationssäkerheten. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har bestämt skyldigheterna i anslutning till informationssäkerheten. Skyldigheterna är täckande och stöder genomförandet av aktörens informationssäkerhet. Av dokumentationen ska |

| |
|---|
| dessutom framgå definitioner och ansvar i anknytning till sekretess samt i allmänhet även hur hanteringen av sekretessbelagt material säkerställs när information överlåts och mottas.<br>2. Tillsynsmyndigheten verifierar till exempel genom intervjuer att skyldigheterna för informationssäkerheten uppfylls, att personalen är medveten om dem och identifierar eventuella sekretessbelagda objekt och känner till ansvaret och skyldigheterna som hänför sig till dem. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (5.10, 6.6)<br>IEC 62443-2-1:2024 (USER 1.4, DATA 1.1, DATA 1.2)<br>IEC 62443-2-4:2024 (SP.01.03)<br>NIST CSF 1.1 (PR.AT-3, PR.AT-4, PR.AT-5)<br>NIST CSF 2.0 (PR.AT-02)<br>NIS CG Implementing guidance (5.1 Supply Chain Security)<br>NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products) |
| **Verktyg** |
| Julkri (HAL-15)<br>Cybermätaren (THIRD-PARTIES-2, WORKFORCE-1, WORKFORCE-3) |

## 6.4 Bakgrundskontroller

| |
|---|
| **Exempel på genomförande** |
| • Aktören har identifierat de arbetsuppgifter och ansvar som kräver speciell tillförlitlighet. I dessa fall ska det vid behov kontrolleras att personen är behörig för uppgifterna i fråga genom bakgrundskontroller.<br>• Bakgrundskontrollerna förnyas till exempel med fem års mellanrum eller när personens arbetsuppgifter ändrar. |
| **Verifiering** |

| |
|---|
| 1. Tillsynsmyndigheten verifierar att aktören har identifierat sådana arbetsuppgifter och ansvar till vilka den person som väljs ska genomgå bakgrundskontroller. |
| **Motiveringar** |
| |
| **Källor** |
| ISO/IEC 27002:2022 (6.1)<br>IEC 62443-2-1:2010 (4.3.3.2.2, 4.3.3.2.3)<br>IEC 62443-2-1:2024 (ORG 1.2, ORG 1.6)<br>IEC 62443-2-4:2015 (SP 01.04)<br>IEC 62443-2-4:2024 (SP.01.04)<br>NIST CSF 1.1 (PR.IP-11)<br>NIST CSF 2.0 (GV.RR-04)<br>NIS CG Reference document (3.5.2 Background checks)<br>NIS CG Implementing guidance (10.2 Background checks) |
| **Verktyg** |
| Julkri (HAL-10)<br>Cybermätaren (WORKFORCE-1) |

## 6.5 Personalutbildning

| |
|---|
| **Exempel på genomförande** |
| Denna punkt kompletterar punkt 11.1 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har sett till att personalen har kunskap och tillräcklig kompetens att agera i enlighet med riktlinjerna för säkerheten i den mån det är väsentligt för arbetsuppgifterna. För att uppnå detta bör det ordnas regelbundna utbildningar om förfaranden och praxis som syftar till att förbättra medvetenheten om den allmänna cybersäkerheten och cybersäkerhetsrisker samt tillräcklig kompetens med tanke på arbetsuppgifterna i anknytning till skydd av informationssystem och kommunikationsnät, identifiering av cybersäkerhetsrisker, |

bedömning av praxis för hantering av cybersäkerhetsrisker och dess effektivitet på tjänster som aktören tillhandahåller.

- Aktören har bestämt på vilket sätt hela personalen utbildas om aktörens funktionssätt i anslutning till cybersäkerheten.
- Personalens utbildning har omfattat åtgärder för hantering av cybersäkerhetsrisker. Syftet med utbildningen är att försäkra sig om att personalen genom sin verksamhet stöder verkställandet av hanteringsåtgärderna till den del det är väsentligt för arbetsuppgifterna.
- Aktören har utbildat sin personal även när det gäller hanteringen av cybersäkerhetsrisker till den del de är väsentliga för arbetsuppgifterna. Detta kan till exempel innebära information om de vanligaste cybersäkerhetsriskerna och vid behov bedömning av hanteringsåtgärdernas effektivitet till exempel anslutning till cyberrisker i de egna arbetsuppgifterna. Dessutom har aktören utbildat sin personal att identifiera eventuella cyberrisker till exempel till stöd för aktörens hantering av cyberrisker.
- Aktören kan identifiera uppgifter och roller som kan vara av särskilt intresse. Dessa personer kan skyddas genom skräddarsydda utbildningar till exempel om social manipulation, påverkansförsök och nätfiske.
- Aktören kan främja personalens allmänna medvetenhet om cybersäkerheten även med lättare metoder. Genom att utnyttja till exempel korta informationsinslag om färska bedrägeriförsök eller händelser inom sektorn.

**Verifiering**

1. Tillsynsmyndigheten verifierar i dokumentationen att aktören tillhandahåller utbildning till sin personal om hantering, identifiering och vid behov bedömning av cybersäkerhetsrisker. Utbildningen inbegriper förfaranden och praxis med hjälp av vilka aktören främjar medvetenheten om cybersäkerhet och hanteringen av cybersäkerhetsrisker. Utbildningen syftar till att personalen har tillräcklig kompetens i förhållande till sina arbetsuppgifter om att skydda kommunikationsnät och informationssystem samt identifiering av cybersäkerhetsrisker. Vid behov ska man genom utbildning även säkerställa, om arbetsuppgifterna kräver det, att personalen har förmåga att bedöma praxis för hantering av cybersäkerhetsrisker och deras effektivitet i fråga om de tjänster som aktören tillhandahåller.

**Motiveringar**

**Källor**

ISO/IEC 27001:2022 (7.2, 7.3)

ISO/IEC 27002:2022 (6.3)

IEC 62443-2-1:2010 (4.3.2.4)

| |
|---|
| IEC 62443-2-1:2024 (ORG 1.3, ORG 1.4, ORG 1.5) |
| NIST CSF 1.1 (PR.AT-1) |
| NIST CSF 2.0 (PR.AT-01) |
| NIST SP 800-161 rev 1 (3.3) |
| NIS CG Reference document (3.6.2 Security training) |
| NIS CG Implementing guidance (8.2 Security training) |
| **Verktyg** |
| Julkri (HAL-13) |
| Cybermätaren (WORKFORCE-2, WORKFORCE-4) |

### 6.5.1 Personalutbildning – utökade anvisningar

| **Exempel på genomförande** |
|---|
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br>• Aktören har genomfört utbildning i anknytning till cybersäkerhet systematiskt och följt upp deltagandet i utbildningen.<br>• Utbildningen är tillräckligt omfattande och som en del av den kan man också mäta hur de deltagande personerna har förstått utbildningens tema.<br>• Aktören har praxis som tillämpas för att genomföra utbildning som saknas. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har bestämt att utbildningen sker systematiskt. Dessutom ska aktören ha praxis för att övervaka deltagandet i utbildningen.<br>2. Tillsynsmyndigheten verifierar till exempel i ett deltagarregister eller motsvarande att personalen deltar i utbildningar och försäkrar sig om detta. Genom intervjuer kan man dessutom verifiera personalens kompetens i och medvetenhet om cybersäkerhet. |
| **Motiveringar** |
| |
| **Källor** |

| |
|---|
| ISO/IEC 27001:2022 (7.2) |
| ISO/IEC 27002:2022 (6.3) |
| IEC 62443-2-1:2010 (4.3.2.4) |
| IEC 62443-2-1:2024 (ORG 1.3, ORG 1.4, ORG 1.5) |
| NIST CSF 1.1 (PR.AT-1) |
| NIST CSF 2.0 (PR.AT-01) |
| NIST SP 800-161 rev 1 (3.3) |
| NIS CG Reference document (3.6.2 Security training) |
| NIS CG Implementing guidance (8.2 Security Training) |
| **Verktyg** |
| Cybermätaren (WORKFORCE-4) |

## 6.6 Ledningens förtrogenhet

| **Exempel på genomförande** |
|---|
| • Aktören ska försäkra sig om att ledningen har tillräcklig kompetens om ledning av allmän hantering av cybersäkerhetsrisker. Detta kan genomföras till exempel genom utbildningar eller självstudier för att säkerställa tillräcklig kompetens för identifiering av cybersäkerhetsrisker, ledning av riskhanteringen samt konsekvensbedömning av praxis för riskhantering.<br>• Med ledning avses aktörens styrelse, förvaltningsråd, verkställande direktör eller någon annan i därmed jämförbar ställning som de facto leder dess verksamhet.<br>• Aktören ska försäkra sig om att ledningen är förtrogen med hanteringen av aktörens cybersäkerhetsrisker och kan fatta beslut som grundar sig på detta. Ledningen är också medveten om sin roll, sitt ansvar och inflytande i hanteringen av cybersäkerhetsrisker. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen att ledningens medlemmar har deltagit i tillräcklig utbildning. I och med detta har ledningen till exempel tillräcklig förståelse för hanteringen av cybersäkerhetsrisker och är medveten om sin roll, sitt ansvar och inflytande i frågan. Ledningen är medveten om hanteringen av cybersäkerhetsrisker i organisationen och kan behandla resultaten av riskhanteringen. |

2. Tillsynsmyndigheten kan verifiera till exempel i utbildningsregister eller genom intervjuer att ledningens medlemmar har deltagit i utbildningar om riskhantering av cybersäkerhet, studieavsnitt eller på annat sätt visar att de har tillräcklig kompetens. Dessutom kan tillsynsmyndigheten utreda hur medlemmarna har beaktat åtgärder för hantering av cybersäkerhetsrisker i sina beslut och i sin verksamhet.

**Motiveringar**

En fungerande hantering av cyberrisker kräver åtagande av ledningen. Å andra sidan krävs kompetens för att förstå cybermiljön och riskerna i anknytning till den. Ledningen har ofta ett stort ansvar och centrala uppgifter när det gäller hanteringen av cybersäkerhetsrisker. Uppgifterna hänför sig till exempel till val av hanteringsåtgärder, beslut som gäller kvarstående risker, ordnande av resurser och bemyndiganden.

**Källor**

ISO/IEC 27001:2022 (5.1, 9.3)

ISO/IEC 27002:2022 (5.4)

ISO/IEC 27005:2022 (10.6)

IEC 62443-2-1:2010 (4.3.2.3.3, 4.3.2.6, 4.4.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 1.3, ORG 1.4, ORG 2.4)

NIST CSF 1.1 (GV.PO-01, GV.PO-02, PR.AT-4)

NIST CSF 2.0 (PR.PS-04, PR.AT-02)

NIST SP 800-30 rev 1 (3.3)

NIS CG Reference document (3.1 Top management commitment and accountability)

**Verktyg**

Cybermätaren (CRITICAL-2, RISK-1, WORKFORCE-4, PROGRAM-2,)

# 7 Åtkomsthantering och autentisering

Rekommendationerna grundar sig delvis på artikel 21.2 i och j i NIS 2-direktivet. Nationellt genomförande av dessa föreskrivs i 9 § 2 mom. 7 punkten i cybersäkerhetslagen och 18 c § 1 mom. 7 punkten i informationshanteringslagen.

1. **Förfaranden för åtkomsthantering:** Förfarandena för åtkomsthantering och autentisering ska gälla både fysiska användare, t.ex. personal och externa aktörer, och systemkoder, t.ex. koder som används av maskinvara, programvara, gränssnitt och andra väsentliga resurser. Åtkomsthanteringen ska gälla både åtkomst som kan autentiseras genom ett program och fysisk åtkomst. Förfarandena ska grunda sig på de verksamhetsrelaterade kraven samt på de krav som ställs på datanätverk och informationssystem med beaktande av systemens särdrag. Aktören kan till exempel i anknytning till åtkomsthanteringen ha definitioner och praxis som övergripande säkerställer en tillförlitlig identifiering och tillåter åtkomst endast till nödvändiga kommunikationsnät och informationssystem, skyddade uppgifter och andra resurser. (Se punkt 7.1).

2. **Kontinuerligt upprätthållande av åtkomsthantering och åtkomsträttigheter:** Aktören kan till exempel ha förfaranden som täcker användarnamnens och åtkomsträttigheternas hela livscykel, och åtkomsträttigheterna ska hanteras i enlighet med dem. (Se punkt 7.2).

3. **Övervakning av åtkomsthanteringen:** Åtkomsträttigheterna och användningen av dem ska övervakas. (Se punkt 7.3 och 7.3.1).

4. **Dokumentering för åtkomsthantering och principen om lägsta behörighet:** Åtkomsträttigheter och roller kan exempelvis fortgående dokumenteras och användarna kan ges endast de rättigheter som de behöver för att utföra sina arbetsuppgifter (principen om lägsta behörighet). (Se punkt 7.4).

5. **Huvudanvändarnamn**: Aktörerna bör ha förfaranden för hantering av användarkonton med stark behörighet och för huvudanvändarkonton, till exempel så att man strävar efter att begränsa huvudanvändarrättigheterna till ett så litet antal användare som möjligt och så att koderna skyddas med starka metoder. Utövandet av huvudanvändarrättigheter ska övervakas. (Se punkt 7.5).

6. **Val av säkra kontrollmetoder och tillförlitlig autentisering:** De kontrollmetoder och kontrolltekniker som väljs bör grunda sig på kraven på åtkomst till informationen och på kontrollförfarandena. Kontrollmetoderna ska vara tillräckligt säkra för att i möjligaste mån förhindra obehörig användning. Vid behov ska som kontrollmetod användas stark autentisering, multifaktorautentisering (MFA) eller kontinuerlig autentisering, om dessa kan användas. (Se punkt 7.6).

## 7.1 Förfaranden för åtkomsthantering

**Exempel på genomförande**

Denna punkt kompletterar punkt 11.6 om grundläggande praxis för informationssäkerhet.

- Förfarandena för åtkomsthantering och autentisering ska gälla både fysiska användare, till exempel personal och externa aktörer, och systemkoder, till exempel koder som används av maskinvara, programvara, gränssnitt och andra väsentliga resurser.
- Aktören ska i anknytning till åtkomsthanteringen ha förfaranden, definitioner och praxis som övergripande säkerställer tillförlitlig identifiering (authentication, AuthN) till kommunikationsnät och informationssystem, skyddade uppgifter och andra resurser. Aktören har vid behov också utarbetat en riktlinje för åtkomsthanteringen.
- Förfaranden för aktörens åtkomsthantering och autentisering omfattar både åtkomst genom ett program och fysisk åtkomst.
- Förfarandena ska grunda sig på de affärsverksamhetsrelaterade kraven samt på de krav som ställs på datanätverk och informationssystem med beaktande av systemens särdrag.
- Åtkomsthantering och autentisering har säkerställt att identifieringen i mån av möjlighet är användarspecifik och säkerställer användarens identitet på en tillräcklig nivå. Valet av identifieringsmetod kan grunda sig på riskbedömning av systemet. I ett system med låg risknivå kan även identifiering som grundar sig på användarnamn och säkert lösenord vara tillräckligt. I system med högre risknivå har man i mån av möjlighet använt kontrollmetoder som grundar sig på flera faktorer (multifaktorautentisering, multi-factor authentication, MFA). De kan förutom användarens lösenord till exempel vara tidsbaserade engångskoder, digitala certifikat, chipkort, identifieringsverktyg eller biometriska metoder.
- Om aktören använder gemensamma användarnamn är det enligt god praxis bra att säkerställa att kontrollmetoderna hanteras av de personer som har rätt till dem och att kontrollmetoderna lätt kan bytas och delas till användarna av användarnamnet på ett säkert sätt.
- Aktören har tillåtit åtkomst (authorization, AuthZ) endast till nödvändiga kommunikationsnät och informationssystem, skyddade uppgifter och andra resurser. Dessa åtkomster har genomförts på basis av definitionerna. Tillåten åtkomst har definierats enligt principen om lägsta behörighet. Det lönar sig i allmänhet att undvika behörigheter som grundar sig på en användare och i stället använda till exempel rollbaserad hantering av åtkomsträttigheter.
- Aktören har beaktat tillräcklig differentiering av uppgifterna när aktören tillåtit åtkomst till nödvändiga resurser. Ytterligare information om differentiering av uppgifter finns i punkt 6.1 Förfaranden för personalsäkerheten.
- Förfaranden och praxis för åtkomsthantering har ordnats utifrån aktörens affärsverksamhetsbehov och riskhantering. När det gäller kritiska system har

man försökt identifiera användarna individuellt till exempel genom passerkontroll. Mer om den fysiska säkerheten och lokalsäkerheten finns i punkt 12.

- Aktören kan enligt eget övervägande delvis eller helt ta i bruk nollförtroendeprincipen (zero-trust) som en del av sina principer för åtkomst, om den kan tillämpas i aktörens arkitektur. Nollförtroendeprincipen används i allmänhet särskilt i molntjänster eller hybridmoln.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har förfaranden, definitioner och praxis för åtkomsthantering och autentisering. Förfarandena är täckande och beaktar aktörens olika funktioner från fysiska lokaler till programgränssnitt. Dessa omfattar både personanvändare och systemkodernas åtkomsthantering och autentisering. Aktören har även beaktat tredje parter i sin åtkomsthantering. Tillsynsmyndigheten säkerställer att aktören har organiserat förfaranden för åtkomsthantering och autentisering, definitioner och praxis så att autentiseringen är tillförlitlig och grundar sig på principen om lägsta behörighet.
2. Tillsynsmyndigheten verifierar att aktörens system endast tillåter användarna sådana åtgärder som de har behörighet till. Detta kan säkerställas till exempel genom inspektion av åtkomsträttigheter eller testning av informationssäkerheten för att testa till exempel att användarna inte kan utföra åtgärder som är mer omfattande än deras bestämda behörigheter. Vid inspektionen kan man kontrollera att de roller och personer som fastställts i systemen motsvarar de beskrivna definitionerna (se 7.4) och på så sätt kontrollera att förfarandena verkställs. I systemen kan man även kontrollera att metoder för säker autentisering och identifiering faktiskt används. För detta kan man använda till exempel konfigurationsuppgifter och skärmdumpar.

**Motiveringar**

Förfaranden och praxis för åtkomsthantering säkerställer att kontrollerna av åtkomsthanteringen är rätt dimensionerade och omfattar alla aktörens system. Åtkomsthanteringens omfattning säkerställer att kontrollen har en inverkan på alla nödvändiga ställen. Förfaranden och praxis ska omfatta förutom funktioner som upplevs vara traditionell inloggning (till exempel inloggning i en dator eller på en webbplats) även omfatta andra funktioner som förutsätter åtkomsthantering, såsom fildelning. Störningssituationer i åtkomsthanteringen kan orsaka dataläckage eller -intrång när obehöriga personer får tillgång till uppgifter de inte har rätt till.

**Källor**

ISO/IEC 27002:2022 (5.3, 5.15, 5.16, 5.17, 5.18, 5.37, 8.3, 8.5)

IEC 62443-2-1:2010 (4.3.3.6, 4.3.3.7)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.2, USER 1.1, USER 1.2, USER 1.4, USER 1.5, USER 1.6, USER 1.7, USER 1.8, USER 1.9, DATA 1.1)

| |
|---|
| IEC 62443-2-4:2024 (SP.09.01, SP.09.02, SP.09.03, SP.09.04) |
| IEC 62443-3-3:2013 (SR 2.1) |
| NIST CSF 1.1 (PR.AC-4, PR.AC-7) |
| NIST CSF 2.0 (PR.AA-03, PR.AA-05) |
| NSA, CISA: Identity and Access Management: Recommended Best Practices for Administrators |
| NIS CG Reference document (3.7.1 Access control policy) |
| NIS CG Reference document (3.7.5 Identification) |
| NIS CG Implementing guidance (11.1. Access control policy) |
| NIS CG Implementing guidance (11.5. Identification) |
| **Verktyg** |
| Julkri (HAL-14, TEK-07, TEK-08) |
| Cybermätaren (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3) |

## 7.2 Kontinuerligt upprätthållande av åtkomsthantering och åtkomsträttigheter

| **Exempel på genomförande** |
|---|
| • Förfaranden och praxis för aktörens åtkomsthantering säkerställer att användarnamn och åtkomsträttigheter är uppdaterade.<br>• I aktörens livscykeltänkande för åtkomsthanteringen har man beaktat konsekvenserna som ändringar i anställningsförhållanden, avtal och andra motsvarande ändringar medför. Till exempel att extra användarnamn och åtkomsträttigheter tas bort när behovet upphör.<br>• I förfarandena har definierats nödvändig praxis och ansvar för ändringar i åtkomsthanteringen och åtkomsträttigheterna.<br>• Man har fäst särskild uppmärksamhet vid åtkomsträttigheterna för underhållsanvändarnamn och huvudanvändarnamn och de är kontinuerligt uppdaterade.<br>• Aktören har en uppdaterad dokumentering eller motsvarande förfarande över användarkonton och deras åtkomsträttigheter (se 7.4). |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har funktionssätt för förfaranden och praxis för åtkomsthantering för att uppföljning av åtkomsträttigheternas livscykel. I funktionssätten har beaktats bland annan användarhanteringsprocessen, borttagning av åtkomsträttigheter och användningen av tillfälliga an- |

vändarnamn. Vid borttagning av åtkomsträttigheter har man i synnerhet beaktat användare som inte längre arbetar i organisationen eller som inte har sakligt behov av resurserna i fråga till exempel på grund av ändringar i arbetsuppgifterna. Dessutom har aktören funktionssätt för användning av eventuella tillfälliga användarnamn.

2. Tillsynsmyndigheten verifierar att aktörens åtkomsthantering är uppdaterad. Genom inspektion kan man konstatera att onödiga användarkonton har tagits bort eller låsts. Rättigheterna till användarkonton inspekteras och säkerställs så att de endast har nödvändiga lägsta behörighet som motsvarar aktörens övriga dokumentation (se 7.4).

**Motiveringar**

Extra användarnamn och åtkomsträttigheter kan ge en angripare åtkomst till systemet. Allt för omfattande åtkomsträttigheter kan ge en arbetstagare möjlighet att se eller hantera resurser som det inte finns ett sakligt behov av på basis av arbetsuppgifterna.

**Källor**

ISO/IEC 27002:2022 (5.18)

IEC 62443-2-1:2010 (4.3.3.5.1, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.8)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5)

IEC 62443-2-4:2024 (SP.03.08, SP.09.04)

NIST CSF 1.1 (PR-AC.1)

NIST CSF 2.0 (PR.AA-01, PR.AA-05)

NIS CG Reference document (3.7.2 Management of access rights)

NIS CG Implementing guidance (11.2. Management of access rights)

**Verktyg**

Julkri (HAL-14, TEK-07.3)

Cybermätaren (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, WORKFORCE-1)

## 7.3 Övervakning av åtkomsthanteringen

**Exempel på genomförande**

- Aktören har övervakat åtkomsten till och användningen av system och enheter. För att det ska vara möjligt att genomföra övervakningen har aktören skapat till exempel logguppgifter över åtkomsthanteringshändelser eller annan

tillförlitlig information som möjliggör händelsespårning. Händelser i anknytning till åtkomsthantering är till exempel redigering av användarnamn, uppgifter om inloggning (vem, vad, varifrån, vart och när), användningen av användarnamn och huvudanvändaråtgärder.

- Händelseloggen i åtkomsthanteringen har förvarats tillräckligt länge för att eventuella fall av missbruk kan utredas även i ett senare skede, till exempel i utredningen av en incident.
- På basis av händelseregistreringarna har man övervakat till exempel onormala inloggningsförsök och andra händelser som grundar sig på riskhanteringen.
- Övervakningen har genomförts till exempel med manuella förfaranden, system som producerar automatiska larm, genom att följa trender och utnyttja anmälningskanaler. Mer information om övervakningen finns i punkt 9.3 Dokumentering och observation av händelser.
- Till följd av incidenter har ett användarkonto vid behov stängts, låsts eller dess kontrollmetod återställts. (Se 9.5)
- I vissa fall har aktören även använt manuell dokumentation, till exempel en gästbok. Det gäller i synnerhet för fysisk åtkomsthantering i situationer där automatisk dokumentation inte är möjlig. Övervakningen av åtkomsthantering som grundar sig på manuell dokumentation kan till exempel organiseras så att dokumentationen inspekteras regelbundet eller när en incident upptäcks.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har övervakat åtkomsten till och användningen av system och enheter. Aktören kan genomföra detta till exempel genom att samla in en logg som uppstår av åtkomsthanteringens händelser och förvara loggen tillräckligt länge. Aktören har praxis för genomgång av åtkomsthanteringens händelser. Aktören kan gå igenom händelsedokumentationen till exempel sporadiskt, med överenskomna intervaller eller när det finns skäl att misstänka en incident.
2. Om aktören övervakar åtkomsten till system och enheter och genom en logg över användningen så verifierar tillsynsmyndigheten att händelserna i anknytning till åtkomsthanteringen faktiskt producerar en logg. Av loggen ska framgå minst det objekt som används, källa, klockslag, användare samt eventuellt andra omständigheter i anknytning till åtkomsthanteringen såsom vilken typ av multifaktorautentisering som använts. Dessutom ska den motsvara aktörens eventuella dokumentation över åtkomsthanteringen. Tillsynsmyndigheten kan be aktören att uppvisa önskade punkter i loggen eller be aktören att lämna in loggen eller delar av den genom att beakta säkerheten.

**Motiveringar**

Övervakning av åtkomsthanteringen är en välkänd metod för att upptäcka obehörig användning av användarnamn samt till exempel intrångsförsök och missbruk. För att möjliggöra övervakningen är det vanligtvis nödvändigt att producera händelseregistreringar.

| **Källor** |
|---|
| ISO/IEC 27002:2022 (5.15, 8.15) |
| IEC 62443-2-1:2010 (4.3.3.6.4) |
| IEC 62443-2-1:2024 (USER 1.4, USER 1.5, USER 1.15, USER 2.1, EVENT 1.4, DATA 1.1) |
| IEC 62443-2-4:2024 (SP.08.02, SP.09.04) |
| NIST CSF 1.1 (PR.PT-1, PR.AC-7) |
| NIST CSF 2.0 (PR.PS-04, PR.AA-03) |
| Cybersäkerhetscentret: Så här samlar du in och använder loggdata[9] |
| NIS CG Reference document (3.7.2 Management of access rights) |
| NIS CG Reference document (3.11.2 Monitoring and logging) |
| NIS CG Implementing guidance (11.2 Management of access rights) |
| NIS CG Implementing guidance (3.2. Monitoring and logging) |
| **Verktyg** |
| Julkri (HAL-07, TEK-12) |
| Cybermätaren (ACCESS-2, ACCESS-3, SITUATION-2) |

### 7.3.1 Tillsynen av händelseregistreringar över åtkomsthantering – utökade anvisningar

| **Exempel på genomförande** |
|---|
| Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.<br><br>• Aktören har på basis av händelsedokumentationen övervakat till exempel onormala inloggningsförsök, ändringar av användare eller åtkomsträttigheter och andra händelser som hänför sig till riskhanteringen.<br>• Övervakningen har genomförts till exempel med system som producerar automatiska larm, genom att följa trender, manuella förfaranden och dessutom utnyttjande av anmälningskanaler. |

[9] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata

- Händelsedokumentationerna har vid behov överförts till exempel till SIEM (Security Information and Event Management) eller annat centraliserat logghanteringssystem i vilket man även kan samla in loggdata i anknytning till andra system.

**Verifiering**

1. Tillsynsmyndigheten verifierar aktörens dokumentation över övervakningen av händelseregistreringar. I dokumentationen ska definieras hur och vilka uppgifter som övervakas i loggen. I loggen har även bestämts fortsatta åtgärder på basis av observationerna i övervakningen, till exempel kommunikationskanaler för automatiska larm och uppföljningen av dem eller fortsatta åtgärder för hantering av en incident som upptäcks i systemansvariges logg.
2. Tillsynsmyndigheten verifierar att övervakningen har producerat händelser och att de har hanterats på behörigt sätt. Händelser som uppstått i övervakningen av loggen ska förvaras och hanteringshistoriken ska vara tydlig.

**Motiveringar**

Kontinuerlig övervakning gör det möjligt att reagera snabbt och förhindra omfattande skador.

**Källor**

ISO/IEC 27002:2022 (8.16)

IEC 62443-2-1:2010 (4.3.3.6.4, 4.3.3.6.7)

IEC 62443-2-1:2024 (DATA 1.1, EVENT 1.4, EVENT 1.7, USER 1.14, USER 1.15)

IEC 62443-2-4:2024 (SP.08.02, SP.08.03, SP.09.04)

NIST CSF 1.1 (PR.PT-1, PR.AC-7)

NIST CSF 2.0 (PR.PS-04, PR.AA-03)

NIS CG Reference document (3.11.2 Monitoring and logging)

NIS CG Implementing guidance (3.2. Monitoring and logging)

Cybersäkerhetscentret: Så här samlar du in och använder loggdata[10]

**Verktyg**

Julkri (HAL-07, TEK-12, TEK-13)

Cybermätaren (ACCESS-1, ACCESS-2, SITUATION-1, SITUATION-2, SITUATION-3)

[10] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata

## 7.4 Dokumentering för åtkomsthantering och principen om lägsta behörighet

| **Exempel på genomförande** |
|---|
| • Aktören har dokumentering eller motsvarande förfarande för att registrera åtkomsträttigheter och åtkomsträttighetsroller. Det finns ett förfarande för att upprätthålla en uppdaterad dokumentering.<br>• På basis av dokumenteringen har användarna endast getts de åtkomsträttigheter som de behöver för att utföra sina arbetsuppgifter (principen om lägsta behörighet). Man har i mån av möjlighet försökt undvika behörigheter som grundar sig på en användare och i stället använt rollbaserad hantering av åtkomsträttigheter. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar aktörens dokumentation över förfaranden i anknytning till registrering av åtkomsthantering. Av dokumentationen framgår hur åtkomsträttigheter och roller dokumenteras. Av aktörens dokumentation i anknytning till åtkomsthanteringen framgår systemens åtkomsträttigheter och åtkomsträttighetsroller. Dokumentationen kan för vissa system vara manuell, men den kan även vara automatisk och till exempel dokumentation på systemnivå för rollbaserade åtkomsträttigheter som grundar sig på användargrupper.<br>2. Tillsynsmyndigheten verifierar åtkomsträttigheterna i aktörens system och att de motsvarar dokumentationen. Detta kan göras till exempel genom ett slumpmässigt urval av användare eller vissa åtkomsträttigheter, såsom genom att kontrollera systemets huvudanvändarrättigheter eller andra förhöjda rättigheter. Åtkomsträttigheterna ska motsvara dokumentationen. Om man i systemet använder till exempel hantering av roll- eller användargruppsbaserade åtkomsträttigheter ska det förutom dessa inte finns beviljade odokumenterade åtkomsträttigheter som baserar sig på en användare. |
| **Motiveringar** |
| Extra användarnamn och åtkomsträttigheter kan ge en angripare åtkomst till systemet. Angriparen kan utnyttja odokumenterade eller glömda åtkomsträttigheter när hen navigerar från ett system till ett annat. Allt för omfattande åtkomsträttigheter kan möjliggöra även andra oönskade avslöjanden av uppgifter. |
| **Källor** |
| ISO/IEC 27002:2022 (5.15, 5.18, 8.3)<br>IEC 62443-2-1:2010 (4.3.3.7) |

| |
|---|
| IEC 62443-2-1:2024 (USER 1.4, USER 1.5) |
| IEC 62443-2-4:2024 (SP.03.08, SP.09.04) |
| NIST CSF 1.1 (PR.AC-4) |
| NIST CSF 2.0 (PR.AA-05) |
| NIS CG Reference document (3.7.2 Management of access rights) |
| NIS CG Reference document (3.7.3 Privileged and administration accounts) |
| NIS CG Implementing guidance (11.2. Management of access rights) |
| NIS CG Implementing guidance (11.3. Privileged accounts and system administra-tion accounts) |
| **Verktyg** |
| Julkri (HAL-14, TEK-07.2) |
| Cybermätaren (ACCESS-1, ACCESS-2, ACCESS-3, ARCHITECTURE-3) |

## 7.5 Huvudanvändarnamn

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkt 11.7 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har ett förfarande för att förhöjda rättigheter eller huvudanvändarrättigheter endast beviljas till befullmäktigade personer, enheter eller applikationer. Rättigheterna har beviljats till en så liten användargrupp som möjligt, men som möjliggör reservarrangemang. Dessutom har rättigheterna beviljats endast för den tid de är nödvändiga för att utföra arbetsuppgifterna. Detta gäller även till exempel underhållsarbete som utförs av en tredje part. Aktören har inkluderat riktlinjerna för huvudanvändarrättigheter i den eventuella riktlinjen för åtkomsthantering.<br>• Förhöjda rättigheter och huvudanvändarrättigheter har skyddats med starka metoder. Detta kan innebära till exempel starkare kontrollmetoder, flera kontrollmetoder eller ett tillräckligt skydd av kontrollmetoderna.<br>• När behoven ändras har extra rättigheter genast tagits bort.<br>• Användningen av förhöjda rättigheter och huvudanvändarrättigheter har i mån av möjlighet övervakats. Detta kan innebära till exempel att funktioner gjorda med förhöjda rättigheter sammanställs i en övervakningslogg eller att det krävs flera personer för att utföra funktioner (two-man rule).<br>• Aktören har kunnat utarbeta en anvisning om användningen av förhöjda rättigheter och huvudanvändarnamn. Användarnamn med förhöjda rättigheter och huvudanvändarnamn ska inte användas till grundläggande funktioner och |

grundläggande användarnamn ska inte användas för funktioner med förhöjda rättigheter eller huvudanvändarfunktioner. Nödanvändarnamn används inte annat än av grundad anledning i nödsituationer. I fråga om nödanvändarnamn har man även säkerställt att de är tillgängliga i en nödsituation, men tillräckligt skyddade.

- Aktören har utarbetat förfaranden och anvisningar för säker användning av hanteringsnätet och hanteringsarbetsstationerna.

**Verifiering**

1. Tillsynsmyndigheten verifierar aktörens dokumentation om förfaranden i anknytning till användningen och upprätthållande av huvudanvändarnamn. Av dokumentationen framgår hanteringens livscykel av förhöjda rättigheter eller huvudanvändarrättigheter. I dokumentationen ska man ta ställning till beviljande av rättigheter, återkallande, deras övervakning, deras koppling till användarnamn eller användargrupper samt speciell praxis i anknytning till dem såsom differentiering från normala användarnamn. Tillsynsmyndigheten verifierar att aktören har förfaranden för att övervaka användningen av huvudanvändarrättigheter och att huvudanvändarnamnen skyddas med starka metoder.
2. Tillsynsmyndigheten verifierar genom inspektion att aktörens förhöjda rättigheter och huvudanvändarrättigheter samt användarnamnen eller användargrupperna i anknytning till dessa. Rättigheternas livscykel ska granskas och säkerställas att förhöjda rättigheter eller huvudanvändarrättigheter endast innehas av personer som har ett sakligt behov som grundar sig på arbetsuppgifterna. Tillsynsmyndigheten kan inspektera övervakningssystemet eller hur övervakningsprocessen genomförs, till exempel genom att undersöka övervakningssystemets skick eller intervjuer och genom att inspektera hur övervakningsprocessen verkställs.

   Tillsynsmyndigheten verifierar i systemet eller genom skärmdumpar att starka metoder (t.ex. MFA) används för huvudanvändarnamn. I fråga om nödanvändarnamn granskar man att de är tillgängliga i en nödsituation, men tillräckligt skyddade. I samband med inspektionen kan man säkerställa att nödanvändarnamn inte har använts annat än av grundad anledning i nödsituationer.

**Motiveringar**

Med förhöjda rättigheter och huvudanvändarrättigheter har man möjlighet att göra betydande ändringar i systemen. Missbruk av dem kan orsaka allvarliga dataläckage, kontinuitetsstörningar, ekonomiska förluster eller andra störningar i affärsverksamheten. De ska skyddas särskilt bra. Därför ska huvudanvändarnamn skyddas med starka metoder.

**Källor**

ISO/IEC 27002:2022 (5.15, 5.18, 5.37, 8.2, 8.18)

IEC 62443-2-1:2010 (4.3.3.6.3, 4.3.3.6.4)

| |
|---|
| IEC 62443-2-1:2024 (USER 1.4, USER 1.5, USER 2.3, USER 2.4, ORG 1.1) |
| IEC 62443-2-4:2024 (SP.03.08, SP.09.04) |
| NIST CSF 1.1 (PR.AC-4) |
| NIST CSF 2.0 (PR.AA-05) |
| NIS CG Reference document (3.7.3 Privileged and administration accounts) |
| NIS CG Reference document (3.7.4 Administration systems) |
| NIS CG Implementing guidance (11.3. Privileged accounts and system administration accounts) |
| NIS CG Implementing guidance (11.4. Administration systems) |
| **Verktyg** |
| Julkri (TEK-04, TEK-07, HAL-14) |
| Cybermätaren (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3) |

## 7.6 Val av säkra kontrollmetoder och tillförlitlig autentisering

| **Exempel på genomförande** |
|---|
| • Aktören har använt endast kontrollmetoder som är tillräckligt säkra med beaktande av objektets säkerhetsbehov.<br>• Aktören har använt multifaktorautentisering i enlighet med sin riskbedömning och systemets förmåga. Aktören har som kontrollmetod använt till exempel multifaktorautentisering (MFA), kontinuerlig autentisering, stark autentisering (mobilcertifikat, bankkoder, medborgarcertifikat) eller motsvarande, om dessa har kunnat användas. Multifaktorsautentisering bör användas särskilt i administratör-ID och underhållssystem.<br>• Aktören har sett till att konfidentiella uppgifter såsom lösenord i anknytning till kontrollmetoderna förblir hemliga. Det är vanligt att till exempel lösenord ska ändras i samband med första inloggningen. När användarnamn skapas och levereras ska användaren identifieras på ett tillförlitligt sätt. När lösenord skapas har man undvikit till exempel svaga och förutsägbara lösenord. Ett undantag kan vara situationer när kortvarig användning av ett förutsägbart lösenord är motiverat, till exempel vid första inloggningen för en ny anställd eller nollställning av ett lösenord. I punkt 3.3 Systemhärdningar finns preciserad information om skydd av lösenord.<br>• Om möjligt har användarna identifierats individuellt och till exempel användningen av gemensamma användarnamn har undvikits. Om aktören inte kan undvika användningen av gemensamma användarnamn ska kontrollmetoderna vara tillräckligt säkra.<br>• Det finns en logg över kontrollmetoder på tillräcklig nivå och incidenter som upptäckts i loggen såsom uttröttningsangrepp och att man har reagerat till |

exempel genom att fördröja inloggningen till det utsatta användarkontot. Närmare information om praxis för loggar finns i punkt 7.4 Dokumentering av åtkomsthantering och 9.3 Dokumentering och observation av händelser.

- Systemets interaktiva inloggningssessioner bör avbrytas efter en på förhand fastställd tid.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har dokumentation över kontrollmetoderna för sina system. Dessa omfattar till exempel praxis för lösenord, systemspecifika specialdefinitioner och kontrollmetodernas hemligheter, såsom tillvägagångssätt för lösenord och distributionen av dem. Tillsynsmyndigheten inspekterar aktörens förfaranden i dokumenten om användningen av tillförlitlig autentisering (t.ex. MFA).
2. Tillsynsmyndigheten verifierar genom skärmdumpar eller inspektion i systemet att aktören har i bruk dokumenterade kontrollmetoder. Användningen av kontrollmetoder är täckande i olika system och har definierats för olika användargrupper. Av skärmdumpar eller inspektion av systemet framgår användningen av tillförlitlig autentisering och den valda kontrollmetoden.

**Motiveringar**

Användarnamn och kontrollmetoder är utsatta för ett betydande antal intrångsförsök i synnerhet i den öppna delen av det offentliga kommunikationsnätet och därför är deras säkerhet viktig. Även kontrollmetoder för system i det interna kommunikationsnätet ska väljas omsorgsfullt och inte bibehålla standardanvändarnamn eller standardlösenord. Tillförlitliga kontrollmetoder ökar säkerheten i systemen de använder genom att särskilt skydda dem mot nätfiske.

**Källor**

ISO/IEC 27002:2022 (8.5)

IEC 62443-2-1:2010 (4.3.3.6.1, 4.3.3.6.3)

IEC 62443-2-1:2024 (USER 1.8, USER 1.9, USER 1.11, USER 1.12, USER 2.3)

IEC 62443-2-4:2024 (SP.09.05, SP.09.06, SP.09.07, SP.09.08, SP.09.09)

NIST CSF 1.1 (PR.AC-7)

NIST CSF 2.0 (PR.AA-03)

NIS CG Reference document (3.7.5 Identification)

NIS CG Reference document (3.7.6 Authentication)

NIS CG Reference document (3.7.7 Multi-factor authentication)

NIS CG Implementing guidance (11.5. Identification)

NIS CG Implementing guidance (11.6. Authentication)

| NIS CG Implementing guidance (11.7. Multi-factor authentication) |
| --- |
| **Verktyg** |
| Julkri (TEK-04, TEK-08)<br>Cybermätaren (ACCESS-1, SITUATION-1) |

# 8 Riktlinjer och förfaranden för användning av krypteringsmetoder samt vid behov åtgärder för användning av säker elektronisk kommunikation

Rekommendationerna grundar sig på artikel 21.2 h och delvis på j i NIS 2-direktivet. Nationellt genomförande av dessa föreskrivs i 9 § 2 mom. 8 punkten i cybersäkerhetslagen och 18 c § 1 mom. 8 punkten i informationshanteringslagen.

1. **Riktlinjer och förfaranden för kryptografi:** Aktören ska fastställa riktlinjer och förfaranden för kryptografi för att vid behov skydda informationens konfidentialitet, äkthet och riktighet. (Se punkt 8.1).

2. **Krypteringsteknik för information:** Det kan vara nödvändigt att kryptera information t.ex. om den överförs i ett öppet datanät eller förvaras utan tillräckligt fysiskt skydd. Aktören ska då välja en krypteringsteknik vars skyddsnivå är tillräcklig med tanke på den krypterade informationens art, krypteringsklassificering, skyddstid och prestandakrav. När det gäller krypteringsteknik ska man utöver algoritmer, användningssätt och nyckelstyrka också beakta åtkomsten till och säker förvaring, generering och hantering av nycklar. (Se punkt 8.2).

3. **Krypteringens livscykel:** Kraven på krypteringsmetoden ska vara uppdaterade under hela systemets livscykel, så att t.ex. krypteringsalgoritmen kan bytas ut (kryptoagilitet). (Se punkt 8.3).

## 8.1 Riktlinjer och förfaranden för kryptografi

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkt 11.8 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har identifierat de uppgifter som kräver kryptografiskt skydd som en del av riskhanteringen.<br>• Aktören har fastställt riktlinjer för kryptografi, såsom krypteringsprodukter som ska användas vid överföring och förvaring av information. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har identifierat och klassificerat tillgångar som ska skyddas med kryptografiska metoder för att säkerställa deras konfidentialitet (t.ex. kryptering), äkthet (t.ex. underskrift) och integritet (t.ex. hashvärde). Dokumentationen beskriver även riktlinjerna i anknytning till kryptografi, vilket kan innebära till exempel definierande av tillåtna krypteringsprodukter och eventuella konfigurationer som hänför sig till dem. |

| **Motiveringar** |
|---|
| Kryptering av information kan förhindra att den hamnar i en form som kan läsas av en obehörig person. Numera är kryptering av information relativt enkelt i flera system. Till exempel kryptering av nättrafiken är numera en vanlig åtgärd. De flesta operativsystem tillhandahåller likaså kryptering av hårddiskarna med endast några klick. Genom kryptografiska metoder kan man även säkerställa att informationen inte har förändrats oavsiktligt eller avsiktligt och att informationen härrör från rätt källa. Med dessa metoder kan man till exempel försöka förhindra att skadligt material kommer in i informationssystem och försäkra sig om att den lagrade informationen inte är korrumperad. |
| **Källor** |
| ISO/IEC 27002:2022 (5.31, 5.37, 8.24)<br>IEC 62443-2-1:2024 (ORG 1.1, DATA 1.5, DATA 1.6)<br>IEC 62443-3-3:2013 (SR 4.3)<br>NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.PT-4)<br>NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.IR-01, PR.AA-06)<br>NIS CG Reference document (3.10.1 Policies and procedures on cryptography)<br>NIS CG Implementing guidance (9. Cryptography) |
| **Verktyg** |
| Julkri (TEK-16)<br>Cybermätaren (ARCHITECTURE-5) |

## 8.2 Krypteringsteknik för information

| **Exempel på genomförande** |
|---|
| • Förfaranden som gäller aktörens kryptografi definierar de protokoll som används och till exempel krypteringsalgoritmer, krypteringsstyrkor och krypteringsprodukter.<br>• Förfaranden och funktionssätt som gäller kryptografi står i proportion till skyddsbehovet, såsom klassificering och förvaringstid samt prestationskraven.<br>• Aktören har definierat hanteringen av kryptografiska nycklar (inklusive certifikat och motsvarande), så att den stöder krypteringsbehoven. Frågor att beakta är bland annat: |

- Att sörja för nycklarnas tillgänglighet, som inbegriper bland annat distribution och säkerhetskopiering av nycklar.
- Hantering av nycklarnas livscykel såsom skapande, byte, förvaring, urbruktagande och eliminering.
- Nycklarnas tekniska egenskaper såsom längd, rättigheter och livslängd.
- Urbruktagande av riskfyllda nycklar (spärrning) samt
- Dokumentering av nycklar i anknytning till händelser

**Verifiering**

1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har definierat förfaranden och funktionssätt som gäller kryptografi så att de står i rätt proportion till behoven att skydda informationen. Aktören har identifierat de fall där information överförs eller lagras utan tillräckligt skydd och för vilka det är nödvändigt att använda kryptering. Aktören har valt en krypteringsteknik vars skyddsnivå är tillräcklig med tanke på den krypterade informationens art, krypteringsklassificering, skyddstid och prestandakrav. Detaljer som granskas är algoritmer som används för krypteringen som ska vara tillräckliga med tanke på skyddskraven, krypteringens användningssätt och nycklarnas styrka. När det gäller nycklar är deras livslängd och till exempel komplexitet (särskilt symmetriska nycklar, delade nycklar det vill säga PSK, Pre-Shared Key) ska man beakta hanteringen av nycklarna. Frågor som ska beaktas i hanteringen av nycklar är till exempel deras säkra förvaring, tillgänglighet, säker generering och hantering av livscykeln. Genereringen kan kontrolleras till exempel genom att nycklarna genereras i ett säkert och vanligen isolerat objekt så att deras slumpmässighet (entropi) är tillräcklig. I hanteringen av livscykeln ska man bland annat beakta detaljer som eliminering och förnyande av en nyckel.
2. Tillsynsmyndigheten verifierar till exempel genom intervjuer och konfigurationsgranskningar att riktlinjerna för de definierade kryptografiska metoderna verkställs. Detta kan till exempel genomföras genom att granska tjänster som använder kryptering och definitioner i anknytning till deras kryptering, såsom algoritmer, praxis för skapandet av nycklar och säker förvaring av nycklar.
3. Tillsynsmyndigheten verifierar användningen av tillräcklig kryptering till exempel genom att skanna tjänster, system eller program som producerar krypterad trafik. Med hjälp av dessa skanningsprogram kan man till exempel granska krypteringsalgoritmer som tjänsten behöver för att trafikera. De använda algoritmerna ska överensstämma med definitionerna. Dessutom kan nycklarnas (speciellt certifikatens) giltighetstid granskas i enlighet med allmänt känd god praxis.

**Motiveringar**

Krypteringens effektivitet grundar sig nästan helt på valda krypteringsalgoritmer och i synnerhet hanteringen av nycklar. Svaga krypteringar är lätta att knäcka. En riskfylld eller svag nyckel kan förstöra nyttan av hela krypteringen. Om nyckeln inte elimineras på ett tillförlitligt sätt och den hamnar i fel händer kan man

| |
|---|
| använda den för att dekryptera alla trafik som krypterats med den. Krypteringsnyckelns tillgänglighet är också lika viktig så att den krypterade informationen är tillgänglig när den behövs. |
| **Källor** |
| ISO/IEC 27002:2022 (8.24)<br>IEC 62443-2-1:2024 (DATA 1.5, DATA 1.6)<br>IEC 62443-3-3:2013 (SR 1.8, SR 1.9, SR 3.1, SR 4.1, SR 4.3)<br>NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.PT-4)<br>NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.IR-01, PR.AA-06)<br>NIS CG Reference document (3.10.1 Policies and procedures on cryptography)<br>NIS CG Implementing guidance (9. Cryptography)<br>CISA: Quantum-Readiness: Migration to Post-Quantum Cryptography<br>On the State of Crypto-Agility |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-04.2, TEK-05.1, TEK-16)<br>Cybermätaren (ARCHITECTURE-5)<br>Skanningsprogram: Nessus, nmap, sslscan |

## 8.3 Krypteringens livscykel

| |
|---|
| **Exempel på genomförande** |
| • Aktören har upprätthållit de valda krypteringsteknikerna så att svaga krypteringstekniker vid behov har bytts ut mot nya och starkare alternativ. I framtiden kommer det att framgå särskilt i ibruktagande av PQC-kryptering (Post-Quantum Cryptography).<br>• Aktören har genomfört arrangemang i anknytning till krypteringar så att byte av kryptering och krypteringsnycklar kan göras så enkelt som möjligt. Detta innebär till exempel ändring av tjänsternas konfigurationer till nyare starkare krypteringstekniker, hantering av certifikatens livscykel, användning av nycklar i tjänster och produkter såt att byte av nycklarna är möjligt utan dessvärre besvär. |
| **Verifiering** |

1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har genomfört sina krypteringsmetoder och kryptografiska metoder så att till exempel byte av krypteringsalgoritmer och nycklar kan genomföras utan större besvär. Möjligheten till byte av krypteringsalgoritmer och nycklar kan även ingå i upphandlingsprocessen, till exempel i aktörens krav i anknytning till val av produkter.
2. Tillsynsmyndigheten verifierar genom inspektion av till exempel konfigurationen att de kryptografiska arrangemangen stöder hanteringen av livscykeln. Detta innebär till exempel att parametrar i anknytning till kryptografin till exempel inte är hårdkodade i programmen, utan de kan hanteras till exempel genom konfigurationsfiler.

**Motiveringar**

När beräkningskapaciteten ökar och algoritmer knäcks hamnar krypteringsmetoderna i ett tillstånd när det till och med kan vara trivialt att knäcka dem. Därför ska en ändring av krypteringsparametrar vara så enkel som möjligt att göra. I framtiden kan även utvecklingen av kvantdatorer leda till ett förändringstryck för de krypteringar som används. Detta ska särskilt beaktas i system som har en lång livscykel eller höga säkerhetsbehov.

Certifikatens livslängd är begränsad. Å andra sidan kan krypteringsnycklar ibland av misstag eller avsiktligt äventyras. Därför ska även byte av nycklar vara så enkelt att krypteringens effekt inte försämras på grund av nyckelns svaghet.

**Källor**

ISO/IEC 27002:2022 (8.24)

IEC 62443-2-1:2024 (DATA 1.5, DATA 1.6)

IEC 62443-3-3:2013 (SR 4.3)

NIST CSF 2.0 (ID.AM-08, PR.PS-06)

NIS CG Reference document (3.10.1 Policies and procedures on cryptography)

NIS CG Implementing guidance (9. Cryptography)

**Verktyg**

Julkri (TEK-16)

Cybermätaren (ARCHITECTURE-5)

# 9 Upptäckande och hantering av incidenter i syfte att återställa och upprätthålla säkerheten och driftsäkerheten

Rekommendationerna grundar sig på artikel 21.2 b i NIS 2-direktivet. Om nationellt genomförande av denna föreskrivs i 9 § 2 mom. 9 punkten i cybersäkerhetslagen och 18 c § 1 mom. 9 punkten i informationshanteringslagen.

1. **Förfaranden för incidenthantering:** För att hantera incidenter ska aktören ha på förhand dokumenterade förfaranden, roller och ansvar för att förebygga, upptäcka, analysera, hantera och rapportera incidenter samt för att återställa läget efter incidenter. (Se punkt 9.1).

2. **Rapporteringskanaler för incidenter:** För att upptäcka incidenter ska aktören ha rapporteringskanaler till interna och externa aktörer. (Se punkt 9.2).

3. **Registrering och upptäckande av händelser:** Aktören ska i princip ha verktyg och processer för att upptäcka och registrera händelserna. Med tanke på observations- och analysförmågan är det nödvändigt att aktören har tillgång till tillräckliga logguppgifter om t.ex. underhåll, ändringar, användning och fel. (Se punkt 9.3).

4. **Analys och klassificering av incidenten:** Aktören ska exempelvis bedöma relevanta händelser för att utreda om de kan orsaka en incident. Aktören ska ha rutiner för bedömning och vid behov klassificering av incidentens allvarlighetsgrad och konsekvenser. (Se punkt 9.4).

5. **Hantering av en incident:** Vid hanteringen av en incident ska det också finnas praxis för att reagera på den samt vid behov för att begränsa och utreda den och eliminera dess konsekvenser. (Se punkt 9.5).

6. **Analys av grundorsaken och lärdom av erfarenheter**: Efter en incident ska man försöka utvärdera orsakerna till den och lära sig av erfarenheterna, så att man i fortsättningen bättre kan förbereda sig på risken för en liknande incident. (Se punkt 9.6).

7. **Kompletterande rekommendationer för betydande incidenter:** För betydande incidenter ska det finnas förfaranden, ansvar och kommunikationskanaler för att varna andra aktörer. (Se punkt 9.7).

8. **Säkerhet vid spridning av information:** Incidenthanteringen ska också inbegripa förfaranden för spridning av information, så att incidenten inte utsätter aktören eller någon annan organisation för risk. (Se punkt 9.8).

9. **Hantering av incidenthanteringens livscykel:** Förfarandena för hantering av incidenter ska upprätthållas och utvecklas under hela livscykeln, och de ska uppdateras till exempel utifrån erfarenheterna. (Se punkt 9.9).

## 9.1 Förfaranden för incidenthantering:

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkt 11.12 om grundläggande praxis för informationssäkerhet.<br><br>• Aktören har omfattande förfaranden för incidenthantering och vid behov en riktlinje som beskriver åtgärder för hantering av incidenter. Åtgärder är till exempel i syfte att förebygga, upptäcka, analysera, hantera och att återhämta sig från en incident. Förfaranden för incidenthantering kan vid behov hänvisa till andra dokument om de beskriver det väsentliga innehållet. Förebyggande av incidenter kan till exempel hänvisa till handlingsmodellen för hantering av cybersäkerhetsrisker och åtgärder för riskhantering.<br>• Förfaranden för incidenthantering inbegriper de roller och kanaler för rapportering och kommunikation som behövs. Det rekommenderas att göra upp en kommunikationsplan för kommunikation under en incident så att den nödvändiga interna och externa kommunikationen har bestämts på förhand. Dessutom beskriver förfaranden åtgärder i anknytning till hanteringen såsom klassificering (kategorisering) av incidenter, åtgärder i anknytning till allvarliga störningssituationer och rapportering. Mer om roller som gäller säkerhet i punkt 6.1 Förfaranden för personalsäkerheten.<br>• Förfaranden för incidenthantering inbegriper tillräcklig dokumentering som beskriver verksamheten under hanteringen av incidenten. Detta kan till exempel innebära åtgärder och resurser i anknytning till utredningen av en incident.<br>• I synnerhet efter allvarliga incidenter kan det vara till nytta ordna ett möte för genomgång för de personer som deltagit i hanteringen av incidenten. På det sättet kan man i bästa fall undvika motsvarande incidenter i framtiden och förbättra verksamheten vid incidenter. Åtgärden främjar även utarbetandet av slutrapporten i anknytning till NIS 2-incidentanmälan.<br>• Aktören kan till exempel utarbeta följande anvisningar för incidenthantering:<br>  ○ Spelböcker för incidenthantering<br>  ○ Anvisningar och tabeller i anknytning till eskalering<br>  ○ Kontaktlistor<br>  ○ Mallar<br>• Förfaranden för incidenthantering beskriver förhållandet mellan kontinuiteten (kontinuitetsplan, Business Continuity Plan, BCP) och incidenthanteringen. Incidenthanteringen beskriver också åtgärder i anknytning till återhämtning. Det är ofta ett separat dokument (återhämtningsplan, Disaster Recovery Plan, DRP).<br>• Förfaranden för incidenthantering beskriver juridiska krav i incidenthanteringen. |
| **Verifiering** |

1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har förfaranden i anknytning till incidenthantering. Dessa är skriftliga och placerade på en plats så att de är tillgängliga vid en incident. Utöver förfarandena har aktören roller och ansvar för olika skeden i incidenthanteringen. Dessa är att förebygga, upptäcka, analysera, hantera, återhämta sig från och rapportering av incidenter. Innehållet i förfarandena kan bestå till exempel av 1 Riktlinjer för riskhantering, 9 Upptäckande och hantering av incidenter och delvis punkt 10 Säkerhetskopiering, återhämtning från de beskrivna sakerna:
   - Förebyggande av incidenter. Förebyggande av incidenter kan till exempel hänvisa till handlingsmodellen för hantering av cybersäkerhetsrisker och riskhanteringsåtgärder (se 1).
   - Upptäckande av incidenter. Metoder som beskriver förfaranden för upptäckande av incidenter. Dessa kan till exempel vara system för upptäckande eller kommunikationskanaler (se 9.3).
   - Analys av incidenter. Det är bra att ha klassificeringskriterier för analys av incidenter, som grundar sig till exempel på direkta och indirekta konsekvenser, omfattning, tid och resurser. Vid behov kan analysen även beskriva mer tekniska förfaranden (se 9.4).
   - Hantering av incidenter och återhämtning. I dessa kan man använda behövliga preciserande dokument eller delar, såsom kommunikationsplanen samt kopplingar i anknytning till kontinuitet och återhämtning (BCP, DRP) (se 10.1).
   - Rapporteringskanaler för incidenter (se 9.2).
   - Interna roller och ansvar. Roller under incidenthanteringen som inbegriper till exempel intern och extern kommunikation (se 2.2 och 9.7), personalresurser och ledning som behövs för att utreda incidenten. Detta kan genomföras till exempel med en (kris)grupp som bildas i enlighet med en överenskommen process.
   - I förfarandet är det även bra att beskriva krav i lagstiftningen. Dessa är till exempel NIS-anmälningar och anmälningsskyldigheter i anknytning till dataskyddskränkningar och förfaranden som dessa medför.
2. Dessutom kan tillsynsmyndigheten genom att använda händelseloggar, tickets, intervjuer och motsvarande källor kontrollera att förfaranden iakttas.

**Motiveringar**

Förfaranden för incidenthantering är en väsentlig del av beredskapen. En välplanerad verksamhet under en incident kan göra hanteringen av den snabbare och smidigare samt å andra sidan hjälpa i klassificeringen av incidenterna, varvid reaktionen blir proportionerlig.

Kommunikationsplanen som en del av rollerna är ett centralt verktyg vid många incidenter. Den säkerställer informationsgången till rätt personer och förhindrar å andra sidan överflödig kommunikation som förvärrar situationen, till exempel flera rapporter om samma incident.

| Källor |
|---|
| ISO/IEC 27002:2022 (5.24, 5.30) |
| ISO/IEC 27035-1:2023 (4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7.1, 5.1, 5.2) |
| ISO/IEC 27035-2:2023 (4.3, 6.2, 6.4, 6.7, 7) |
| IEC 62443-2-1:2010 (4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4) |
| IEC 62443-2-1:2024 (EVENT 1.1, EVENT 1.8) |
| IEC 62443-2-4:2024 (SP.08.01, SP.08.02, SP.08.03) |
| NIST CSF 1.1 (RS.RP-1, RS.CO-1, RS.IM-2) |
| NIST CSF 2.0 (GV.SC-08, RS.MA-01, PR.AT-01, ID.IM-03) |
| NIST SP 800-61 rev 2 (2.1, 2.2, 2.3, 2.4, 2.5, 3.1) |
| NIS CG Reference document (3.11.1 Incident handling policy) |
| NIS CG Implementing guidance (3.1 Incident handling policy) |
| **Verktyg** |
| Julkri (HAL-08) |
| Cybermätaren (CRITICAL-3, RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-4, RESPONSE-5) |

## 9.2 Rapporteringskanaler för incidenter

| Exempel på genomförande |
|---|
| • Aktören har en rapporteringskanal där personalen, journalister, sårbarhetsutredare, myndigheter och kunder kan rapportera incidenter, misstänkta incidenter, sårbarheter och andra motsvarande observationer.<br>• Aktören ska se till att personalen är medveten om rapporteringskanalen. Dessutom ska externa aktörer informeras om rapporteringskanalerna.<br>• Vid behov ska rapporteringskanalen vara konfidentiell. Personer som behandlar rapporterna är medvetna om praxis för hantering av rapporter. Detta gäller i synnerhet när de innehåller till exempel personuppgifter eller annan information vars behandling är förenad med lagstadgade skyldigheter.<br>• Vid bestämmande av rapporteringskanaler är det även bra att beakta situationer när de normala rapporteringskanalerna kan vara riskfyllda på grund av en incident. Det viktigaste är att identifiera en sådan möjlighet och skapa en reservplan eller alternativa oberoende kanaler för sådana situationer. |
| **Verifiering** |

1. Tillsynsmyndigheten verifierar att aktören har rapporteringskanaler som är tillgängliga till exempel för personalen, journalister, sårbarhetsutredare, myndigheter och kunder. Rapporteringskanalerna har genomförts så de vid behov är lätta att hitta och användningen av dem vid behov är oförhindrad. Rapporteringskanalerna ska beakta situationer när rapporteringskanalen kan vara utsatt för risk. Till exempel e-post kan inte användas när en angripare eventuellt hanterar e-posttjänsten (se 10.4).
2. Vid behov kan rapporteringskanalernas funktion testas till exempel genom att aktören gör en exempelrapport via kanalerna och tillsynsmyndigheten följer upp hanteringen av rapporten.

**Motiveringar**

**Källor**

ISO/IEC 27002:2022 (6.8)

ISO/IEC 27035-1:2023 (4.7.2, 5.2)

IEC 62443-2-1:2010 (4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5)

IEC 62443-2-1:2024 (EVENT 1.2, EVENT 1.3, EVENT 1.8, EVENT 1.9, ORG 1.1)

IEC 62443-2-4:2024 (SP.03.03, SP.08.01)

NIST CSF 1.1 (RS.CO-1, RS.CO-2)

NIST CSF 2.0 (PR.AT-01, DE.AE-07, RS.CO-02)

NIST SP 800-61 rev 2 (3.1.1)

NIS CG Reference document (3.11.3 Event reporting)

NIS CG Implementing guidance (3.3. Event reporting)

**Verktyg**

Cybermätaren (RESPONSE-1, WORKFORCE-2)

## 9.3 Registrering och upptäckande av händelser

**Exempel på genomförande**

Denna punkt kompletterar punkt 11.13 om grundläggande praxis för informationssäkerhet.

- Aktören har processer och verktyg för att upptäcka incidenter. Dessutom har aktören förmåga att upptäcka händelser som påverkar säkerheten och hantera dem enligt hur kritiska de är.
- Aktören har sammanställt en logg med tillräcklig omfattning och med noggrannhet över sina kommunikationsnät och informationssystem. För att åstadkomma en heltäckande observationsförmåga har logguppgifter i mån av möjlighet samlats in till exempel av följande händelser:
  - Utgående och inkommande nättrafik
  - Skapande av användare, ändring och eliminering samt att lägga till åtkomsträttigheter
  - Händelser i anknytning till åtkomsthantering för system och applikationer
  - Huvudanvändaråtgärder eller åtgärder gjorda med förhöjda rättigheter i system, tjänster och program
  - Hantering av konfigurationer och säkerhetskopierade filer som är väsentliga för verksamheten eller säkerheten, inklusive läsning, ändringar och eliminering
  - Logg som produceras av system och applikationer i anknytning till säkerheten (t.ex. endpoint detection and response EDR, intrångsdetektionssystem/intrusion detection system IDS, brandvägg, fjärråtkomstpunkter)
  - Användning av systemets resurser och prestanda
  - Vid behov funktioner i anknytning till åtkomst eller användning (t.ex. passerkontroll)
  - Åtkomst till och användning av nätverks- och kommunikationsutrustning
  - Vid behov händelser i anknytning till miljön (t.ex. omständighetslarm)
  - Loggkällan och ändring som gäller dess säkerhet såsom start, avstängning och avbrott
- Via loggarna har man upptäckt händelser som avviker från det normala eller är icke-önskade. Övervakningen är så automatisk som möjligt, dock genom att beakta behovet av riskhantering och resurser. Om möjligt skapas larm automatiskt om observationer. Trender kan också följas i analytiken. Vid behov kan automatiken ersättas till exempel med regelbundna inspektioner. Det finns en process och resurser för hantering av larm. Vid behov kan aktören utnyttja typiska lösningar i form av en nätverksövervakningscentral (network operations center, NOC) eller säkerhetskontrollrum (security operations center, SOC).
- Logguppgifterna ska bevaras tillräcklig länge och de ska i mån av möjlighet och vid behov säkerhetskopieras. Förvaringstiden kan till exempel bero på behov som grundar sig på lagstiftning, straffrätt eller riskhantering. Till exempel sex månader kan vara tillräcklig för riskhanteringen i fråga om mindre kritiska logguppgifter, medan till exempel det straffrättsliga behovet kan förutsätta en förvaringstid på flera år.
- I första hand ska logguppgifterna överföras till en separat enhet som är isolerad från det övriga systemet. Dessutom har aktören genomfört differentiering av uppgifter så att en person som har tillgång till loggservern inte får tillgång

till loggkällorna (och tvärtom). Med sådana åtgärder är det för det mesta möjligt att undvika förstöring av bevis i missbruksfall. Om differentiering av uppgifterna inte är möjligt till exempel på grund av resursorsaker har aktören vidtagit tillräckliga ersättande åtgärder för att minska risken.

- Aktören har en pålitlig centraliserad tidkälla och alla loggkällor ska konfigureras så att loggarnas tidsstämplar kan kombineras.
- Aktören har upprätthållit en uppdaterad lista över olika loggkällor, källornas läge samt hur övervakningen fungerar och tillgängligheten har granskats regelbundet.
- Hanteringen och förvaringen av logguppgifter beaktar eventuella krav som hänför sig till lagstiftning eller reglering. Tillräckligt förvaringsutrymme har reserverats för loggarna och i allmänhet larm om att lagringsutrymmet håller på att fyllas.
- I fråga om logguppgifter och observationer har man beaktat händelser i anknytning till den fysiska säkerheten, i synnerhet när den fysiska säkerheten producerar metoder för hantering av cybersäkerhetsrisker.

**Verifiering**

1. Tillsynsmyndigheten verifierar registreringen av händelser och observationsförmågan genom att utnyttja befintlig dokumentation. Sådan dokumentation kan till exempel vara loggpolicy, loggkällor och beskrivningar av logginnehållet, lagstadgade skyldigheter som gäller loggen och övervakning, beskrivningar av övervakningssystem, beskrivningar av övervakningsprocesser och beskrivningar av loggsystemet. Dessutom kan man be om skärmdumpar eller stickprov av logg- och övervakningssystem av vilka systemets funktion och omfattning framgår med beaktande av urvalets storlek (se Genomförandeexempel). Hanteringen av observationer som gjorts utifrån loggarna kan kontrolleras till exempel i hanteringshistoriken, genom intervjuer och övervakningsvyer.
2. Läget i logg- och övervakningssystem kan kontrolleras genom att vid behov med aktörens hjälp undersöka systemens konfigurationer och övervakningsvyer. Det går även att använda intervjuer. Beroende på kommunikationsnätens och informationssystemens storlek kan konfigurationerna i anknytning till sammanställande av logguppgifter för enheter, tjänster och andra resurser gås igenom antingen genom stickprov eller i sin helhet. Urvalet ska minst omfatta enheter (t.ex. brandvägg, fjärråtkomstpunkt, krypteringsapparat) som finns vid kommunikationsnätets och informationssystemets yttermarginal, de viktigaste resurserna med tanke på verksamheten och säkerheten samt kritiska tillgångar som har plockats ur riskhanteringen och tillgångsförteckningen. I urvalet ska också inkluderas ett urval av andra objekt för att få en tillräcklig täckning. När det gäller loggarna som valts ut för urvalet kontrolleras att loggar skapas från alla centrala system (se ovan Exempel på genomförande), att deras innehåll är täckande med tanke på aktörens behov, tidsstämplar är enhetliga, att loggarna överförs till loggsystemet och att loggarna förvaras tillräckligt länge och att tillräckligt förvaringsutrymme har reserverats för dem. Förvaringstiden ska vara proportionerlig till exempel i anknyt-

ning till lagstiftningsmässiga, straffrättsliga och riskhanteringsrelaterade behov. Förvaringstiden kan variera från ett system till ett annat och kan vara flera år. Observationsförmågan av loggkällornas funktion kan inspekteras till exempel genom att i övervakningssystemet granska de regler som finns för detta ändamål. Händelsedokumentering som till exempel görs manuellt kan granskas genom inspektion. I inspektioner och observationer av incidenter som hänför sig till dessa kan man använda intervjuer och eventuella andra uppgifter, såsom tickets i anknytning till incidenter.

3. Logg- och observationsförmågan kan testas till exempel genom att följa upp producerade larm. I fråga om detta kan man ta hjälp till exempel av aktörens underhållspersonal eller informationssäkerhetstestare. I testningen kan man simulera olika situationer som avviker från det normala och följa upp hur händelsen registreras i loggen samt säkerställa att händelsen framkallar ett larm. Den simulerade händelsen kan till exempel vara ett misslyckat inloggningsförsök, användning av underhållsanvändarnamn, försök att köra olovlig men säker programvara eller införande av EICAR-testvirusfiler i systemet. Vid testningar ska man dock försäkra sig om att de inte utgör ett hot mot systemet. Eventuella extra användarnamn, filer och åtkomsträttigheter ska tas bort efter testet.

## Motiveringar

Förmågan att upptäcka incidenter är viktig för att eventuella cyberhot ska identifieras i ett så tidigt skede som möjligt. Registrering av händelserna gör att de kan analyseras efteråt och utan en täckande logg är det för det mesta inte möjligt att utreda de grundläggande orsakerna till incidenten.

Det lönar sig att differentiera loggsystem och övervakning från andra system, också när det gäller personroller. Dessa system producerar i allmänhet bevis på att något skadligt har inträffat. Då är det viktigt att ingen kan förstöra bevisen. Vid behov kan dessa system även producera bevis på att till exempel underhållspersonalen inte har orsakat incidenten, fastän det finns misstanke om detta.

Det är vanligt att incidenter inte upptäcks i tid. Det kan ta lång tid innan man upptäcker att en angripare fått fotfäste. Av den orsaken är observationsförmågan viktig när den i bästa fall förhindrar en allvarlig incident.

## Källor

ISO/IEC 27002:2022 (5.24, 5.28, 8.15, 8.16, 8.17)

ISO/IEC 27035-1:2023 (4.7.3, 5.3)

IEC 62443-2-1:2010 (4.3.3.6.4)

IEC 62443-2-1:2024 (EVENT 1.4, EVENT 1.5, EVENT 1.8, DATA 1.1, NET 1.9)

IEC 62443-2-4:2024 (SP.03.04, SP.08.01, SP.08.02, SP.08.03)

IEC 62443-3-3:2013 (SR 1.11, SR 1.12, SR 1.13, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 6.1, SR 6.2)

NIST CSF 1.1 (DE.CM, RS.AN-1)

NIST CSF 2.0 (DE.AE-06, DE.CM, RS.MA-02, RS.AN-07)

NIST SP 800-61 rev 2 (3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.5)

NIS CG Reference document (3.11.2 Monitoring and logging)

NIS CG Reference document (3.11.4 Event assessment and classification)

NIS CG Reference document (3.11.5 Incident response)

NIS CG Implementing guidance (3.2. Monitoring and logging)

NIS CG Implementing guidance (3.4. Event assessment and classification)

NIS CG Implementing guidance (3.5. Incident response)

Transport- och kommunikationsverkets anvisning om dokumentation av uppgifter som gäller behandling av förmedlingsuppgifter (Traficom/376384/03.04.05.01/2022)

**Verktyg**

Kartläggning av angreppsytan Hyöky.fi

Julkri (TEK-12)

Cybermätaren (ACCESS-2, ACCESS-3, SITUATION-1, SITUATION-2, SITUATION-3)

För testning av incidenter: EICAR-testivirustiedosto https://www.eicar.org

## 9.4 Analys och klassificering av incidenter

**Exempel på genomförande**

- Aktören har i logguppgifterna identifierat incidenter i anknytning till säkerheten och analyserat incidenternas verkningar och allvarlighetsgrad till exempel utifrån kriterierna. Bedömningen av hur allvarlig incidenten är kan grunda sig till exempel på materiell eller immateriell skada som incidenten orsakar samt ekonomiska förluster, omfattningen av störningar i tjänsten, incidentens varaktighet och antalet tjänstemottagare som påverkas.
- Aktören har vid behov metoder för analys och korrelation av loggar, varvid incidenter bättre kan upptäckas. Aktören bör kunna omvärdera gamla incidenter i ljuset av den nya hotinformationen (se punkt 1.4).
- Vid behov har aktören ett system som analyserar och korrelerar logguppgifterna automatiskt och utnyttjar den erhållna informationen till exempel som en del i jakten på hot (threat hunting, threat intelligence).

## Verifiering

1. Tillsynsmyndigheten verifierar genomförandet av analys och klassificering av en incident till exempel i dokument som beskriver förfaranden för incidenthantering. Aktören har beskrivit förfaranden i anknytning till händelser. Aktören ska ha tydliga kriterier för att identifiera händelser som incidenter, klassificera incidenterna och bedöma om det är fråga om en betydande incident enligt cybersäkerhetslagen. Klassificeringen ska vara tydlig och grunda sig till exempel på lagstiftning och klassificeringar som härstammar från tillgångsförvaltningen. Klassificeringen görs från fall till fall, men bedömningen av hur allvarlig incidenten är kan grunda sig till exempel på materiell eller immateriell skada som incidenten orsakar samt ekonomiska förluster, omfattningen av störningar i tjänsten, incidentens varaktighet och antalet tjänstemottagare som påverkas. Hur förfarandena genomförs kan kontrolleras till exempel genom tickets och intervjuer. I fråga om detta kan man använda upptäckta incidenter och granska genomföranden i anknytning till dem.
2. Om aktören har behov och förmåga att automatiskt analysera och korrelera logguppgifter kan tillsynsmyndigheten till exempel i dokumentationen verifiera förfaranden och funktionssätt i anknytning till detta. Dessutom kan man inspektera funktionen hos systemet som utför analysen och jämförelsen samt experternas förmåga att utföra analyser. Genom intervjuer och till exempel ärendehanteringssystemet kan man kontrollera att analys och jämförelse har utförts och att den vid behov haft effekt. Detta kan framkomma till exempel i ändringar som fynden orsakat, som kan kontrolleras till exempel i loggen för ändringshantering.

## Motiveringar

Syftet med analys och klassificering av incidenter är att åtgärderna för incidenthantering ska vara så proportionerliga som möjligt. Detta innebär att till exempel extra att resurser av misstag inte används för att utreda incidenter med obetydlig inverkan och å andra sidan att betydande incidenter identifieras i tid för att hantera allvarliga konsekvenser.

Mer avancerade attacker kännetecknas ofta av att det första fotfästet sker betydligt tidigare än den egentliga skadan. För detta ändamål har vissa aktörer ett riskbaserat behov att analysera incidenter automatisk till exempel på basis av korrelation.

## Källor

ISO/IEC 27002:2022 (5.25)

ISO/IEC 27035-1:2023 (5.4)

ISO/IEC 27035-2:2023 (6.5, 6.6)

IEC 62443-2-1:2010 (4.3.4.5.6, 4.3.4.5.7)

| |
|---|
| IEC 62443-2-1:2024 (EVENT 1.7) |
| IEC 62443-2-4:2024 (SP.08.01) |
| NIST CSF 1.1 (DE.AE-4, RS.AN-2, RS.AN-4) |
| NIST CSF 2.0 (DE.AE-03, DE.AE-04, DE.AE-07, DE.AE-08, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-08) |
| NIST SP 800-61 rev 2 (3.2, 3.2.4, 3.2.6, 3.2.7) |
| NIS CG Reference document (3.11.4 Event assessment and classification) |
| NIS CG Implementing guidance (3.4. Event assessment and classification) |
| **Verktyg** |
| Julkri (TEK-13) |
| Cybermätaren (SITUATION-2, SITUATION-3) |

## 9.5 Hantering av en incident

| **Exempel på genomförande** |
|---|
| • Aktören har skriftliga förfaranden för hantering av incidenter. Förfarandena omfattar:<br>  ○ Praxis för att reagera på incidenter.<br>  ○ Åtgärder för att förhindra allvarliga konsekvenser som incidenten orsakar och att incidenten sprids.<br>  ○ Utredning av incidenten för att utreda och eliminera incidentens inverkan och upphov.<br>• Vid utredning av incidenter ska det säkerställas att incidenter i framtiden förhindras.<br>• Aktören har skapat förutsättningar för att hantera betydande incidenter (se 9.7) och vid behov anmäla lindrigare incidenter till den nationella CSIRT-enheten och/eller tillsynsmyndigheten.<br>• Hantering incidenten bör dokumenteras så detaljerat att det senare kan användas i anmälning (se 9.7) och att man kan lära sig av det (se 9.6). |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar till exempel i dokumentationen att aktören har förfaranden i anknytning till incidenthantering. Förfarandena beskriver praxis för att reagera på incidenter.<br>Praxis för att reagera på incidenter kan till exempel vara åtgärder i anknytning till incidenthantering, såsom åtgärder för att minimera incidentens konsekvenser och förhindra att incidenten sprids till exempel till andra aktörer |

och system. Av dokumentationen ska också framgå funktionssätt för att förhindra incidentens konsekvens och förekomst i fortsättningen. För att uppnå detta ska det av dokumentation framgå att incidenter utreds ingående och att aktören har tillräcklig kompetens eller anlitar en tredje part. Ovanstående ska granskas särskilt mot bakgrund av att de nya incidenterna kan bero på att den gamla incidenten inte tidigare har utretts tillräckligt. För att förhindra att konsekvensen av incidenten ökar och sprids ska aktören ha tillräckliga uppgifter om aktörer som kan påverkas av incidenten. Informationen till aktörerna som nämndes ovan ska vara snabb, tydlig och ansvaret delegerat (se 9.7). Dessutom ska till exempel skyldigheter i lagstiftningen beaktas. Dessa och ansvar som hänför sig till dem ska vara tydligt dokumenterade.

2. Tillsynsmyndigheten klarlägger hur förfarandena genomförs, om detta är möjligt. För detta kan man till exempel använda intervjuer, dokumentation som uppstått vid incidenthantering såsom tickets och loggen samt ändringar och kommunikation.

**Motiveringar**

**Källor**

ISO/IEC 27002:2022 (5.24, 5.25, 5.26, 5.37)

ISO/IEC 27035-1:2023 (4.7.4)

IEC 62443-2-1:2010 (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, 4.3.4.5.9, 4.3.4.5.10)

IEC 62443-2-1:2024 (EVENT 1.7, EVENT 1.8, ORG 1.1)

IEC 62443-2-4:2024 (SP.08.01)

NIST CSF 1.1 (PR.IP-9, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-3, RS.MI-1, RS.MI-2, RC.RP-1, RC.CO-1, RC.CO-2, RC.CO-3)

NIST CSF 2.0 (ID.IM-04, RS.MA-01, RS.MA-04, RS.CO-03, RS.AN-06, RS.MI-01, RS.MI-02, RC.RP-01, RC.CO-03, RC.CO-04)

NIST SP 800-61 rev 2 (3.3, 3.3.1, 3.3.2, 3.3.3, 3.3.4)

NIS CG Reference document (3.11.5 Incident response)

NIS CG Implementing guidance (3.5. Incident response)

**Verktyg**

Julkri (HAL-08, TEK-13)

Cybermätaren (CRITICAL-3, SITUATION-3, RESPONSE-3)

## 9.6 Analys av grundorsaken och lärdom av erfarenheter

| **Exempel på genomförande** |
|---|
| • I synnerhet efter en betydande incident inspekterar aktören incidenthanteringen. Det inbegriper till exempel omständigheter i anknytning till upptäckande, hantering och avgörande.<br>• Om aktören har upptäckt brister under hanteringen av incidenten har aktören förbättrat sina förfaranden, anvisningar och resurser, såsom förmågor eller kompetens. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har praxis för genomförande av analys av grundorsaken (root cause analysis, RCA) och lärdom av erfarenheter. Analys av grundorsaken och lärdom av erfarenheter har utnyttjats i dokumentationen. Åtgärderna för analys av grundorsaken ska vara beskrivna och ansvaret delegerat. Behövlig kompetens och resurser ska vara tillgängliga. Lärdom av erfarenhet ska utgöra en del av åtgärderna för incidenthantering.<br>2. Tillsynsmyndigheten verifierar en betydande incident i materialet som hänför sig till dess hantering och genom intervjuer. Syftet är att utreda om aktören har genomfört analys av grundorsaken och fått lärdom av erfarenheten. Lärdom av erfarenhet kan verifieras till exempel genom att inspektera att aktören har planerat eller genomfört korrigerande åtgärder efter incidenten. |
| **Motiveringar** |
| Syftet med analys av grundorsaken och lärdom av erfarenheter är att hitta praxis för att förebygga incidenter och agera bättre och effektivare vid incidenter i fortsättningen. Analys av grundorsaken är ett hjälpmedel för kraven i regleringen för att aktören kan utarbeta slutrapporten för NIS-anmälningen. |
| **Källor** |
| ISO/IEC 27002:2022 (5.27, 5.28)<br>ISO/IEC 27035-1:2023 (4.7.5, 9.6)<br>ISO/IEC 27035-2:2023 (9.6)<br>IEC 62443-2-1:2010 (4.3.4.5.8, 4.3.4.5.11)<br>IEC 62443-2-1:2024 (EVENT 1.4, EVENT 1.5, EVENT 1.7, EVENT 1.8, ORG 1.1)<br>NIST CSF 1.1 (DE.AE-2, RS.IM-1)<br>NIST CSF 2.0 (DE.AE-02, ID.IM-03, RS.AN-03)<br>NIST SP 800-61 rev 2 (3.4.1) |

| |
|---|
| NIS CG Reference document (3.11.6 Post-incident review)<br>NIS CG Implementing guidance (3.6. Post-incident review) |
| **Verktyg** |
| Cybermätaren (RESPONSE-3, RESPONSE-4) |

## 9.7 Kompletterande rekommendationer för betydande incidenter

| **Exempel på genomförande** |
|---|
| Denna punkt kompletterar punkt 11.12 om grundläggande praxis för informationssäkerhet.<br>• Förfaranden för incidenthantering inbegriper hantering av betydande incidenter. Aktören har med tanke på dessa bestämt roller och ansvar samt kommunikationskanaler till exempel till nödvändiga myndigheter.<br>• Aktören har beaktat eventuella branschspecifika preciseringar i fastställandet av betydande incidenter och tröskelvärden.<br>• Aktören har planerat uppföljningen av lägesutvecklingen för att identifiera en betydande incident och vidtar nödvändiga åtgärder i situationerna.<br>• Aktören har en kommunikationsplan och sätt att hålla kontakt med de aktörer som eventuellt påverkas av incidenten för att skydda dessa aktörer.<br>• Aktören har planerat metoder för att uppskatta ekonomiska förluster orsakade av incidenten och planerade handlingsmodeller för situationer där de ekonomiska förlusterna är omfattande.<br>• Aktören har bestämt förfaranden för att göra första anmälan och fortsatt anmälan om betydande incidenter med NIS-anmälningsblanketten och att lämna in slutrapporten.<br>• Aktören har förberett sig på att samla in och lämna in nödvändiga angreppsindikatorer, dvs. IoC-uppgifter (Indicator of Compromise) för att utreda incidenten. Dessa uppgifter behövs till exempel i den fortsatta anmälan. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att förfaranden vid betydande incidenter beskrivs separat i dokumentationen. Förfaranden för betydande incidenthantering innefattar vanligen en eskalering av incidenten. Behoven i anknytning till bedömning och hantering av betydande incidenter samt kommunikation och roller ska vara tydligt definierade i förfaranden för incidenthantering och i tillhörande dokument. Betydande incidenter kräver ofta olika kommunikation till exempel till myndigheter, och detta ska beaktas. Delning av information vid betydande incidenter (se 9.8) och särskilt nödkommunikationssystem i anknytning till det (se 10.4) ska beskrivas och bestämmas på förhand. |

| **Motiveringar** |
| --- |
| |
| **Källor** |
| ISO/IEC 27002:2022 (5.26, 5.29, 5.30)<br>ISO/IEC 27035-2:2023 (6.5, 6.6)<br>IEC 62443-2-1:2010 (4.3.4.5.3, 4.3.4.5.5)<br>IEC 62443-2-1:2024 (EVENT 1.2, EVENT 1.8, AVAIL 1.1)<br>IEC 62443-2-4:2024 (SP.08.01, SP.08.03)<br>NIST CSF 1.1 (ID.GV-2, ID.GV-3, RC.CO-3)<br>NIST CSF 2.0 (GV.RR-02, GV.OC-03, DE.AE-08, RS.AN-07, RS.AN-08, RC.CO-03) |
| **Verktyg** |
| Julkri (HAL-08, TSU-14)<br>Cybermätaren (RESPONSE-2, RESPONSE-3, RESPONSE-5) |

## 9.8 Säkerheten vid spridning av information i incidenter

| **Exempel på genomförande** |
| --- |
| • Aktörens kommunikationskanaler i samband med incidenter som gäller cybersäkerhet är tillräckligt säkra när det gäller tillgänglighet, konfidentialitet och integritet.<br>• Vid valet av kommunikationskanalerna ska man beakta en situation där sedvanliga kommunikationskanaler inte är tillgängliga.<br>• Eventuell information om fientlig verksamhet delas så att den inte hamnar hos en angripare. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören i sin dokumentation har definierat kommunikationskanaler som säkra för informerande vid incidenter. Kommunikationskanalernas tillgänglighet är en central säkerhetsegenskap och där har man i synnerhet beaktat situationer när sedvanliga tjänster inte är tillgängliga (se 10.4). Vid valet av kommunikationskanaler ska man beakta att den delade informationen inte utgör en risk för de olika parterna. Detta kan genomföras till exempel genom att använda kryptering och annan teknik som är differentierad från det riskfyllda systemet. I dokumentationen och planerna ska |

man också beakta situationer när en incident påverkar kommunikationskanalen och producera en reservplan och reservkommunikationskanal (se 10.4). Dessutom är det bra att inspektera att aktören upprätthåller och regelbundet testar sina kommunikationskanalers funktion.

2. Tillsynsmyndigheten kan även genom testning verifiera att delningen av information är säker. Man kan till exempel be aktören att skicka textmeddelanden via olika kommunikationskanaler. Samtidigt kan man kontrollera att skyddsmetoder såsom kryptering av meddelanden kan användas.

**Motiveringar**

Vid incidenter ska man se till säker delning av information i anknytning till en incident. Det är ytterst viktigt att detta har bestämts på förhand, eftersom resurserna vid en incident behövs för annat än detta.

När det gäller säkerheten för delning av information ska flera saker beaktas såsom huruvida informationen i anknytning till angreppet är klassificerad och därför ska skyddas, hur angriparens tillgång till informationen förhindras och hur tillgängligheten till information som delas säkerställs. Informationen ska skyddas från angriparen så att hen inte får fördelar av att känna till aktörens eventuella svagheter och kan utnyttja aktörens lägesinformation om utredningen av angreppet.

**Källor**

ISO/IEC 27002:2022 (5.24, 5.26, 5.28, 5.29)

ISO/IEC 27035-1:2023 (4.6)

ISO/IEC 27035-2:2023 (4.2, 6.3, 6.8, 8.9)

IEC 62443-2-1:2024 (EVENT 1.4, EVENT 1.8, AVAIL 1.1)

IEC 62443-2-4:2024 (SP.08.01, SP.08.03)

IEC 62443-3-3:2013 (SR 4.1 RE 1)

NIST CSF 1.1 (PR.DS-2, PR.PT-4)

NIST CSF 2.0 (PR.DS-02, PR.AA-06, PR.IR-01)

NIST SP 800-61 rev 2 (3.4.2, 4.1, 4.2, 4.3)

NIS CG Implementing guidance (3.3. Event reporting)

NIS CG Implementing guidance (4.1. Business continuity and disaster recovery plans)

NIS CG Implementing guidance (4.2. Backup management)

NIS CG Implementing guidance (4.3. Crisis management)

NIS CG Implementing guidance (6.7. Network security)

NIS CG Implementing guidance (9. Cryptography)

| |
|---|
| NIS CG Implementing guidance (12.2. Handling of information and assets) |
| **Verktyg** |
| Julkri (TEK-16)<br>Cybermätaren (RESPONSE-3, RESPONSE-5, ARCHITECTURE-5) |

## 9.9 Hantering av incidenthanteringens livscykel

| |
|---|
| **Exempel på genomförande** |
| • Förfaranden för incidenthantering av cybersäkerheten upprätthålls och förbättras regelbundet samt i synnerhet efter betydande incidenter.<br>• Aktören håller roller, resurser, kriterier för incidentklassificering och annan väsentlig information i anknytning till incidenthantering uppdaterade. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen att aktören har dokumenterat åtgärder i anknytning till regelbunden utveckling av förfaranden såsom planerad uppdateringstidtabell och uppdateringspraxis av det man lärt sig efter betydande incidenter.<br>2. Tillsynsmyndigheten kan kontrollera den genomförda utvecklingen i förändringshistoriken och genom intervjuer. |
| **Motiveringar** |
| Regelbundet underhåll av förfaranden för incidenthantering främjar incidenthantering i en verklig situation. Det är viktigt med kontinuerlig utveckling av förfarandena. Det är dock naturligt att även resurserna i anknytning till incidenthanteringen förändras hela tiden, till exempel på grund av personalbyten. Vid incidenter finns det i allmänhet inte tid för att uppdatera och utreda saker. |
| **Källor** |
| ISO/IEC 27002:2022 (5.24, 5.27)<br>ISO/IEC 27035-1:2023 (5.5)<br>ISO/IEC 27035-2:2023 (9, 10, 11, 12)<br>IEC 62443-2-1:2010 (4.3.4.5.8)<br>IEC 62443-2-1:2024 (EVENT 1.8, ORG 1.1)<br>NIST CSF 1.1 (PR.IP-7, DE.DP-5, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2) |

| |
|---|
| NIST CSF 2.0 (ID.IM-03) |
| NIST SP 800-61 rev 2 (3.3.4, 3.4, 3.5) |
| NIS CG Reference document (3.11.1 Incident handling policy) |
| NIS CG Implementing guidance (3.1. Incident handling policy) |
| **Verktyg** |
| Julkri (HAL-08) |
| Cybermätaren (RESPONSE-3, RESPONSE-5) |

# 10 Säkerhetskopiering, katastrofhantering, krishantering och övrig driftskontinuitet och vid behov användning av säkrade reservkommunikationssystem

Rekommendationerna grundar sig på artikel 21.2 c och delvis på j i NIS 2-direktivet. Nationellt genomförande av dessa föreskrivs i 9 § 2 mom. 10 punkten i cybersäkerhetslagen och 18 c § 1 mom. 10 punkten i informationshanteringslagen.

1. **Kontinuitets- och återhämtningsplanering:** Aktören ska ha dokumenterade förfaranden för driftskontinuitet och återhämtning från störningssituationer. Kontinuiteten kan säkerställas till exempel genom en kontinuitetsplan som skapas på basis av riskhanteringen samt genom en återhämtningsplan. Planerna kan till exempel innehålla de omständigheter under vilka de ska aktiveras samt planer som gäller behövliga roller, resurser, åtgärder och kommunikationskanaler samt behövliga säkrade reservkommunikationssystem. Planerna ska innehålla eller aktören ska på annat sätt planera krishanteringsförfaranden med tanke på åtminstone synnerligen allvarliga incidenter. I enlighet med den övriga riskhanteringen ska planerna uppdateras och utvecklas regelbundet och genomförandet av planerna övas. (Se punkt 10.1).

2. **Säkerhetskopior och reservsystem:** När det gäller säkerhetskopiering kan aktören till exempel på basis av riskhanteringen fastställa vilka uppgifter, system och reservsystem som det är nödvändigt att ta säkerhetskopior av. Aktören ska normalt ha praxis för hur ofta säkerhetskopior ska tas, förvaringstiden för säkerhetskopior, skyddet av säkerhetskopior och testningen av återställning i ett läge där det ursprungliga systemet inte är tillgängligt. Förvaringstiden för säkerhetskopior bör bedömas i förhållande till förvaringssyftet och säkerhetskopior ska tas tillräckligt ofta för att funktionerna ska kunna återställas tillräckligt snabbt och med tillräckligt färsk information i händelse av en incident eller kris. (Se punkt 10.2).

3. **Återställningstest och skyddande av säkerhetskopior**: Återställningen kan testas regelbundet för att säkerställa att den fungerar. Säkerhetskopior kan t.ex. skyddas så att de inte utsätts för samma hot som det system som säkerställs. (Se punkt 10.3).

4. **Reservkommunikationssystem:** Behovet av säkrade reservkommunikationssystem kan till exempel grunda sig på att det i riskbedömningen har konstaterats vara nödvändigt att säkra kommunikationskanalerna också när vanliga system (t.ex. telefon, e-post, snabbmeddelanden) inte finns att tillgå. Om behov föreligger, kan aktören fastställa exempelvis vilka reservkommunikationssystem som ska användas och behovet av dem samt sättet att ta i bruk dem. (Se punkt 10.4).

## 10.1 Kontinuitets- och återhämtningsplanering

**Exempel på genomförande**

- Aktören har dokumentation som beskriver förfaranden när det gäller verksamhetens kontinuitet och återhämtning från störningssituationer. Dokumentationen innehåller till exempel kontinuitetsplan (business continuity plan, BCP), återhämtningsplan (disaster recovery plan, DRP) och konsekvensbedömning av störningar (business impact analysis, BIA) som grundar sig på riskbedömning, verksamhetens krav och lagstiftning (se 9.1).
- Kontinuitets- och återhämtningsplanerna innehåller till exempel en beskrivning av de situationer där de processer och åtgärder som planerna beskriver tas i bruk, ordningen av processer och åtgärder, kommunikationskanaler och personalresurser med roller, återhämtningsförfaranden och beroendeförhållanden till andra system, resurserna som behövs för återhämtningen, tillfälliga arrangemang och målen för återhämtningen (se 6.1).
- Kontinuitets- och återhämtningsplanerna beskriver också åtgärder i anslutning till mycket allvarliga incidenter (kriser), kommunikationskanaler och identifieringsfaktorer (se 9.7).
- Kontinuitets- och återhämtningsplanerna uppdateras regelbundet och processer, funktionssätt och resurser som beskrivs i planerna utvecklas och genomförandet av planerna övas, särskilt med tanke på betydande incidenter eller förändringar i affärsmiljön.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har dokumenterade förfaranden för verksamhetens kontinuitet vid återhämtning från störningssituationer. För dessa har aktören åtminstone en kontinuitetsplan och en återhämtningsplan som baserar sig på riskhantering, eller dokumentation med motsvarande innehåll. Planerna innehåller omfattande information som används för att påbörja åtgärderna i planen. Planerna innehåller också roller, resurser, åtgärder och kommunikationskanaler som används under incidenthantering. I planerna har också behandlats allvarliga störnings- och krissituationer då aktören eller aktörens verksamhetsmiljö är utsatt för en allvarlig störningssituation. Tillsynsmyndigheten verifierar att planerna har uppdaterats, utvecklats och övats regelbundet. Det kan verifieras till exempel i dokumentationens uppdateringshistorik och dokument i anknytning till övningar. Den enklaste formen av övning kan vara simulering genom diskussion (s.k. skrivbordsövning, tabletopövning) om förfaranden i anslutning till kontinuitet och återhämtning.
2. Tillsynsmyndigheten verifierar till exempel genom intervjuer att förfaranden för aktörens kontinuitets- och återhämtningsplanering har förankrats i verksamheten. Detta kan kontrolleras till exempel genom att resurserna i planerna finns och att personerna är medvetna om sina uppgifter i verkställandet av planerna. Dessutom kan tillsynsmyndigheten genom intervjuer utreda hur planerna uppdateras och övas. Om aktören har haft incidenter där planerna har utnyttjats kan tillsynsmyndigheten utvidga intervjun även till dessa händelser och inspektera data i anknytning till dessa situationer.
3. Tillsynsmyndigheten kan delta i aktörens övning som gäller kontinuitets- och återhämtningsplaneringen till exempel som observatör i samarbete med aktören. Vid övningarna kan man också utnyttja samarbetet mellan flera aktörer

| |
|---|
| och ordna till exempel nationella cybersäkerhetsövningar där deltagarna består av myndigheter, aktörer och andra samarbetspartner. |
| **Motiveringar** |
| Kontinuitets- och återhämtningsplanering är en väsentlig del för hantering av incidenter och kriser. Färdigt bestämda handlingssätt, resurser, omständigheter och kommunikationskanaler främjar återhämtningen från incidenter och återställandet av verksamhetens kontinuitet.<br><br>Övning av planerna på förhand gör att återhämtningen sker märkbart snabbare och gör den smidigare. Redan en skrivbordsövning kan hjälpa till att hitta problem i planerna och förhindra att de förverkligas i en verklig situation. |
| **Källor** |
| ISO/IEC 27002:2022 (5.30, 5.37)<br><br>IEC 62443-2-1:2010 (4.3.4.5)<br><br>IEC 62443-2-1:2024 (ORG 1.1, EVENT 1.8, AVAIL 1.1)<br><br>IEC 62443-2-4:2024 (SP.12.09)<br><br>NIST CSF 1.1 (PR.IP-9-10, ID.BE-5, ID.SC-5, RC.RP-1, RC.IM-1, RC.IM-2)<br><br>NIST CSF 2.0 (ID.IM-02, ID.IM-03, ID.IM-04, GV.OC-04, GV.SC-08, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06)<br><br>NIS CG Reference document (3.12.1 Business continuity and disaster recovery plans)<br><br>NIS CG Implementing guidance (4.1. Business continuity and disaster recovery plans) |
| **Verktyg** |
| Julkri (VAR-02, TEK-13, TEK-22.1)<br><br>Cybermätaren (CRITICAL-3, RESPONSE-3, RESPONSE-4, RESPONSE-5)<br><br>Cybersäkerhetscentrets anvisning om cyberövningar11 |

## 10.2 Säkerhetskopior och reservsystem

| |
|---|
| **Exempel på genomförande** |

[11] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Anvisning%20om%20cyberövningar.pdf

Denna punkt kompletterar punkt 11.11 om grundläggande praxis för informationssäkerhet.

- Aktören har planerat, genomfört, testat och beskrivit säkerhets- och återhämtningsprocesser för säkerhetskopiering.
- Säkerhetskopiering görs tillräckligt ofta så att systemen och informationen i dem kan återställas med tillräckligt uppdaterad information (recovery point objective, RPO). Dessutom ska återhämtningssystemet dimensioneras så att återhämtningen kan göras tillräckligt snabbt (recovery time objective, RTO).
- Säkerhetskopior ska förvaras säkert och tillräckligt länge med beaktande av affärsverksamhetsbehoven och lagstiftningskraven.
- Säkerhetskopior har gjorts av alla behövliga uppgifter och system. I objekten som kopieras ska också beaktas till exempel säkerhetskopiering av konfigurationer och molntjänster.
- Aktören ska vid behov snabbt ta i bruk reservsystem som är oberoende av andra system, som inbegriper till exempel förmåga och kapacitet på grundval av beredskap i anslutning till lokaler, enheter, nätförbindelser, informationssystem, kommunikationskanaler och personal.
- Tilläggskapacitet kan till exempel vara att reservera kapacitet från två olika molnleverantörer, färdigt konfigurerade reservenheter eller att bygga upp ett informationssystem så att det tål störningar i kritiska funktioner. Förmågan kan säkerställas genom ersättararrangemang och kompetensutveckling.
- Aktörens säkerhetskopior och reservsystem motsvarar kraven i lagstiftningen och verksamheten.

## Verifiering

1. Tillsynsmyndigheten verifierar att aktören har bestämt de uppgifter och system som ska säkerhetskopieras för att säkerställa verksamhetens kontinuitet. När detta bestäms har man också beaktat system och uppgifter som andra tjänster är beroende av och vars funktion därför är nödvändig med tanke på verksamheten. Dessutom verifierar tillsynsmyndigheten att aktören vid behov har tillräckliga reservsystem. Reservsystemen har vid behov beskrivits till exempel i arkitekturbeskrivningarna samt i planerna i punkt 10.2. Reservsystemen kan i vissa fall beroende på fallet även ersätta en del av säkerhetskopieringen. Tillsynsmyndigheten verifierar att aktören har bestämt värden för säkerhetskopiornas förvaringstid och hur ofta den ska göras. Tillsynsmyndigheten säkerställer att värdena är i linje med hur mycket data aktören kan förlora vid en incident och hur snabbt data kan återställas. Värdena kan vara olika för olika system och information. När det gäller säkerhetskopieringens förvaringstid ska till exempel lagstadgade skyldigheter beaktas samt olika riskscenarier när man kan bli tvungen att söka säkerhetskopior långt tillbaka till exempel på grund av obemärkt dataförvanskning, lång svarstid för incidenten eller av någon annan orsak. Aktören kan ha bestämt att säkerhetskopior förvaras under en längre tid till exempel i mindre omfattning, till exempel fullständiga kopior (s.k. full backup) överförs en gång per månad till långvarig

förvaring och annars förvaras kopior (t.ex. incremental) till exempel i några veckor.

2. Tillsynsmyndigheten verifierar till exempel genom skärmdumpar eller genom att inspektera systemen att aktören har genomfört de reservsystem och säkerhetskopior som beskrivs i punkt 1. Om aktören har haft incidenter kan man genom intervjuer och genom att kontrollera händelseloggen i anknytning till händelsen verifiera att genomförandet av reservsystem och säkerhetskopiering är tillräckliga.
3. Tillsynsmyndigheten kan tillsammans med aktören testa funktionen hos reservsystem och säkerhetskopior.

**Motiveringar**

I många fall, i synnerhet vid allvarliga incidenter, har reservsystem och säkerhetskopior en mycket viktig roll för att återställa verksamheten. Incidenter kan vara oavsiktliga eller avsiktliga och i synnerhet i vissa situationer såsom angrepp som krypterar alla information är det mycket viktigt att det finns säkerhetskopior.

Dessutom kan vissa system och att de inte fungerar medföra stora problem för återställningen. De är ofta även särskilt eftertraktade objekt för en angripare. Sådana är till exempel tjänster i anknytning till åtkomsthantering (t.ex. Active Directory, AD) och det finns skäl att beakta snabb återställning av tjänsterna.

**Källor**

ISO/IEC 27002:2022 (8.13, 8.14)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03)

NIST CSF 1.1 (PR.IP-4)

NIST CSF 2.0 (PR.DS-11, PR.IR-03, RC.RP-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

NIS CG Implementing guidance (4.2. Backup management)

**Verktyg**

Julkri (TEK-20, VAR-02, VAR-07, VAR-08)

Cybermätaren (CRITICAL-2, ASSET-2, RESPONSE-4)

## 10.3 Återställningstest och skyddande av säkerhetskopior

**Exempel på genomförande**

Denna punkt kompletterar punkt 11.11 om grundläggande praxis för informationssäkerhet.

- Återställandet av säkerhetskopiorna och reservsystemens funktion ska testas regelbundet, i första hand automatiskt. Vid testningen ska även säkerhetskopiornas riktighet kontrolleras. Återställningstest av säkerhetskopior ska utföras säkert så att det inte äventyrar produktionssystemet.
- Säkerhetskopior ska förvaras i ett säkert utrymme som på grundval av aktörens riskhantering är tillräckligt differentierat från systemet som ska säkerhetskopieras. Detta kan innebära till exempel en annan lokal eller ett separat brandsäkert utrymme. Säkerhetskopior kan vid behov förvaras i flera format som kan ha olika återställningshastigheter, såsom diskkopior eller separata långtidsarkiv.
- Vid skyddande av säkerhetskopior kan man beakta behoven för deras riktighet, tillgänglighet och konfidentialitet. Detta innebär till exempel tillräckligt fysiskt skydd och andra kontroller såsom kryptering.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören i mån av möjlighet och enligt behovet har bestämt åtgärder för att regelbundet testa funktionen hos säkerhetskopior och reservsystem, till exempel en gång i veckan. Detta kan vara automatiserat eller manuellt. Det väsentliga är att man förutom den mekaniska återställningen även granskar hur informationen kan återställas oskadd och användningsbar samt att ett eventuellt reservsystem kan byggas med rätt information. Tillsynsmyndigheten verifierar att säkerhetskopiorna är tillräckligt skyddade. Till exempel i arkitekturbeskrivningar, systemdokumentation eller motsvarande ska beskrivas hur säkerhetskopieringen eller en del av den har differentierats från det övriga systemet. Detta ska säkerställa till exempel att en angripare som får tillgång till kommunikationsnätet och informationssystemet inte får tillgång till alla säkerheter.
2. Tillsynsmyndigheten verifierar genom inspektioner och intervjuer hur aktören testar säkerhetskopiors funktion i mån av möjlighet och enligt behovet. Av detta ska framgå till exempel genomförda åtgärder för att försäkra sig om säkerhetskopiornas riktighet och regelbunden testning. Tillsynsmyndigheten kan vid behov även använda fysiska inspektioner för att säkerställa att säkerhetskopior är tillräckligt differentierade från det övriga systemet. Vid inspektionen ska man säkerställa att till exempel hot såsom en eldsvåda, översvämning och personhot inte berör både systemet som ska säkerställas och säkerhetskopior.
3. Om det gäller en motiverad logisk differentiering i stället för fysisk differentiering kan tillsynsmyndigheten utnyttja till exempel skanningar gjorda av aktö-

| |
|---|
| ren och kontaktförsök för att säkerställa att det differentierade säkerhetskopieringssystemet inte är tillgängligt från det kommunikationsnät och informationssystem som ska säkras. |
| **Motiveringar** |
| I samband med återhämtning från incidenter händer det alltför ofta att återställningen inte lyckas eller att angriparen lyckas förstöra både informationssystemet och säkerhetskopiorna. Därför kan en omfattande och regelbunden testning av återställning samt skydd av återställningssystemet vara livsviktiga med tanke på verksamheten. |
| **Källor** |
| ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)<br>IEC 62443-2-1:2010 (4.3.4.3.9)<br>IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, AVAIL 1.2, AVAIL 2.3)<br>IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03, SP.12.04, SP.12.05, SP.12.06, SP.12.07)<br>NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)<br>NIST CSF 2.0 (PR.DS-11, RC.RP-01, RC.RP-05, ID.IM-03)<br>NIS CG Reference document (3.12.2 Backup and redundancy management) |
| **Verktyg** |
| Julkri (TEK-20, VAR-09)<br>Cybermätaren (RESPONSE-4, ARCHITECTURE-1, ARCHITECTURE-5) |

## 10.4 Reservkommunikationssystem

| **Exempel på genomförande** |
|---|
| • Aktören ska ha skyddade kommunikationskanaler utifrån riskbedömningen som möjliggör tillräcklig och säker kommunikation till myndigheter, kunder, tjänsteleverantörer och andra väsentliga sektorer. Systemen ska vara sådana att de även fungerar vid allvarliga störningssituationer och kriser. Se även punkt 9.8 Säkerhet vid spridning av information<br>• Dessa reservkommunikationssystem ska vara oberoende och åtskilda från andra system. |

- Reservkommunikationskanalen kan grunda sig till exempel på kurirförfarande, alternativa snabbmeddelanden eller mobilnätet.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har fastställt behövliga reservkommunikationssystem utifrån sin riskbedömning. Reservkommunikationssystemet används när systemen som används i vanliga fall inte är i bruk. Dessa system nämns till exempel i planerna i punkt 10.1. Tillsynsmyndigheten verifierar särskilt att de valda reservkommunikationssystemen inte är beroende av aktörens övriga infrastruktur.
2. Tillsynsmyndigheten verifierar i samarbete med aktören att reservkommunikationssystemen fungerar. Detta kan genomföras till exempel genom att skicka textmeddelanden med reservkommunikationssystemet.

**Motiveringar**

**Källor**

ISO/IEC 27002:2022 (5.5, 5.29, 5.30, 7.13)

IEC 62443-2-1:2024 (ORG 1.1, AVAIL 1.1, AVAIL 1.2)

IEC 62443-2-4:2024 (SP.08.04, SP.12.09)

NIST CSF 2.0 (RC.CO-03)

NIS CG Reference document (3.12.3 Crisis management)

NIS CG Implementing guidance (4.3. Crisis management)

**Verktyg**

Julkri (VAR-06, TEK-22.1)

Cybermätaren (RESPONSE-3)

# 11 Grundläggande praxis för informationssäkerhet för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet

Rekommendationerna grundar sig på delvis på artikel 21.2 g i NIS 2-direktivet. Om nationellt genomförande av denna föreskrivs i 9 § 2 mom. 11 punkten i cybersäkerhetslagen och 18 c § 2 mom. 11 punkten i informationshanteringslagen.

Aktören ska skydda sitt kommunikationsnät och sina informationssystem genom grundläggande praxis för informationssäkerhet. Aktören ska se till att behövliga grundläggande åtgärder för informationssäkerhet tillämpas och att arbetstagarna följer dem. Nivån på denna informationssäkerhets- eller cyberhygienpraxis ska dimensioneras så att den är tillräcklig med hänsyn till hur kritiska funktionerna är. De valda åtgärderna ska bygga på allmän god praxis och riskbedömning.

Med informationssäkerhets- eller cyberhygienpraxis avses allmänna goda grundläggande informationssäkerhetsåtgärder som säkerställer en säker grundläggande användning av system, program och tjänster. Det innebär tekniska och andra åtgärder på basnivå för att säkerställa säkerheten i de objekt som beskrivs i punkten.

De rekommendationer om grundläggande praxis för informationssäkerhet som beskrivs i detta underavsnitt har utarbetats så att även aktörer som hör till tillämpningsområdet för NIS-regleringen genom att följa rekommendationerna kan utvärdera cybersäkerhetens mognadsnivå och förbättra den. Grundläggande praxis för informationssäkerhet är en lätt formulerad samling av alla åtgärders som föreslås i denna rekommendation och överlappar delvis med rekommendationer i de andra underavsnitten.

Tillsynsmyndigheten kan använda grundläggande praxis för informationssäkerhet för att skapa en allmän bild av nivån på cybersäkerheten hos aktörerna som övervakas och om läget inom sektorn.

Praxis för informationssäkerhet kan innehålla både administrativa och tekniska åtgärder. Grundläggande praxis för informationssäkerhet i rekommendationen:

1. Aktören har instruerat personalen, underleverantörer och andra partner om grundläggande praxis för informationssäkerhet (se punkt 11.1 och 11.1.1).

2. Aktören har identifierat sina mest kritiska tillgångar (se punkt 11.2).

3. Aktören har skyddat sina kommunikationsnät och informationssystem (se punkt 11.3).

4. Aktören har differentierat kritiska och sårbara kommunikationsnät och informationssystem från andra miljöer (se punkt 11.4).

5. Aktören har skyddat sina kommunikationsnät och informationssystem mot skadlig och otillåten programvara (se punkt 11.5).

6. Aktören har ordnat identifieringen av sina interna och externa tjänster och enheter på ett säkert sätt (se punkt 11.6).

7. Aktören har i sina system differentierat huvudanvändarnamn och användarnamn med förhöjda rättigheter från andra användarnamn (se punkt 11.7).

8. Aktören har säkerställt att konfidentiella uppgifter behandlas på ett säkert sätt (se punkt 11.8).

9. Aktören har sett till att systemen uppdateras regelbundet och kritiska uppdateringar installeras utan dröjsmål (se punkt 11.9).

10. Aktören har sett till att tjänsterna och enheterna är säkert konfigurerade (se punkt 11.10).

11. Aktören har sett till att kritiska tjänster och dataegendom är säkerhetskopierade (se punkt 11.11).

12. Aktören har förberett sig på hur verksamheten kan upprätthållas vid allvarliga incidenter (se punkt 11.12).

13. Aktören har i bruk registrering av händelser (logg) i fråga om kritiska funktioner (se punkt 11.13).

### 11.1 Aktören har instruerat personalen, underleverantörer och andra partner om grundläggande praxis för informationssäkerhet

**Exempel på genomförande**

- Aktören har skriftlig grundläggande praxis för informationssäkerhet som är tillgänglig för personalen, underleverantörer och andra partner. De är också medvetna om var dokumenten finns. Praxisen granskas och uppdateras vid behov regelbundet, till exempel årligen.
- Grundläggande praxis för informationssäkerhet stöder förbättringen av medvetenheten om cybersäkerhet (awareness).
- Praxis för informationssäkerhet är i linje med riktlinjerna för säkerhet och andra branschspecifika riktlinjer. Det finns kontaktpersoner och kontaktkanaler för praxis för informationssäkerhet.
- Aktörens grundläggande praxis för informationssäkerhet kan innehålla den praxis som presenteras i rekommendationen. Aktören har också inkluderat andra åtgärder i praxisen i enlighet med riskbedömningen.
- Åtgärderna kan omfatta god praxis för informationssäkerhet som personalen iakttar och säkerhetsrelaterade förfaranden som organisationen tillämpar.

| **Verifiering** |
| --- |
| 1. Tillsynsmyndigheten verifierar att aktören har skriftlig grundläggande praxis för informationssäkerhet som är tillgänglig för hela personalen, underleverantörer och andra partner.<br>Innehållet omfattar funktionssätt som beskrivs i praxisen för informationssäkerhet som bland annat består av funktionssätt i anknytning till informationssäkerheten, anmälningskanaler, hanteringsanvisningar för information och utrustning, praxis för lösenord och användarnamn, fjärråtkomstlösningar, skydd mot nätfiske, skydd mot fakturabedrägerier samt identifiering av andra vanliga hot.<br>2. Tillsynsmyndigheten försäkrar sig genom intervjuer om personalens kompetens och genomförandet av praxis för informationssäkerhets i praktiken. |
| **Motiveringar** |
| Aktörens personal ska känna till grundläggande praxis för att man ska kunna säga att den allmänna medvetenheten om cybersäkerheten är på en skälig nivå. Grundläggande praxis för informationssäkerhet kan, om den genomförs korrekt och heltäckande, i bästa fall förhindra de vanligaste informationssäkerhetshoten. |
| **Källor** |
| CCB CYFUN Basic (PR.AT-1)<br>ISO/IEC 27002:2022 (6.3)<br>IEC 62443-2-1:2010 (4.3.2.4.1, 4.3.2.4.2)<br>IEC 62443-2-1:2024 (ORG 1.4, ORG 1.5)<br>IEC 62443-2-4:2024 (SP.01.01)<br>NIST CSF 1.1 (PR.AT-1)<br>NIST CSF 2.0 (PR.AT-01)<br>NIS CG Implementing guidance (8.1 Awareness raising and basic cyber hygiene practices)<br>NIS CG Implementing guidance (8.2 Security training) |
| **Verktyg** |
| Julkri (HAL-13, HAL-15)<br>Cybermätaren (WORKFORCE-1, WORKFORCE-2, PROGRAM-1, PROGRAM-2, Allmänna förvaltningsåtgärder) |

### 11.1.1 Program för att öka cybermedvetenheten – utvidgade anvisningar

**Exempel på genomförande**

Denna rekommendation är inriktad på tillsyn av aktörer som tillsynsmyndigheten förväntar sig ha en högre cybermognad.

- Aktören har ett utbildningsprogram för att öka de anställdas cybermedvetenhet. Syftet med programmet är att erbjuda arbetstagarna medvetenhet om cybersäkerhetsriskerna i arbetet, vikten av cybersäkerhet och allmän god praxis för cybersäkerhet. Målet med programmet är att förhindra de vanligaste cyberincidenterna.
- Programmet är avsett för alla arbetstagare, inklusive högsta ledningen.
- Programmet bör vara kontinuerligt så att det omfattar alla arbetstagare, inklusive nya arbetstagare.
- Programmet ska grunda sig på aktörens gällande praxis förcybersäkerhetför att förbli väsentligt med tanke på dess mål.
- Programmet ska omfatta riskhanteringsåtgärder, kontaktkanaler och andra resurser som är betydelsefulla för arbetstagarna, såsom kontaktpersoner och databanker för att få cybersäkerhetsanvisningar samt allmän god praxis i anslutning till cybersäkerhet.
- Programmet ska uppdateras regelbundet.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har ett utbildningsprogram för att öka cybermedvetenheten. Programmet, dess mål och praxis för uppdatering av programmet ska finnas i skriftlig form.

**Motiveringar**

Personalen har en stor roll i genomförandet av aktörens cybersäkerhet. Aktörens personal kan till exempel utsättas för mycket skickligt riktad social manipulation och nätfiske, som vanliga arbetstagare har en stor roll i att bekämpa och upptäcka. Även olika skadliga program kan spridas av okunniga arbetstagare, men epidemier av skadliga program kan bekämpas med en god cybersäkerhetsmedvetenhet hos arbetstagaren.

**Källor**

ISO/IEC 27001:2022 (7.3)

IEC 62443-2-1:2024 (ORG 1.4)

IEC 62443-2-4:2024 (SP.01.01)

| |
|---|
| NIST CSF 1.1 (PR.AT-1)<br>NIST CSF 2.0 (PR.AT-01)<br>NIS CG Implementing guidance (8.1 Awareness raising and basic cyber hygiene practices) |
| **Verktyg** |
| Cybermätaren (WORKFORCE-2) |

## 11.2 Aktören har identifierat sina mest kritiska tillgångar

| **Exempel på genomförande** |
|---|
| Denna grundläggande praxis för informationssäkerhet leder till punkterna 5.1, 5.2 och 5.3.<br>• Aktören har identifierat objekt som är kritiska med tanke på verksamheten. Dessa objekt är sådana som aktören behöver för att fungera, som omfattas av sektorspecifika lagstadgade skyldigheter eller där ett brott mot informationssäkerheten kan orsaka stor skada. Objekten kan till exempel vara enheter, programvara, applikationer eller data som är kritiska med tanke på affärsverksamheten.<br>• Aktören har utarbetat, informerat och tillgängliggjort praxis för riktlinjer i anknytning till säkerheten i kommunikationsnät och informationssystem samt anvisningar för tillgångsförvaltning.<br>• Aktörens tillgångsförvaltning ska vara regelbunden och konsekvent och omfatta de kritiska funktioner och tjänster som organisationen identifierat, datalager och annan immateriell och materiell egendom, såsom de tjänster, konton och licenser som organisationen tagit i bruk. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har praxis och anvisningar i anknytning till tillgångsförvaltning. Det finns skriftliga bevis på att tillgångsförvaltningen är regelbunden och konsekvent. Tillgångsförvaltningen omfattar åtminstone de komponenter som är mest betydande med tanke på verksamheten. I bruksanvisningar eller användarutbildning berättas om säkerhetspraxis i fråga om dessa system. |
| **Motiveringar** |
| Identifieringen och klassificeringen av kritiska tillgångar möjliggör en riskbaserad metod. En riskbaserad strategi för cybersäkerhet förbättrar aktörens cybersäkerhetssituation genom att den blir mer systematisk och mindre sporadisk. Man bör |

| |
|---|
| särskilt uppmärksamma de tillgångar som är viktigast med tanke på verksamheten, eftersom störningar i tillgångarna kan orsaka aktören stor skada. |
| **Källor** |
| CCB CYFUN Basic (ID.AM-1, ID.RA-1))<br>ISO/IEC 27002:2022 (5.9, 5.12)<br>IEC 62443-2-1:2010 (4.2.3.4, 4.2.3.6)<br>IEC 62443-2-1:2024 (CM 1.1, CM 1.3)<br>IEC 62443-2-4:2024 (SP.06.02)<br>NIST CSF 1.1 (ID.AM-1, ID.RA-1)<br>NIST CSF 2.0 (ID.AM-01, ID.RA-01) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (HAL-04)<br>Cybermätaren (CRITICAL-1, ASSET-1, ASSET-2, ASSET-5) |

## 11.3 Aktören har skyddat sina kommunikationsnät och informationssystem

| |
|---|
| **Exempel på genomförande** |
| Denna grundläggande praxis för informationssäkerhet leder till punkterna 3.8 och 3.9.<br>• Aktören har begränsat tillgången till sina tjänster enligt principen om lägsta behörighet.<br>• Aktören använder en lösning som förhindrar skadlig eller oönskad trafik från icke-pålitliga kommunikationsnät, såsom en brandvägg.<br>• Utifrån aktörens riskhantering kan man också använda till exempel system för att upptäcka eller förhindra intrång.<br>• Det finns åtminstone enkel dokumentation om aktörens kommunikationsnät och informationssystem såsom nätverksbilder och nätscheman. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar i dokumentationen som aktören lämnat in att åtkomst till aktörens tjänster är begränsad enligt principen om lägsta behörighet i synnerhet i osäkra kommunikationsnät. |

| |
|---|
| Av dokumentationen framgår att aktören har valt skydden till kommunikationsnätet så att de är tillräckliga utifrån organisationens riskhantering. |
| **Motiveringar** |
| Kommunikationsnät och informationssystem som är kopplade till internet är föremål för en betydande mängd automatiserad skadlig trafik för att identifiera och utnyttja svagheter i systemen. Genom att begränsa tillgången till tjänster endast till källor från kända tjänster samt stänga telekommunikationsportar som är öppna i onödan kan man förhindra de flesta automatiserade hoten. Motsvarande princip gäller också mellan olika tillförlitliga och delvis tillförlitliga kommunikationsnät.<br><br>Det lönar sig för aktören i planeringen av sitt kommunikationsnät att även beakta intranätets struktur. Aktören ska sträva efter att skydda sitt intranät så att om en angripare lyckas till exempel få åtkomst till en arbetsstation i intranätet ska det vara svårt för angriparen att navigera vidare i nätet. |
| **Källor** |
| CCB CYFUN Basic (PR.AC-3)<br>ISO/IEC 27002:2022 (8.20, 8.21)<br>IEC 62443-2-1:2010 (4.2.3.5)<br>IEC 62443-2-1:2024 (NET 1.1, ORG 1.1)<br>IEC 62443-2-4:2024 (SP.03.02)<br>IEC 62443-3-3:2013 (SR 1.13, SR 3.1, SR 5.2, SR 7.7)<br>NIST CSF 1.1 (PR.AC-3)<br>NIST CSF 2.0 (PR.AA-03) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-01, TEK-02)<br>Cybermätaren (ACCESS-2, ACCESS-3, ARCHITECTURE-2, ARCHITECTURE-3) |

## 11.4 Aktören har differentierat kritiska och sårbara kommunikationsnät och informationssystem från andra miljöer

| |
|---|
| **Exempel på genomförande** |

Denna grundläggande praxis för informationssäkerhet leder till punkt 3.8.

- Aktören har differentierat de system som är mycket sårbara eller kritiska eller som i händelse av att de blir utsatta för risker kan leda till att hela nätet eller systemet äventyras. Sådana system är till exempel hanteringsnät och hanteringsarbetsstationer.
- Differentieringen kan genomföras med många olika tekniker, såsom fysisk eller logisk differentiering.
- Aktören har skyddat sina trådlösa nät så att de inte utgör en risk för andra system.
- I trafiken mellan aktörens differentierade kommunikationsnät har man beaktat principen om lägsta behörighet (se 11.3).

**Verifiering**

1. Tillsynsmyndigheten verifierar i den dokumentation aktören lämnat in att aktören har identifierat de mest kritiska systemen i anslutning till verksamheten och differentierat dem. Systemen och genomförandet av deras differentiering har beskrivits. Vid differentieringen ska man beakta offentliga nät, aktörens egna nät och möjliga kopplingar till tredje parts nät.

   I vissa fall i mycket små kommunikationsnät eller informationssystem kan differentiering vara onödigt med tanke på riskhanteringen. Då kan godkännande av en kvarstående risk på basis av riskhantering vara tillräckligt.

**Motiveringar**

Differentiering av kommunikationsnät är en viktig skyddsmetod och skyddar till exempel de mest sårbara systemen. Differentiering kan i många fall förhindra skadlig trafik, såsom spridning av utpressningsprogram från systemet och kommunikationsnätet till ett annat. Genom differentiering av kommunikationsnät kan man dela in informationssystem i mindre och tydligare helheter, vilket även gör det lättare att kontrollera filtreringsregler och andra skyddsåtgärder. I och med differentiering kan utredningsarbetet vid problemsituationer inriktas till en mer begränsad del och underlätta återhämtningen.

**Källor**

CCB CYFUN Basic (PR.AC-5)

ISO/IEC 27002:2022 (8.22)

IEC 62443-2-1:2010 (4.3.3.4)

IEC 62443-2-1:2024 (NET 1.1)

IEC 62443-2-4:2024 (SP.03.02)

IEC 62443-3-3:2013 (SR 5.1)

NIST CSF 1.1 (PR.AC-5)

| |
|---|
| NIST CSF 2.0 (PR.IR-01) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-01, TEK-02, TEK-04)<br>Cybermätaren (ARCHITECTURE-2) |

## 11.5 Aktören har skyddat sina kommunikationsnät och informationssystem mot skadlig och olovlig programvara

| **Exempel på genomförande** |
|---|
| Denna grundläggande praxis för informationssäkerhet leder till punkt 3.9.<br>• Aktören har skriftlig praxis för installation av programvara och skydd mot skadliga program. Aktören har gett personalen anvisningar om de vanligaste nätbedrägerierna, såsom nätfiske- och bedrägerimeddelanden.<br>• Aktören ska automatiskt behärska installation och utförande av programvara samt användning av lagringsmedier.<br>• Aktören har tekniska kontroller mot skadliga och olovliga program. Dessa kan vara till exempel skydd mot skadliga program, såsom antivirussystem i terminaler och e-posttjänster, system för att upptäcka eller förhindra intrång eller mellanserver. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har anvisningar eller praxis för att förhindra installation och genomförande av skadliga och otillåtna program.<br>Eventuella använda skydd mot skadligt program eller programvara som förhindrar genomförande av programmen fungerar och är tillräckligt uppdaterade.<br>2. Tillsynsmyndigheten ber aktören verifiera hur aktören har genomfört identifiering av ett skadligt meddelande, förhindrat otillåtna externa lagringsmedier och applikationer samt hållit skyddet mot skadliga program uppdaterat. |
| **Motiveringar** |
| Spridningen av skadliga program sker både inriktat till exempel via e-post och länkar och via källor som verkar tillförlitliga såsom via programvara som verkar äkta. Nätfiskemeddelanden och andra motsvarande skadliga meddelanden är ett av de vanligaste cyberhoten. |

| |
|---|
| Spridningen av skadliga program kan förhindras med både administrativa och tekniska metoder. Skadliga program kan förekomma i vilken som helst programvara, till exempel på grund av angrepp i leveranskedjan eller så kan programvaran i sig öka angreppsytan. |
| **Källor** |
| CCB CYFUN Basic (DE.CM-1, DE.CM-4, DE.CM-5)<br>ISO/IEC 27002:2022 (8.7, 8.19)<br>IEC 62443-2-1:2010 (4.3.4.3.8)<br>IEC 62443-2-1:2024 (COMP 2.1, COMP 2.2, COMP 2.3, CM 1.4)<br>IEC 62443-2-4:2024 (SP.10.01, SP.10.03)<br>IEC 62443-3-3:2013 (SR 3.2)<br>NIST CSF 1.1 (DE.CM-1, DE.CM-2, DE.CM-4, DE.CM-5, DE.CM-7)<br>NIST CSF 2.0 (DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-09) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-11)<br>Cybermätaren (ASSET-3, ARCHITECTURE-3, ARCHITECTURE-4) |

## 11.6 Aktören har ordnat identifieringen av sina interna och externa tjänster och enheter på ett säkert sätt

| |
|---|
| **Exempel på genomförande** |
| Denna grundläggande praxis för informationssäkerhet leder till punkt 7.1.<br>• Aktören har lösenordspraxis och anvisningar om hur man väljer säkra och individuella användarnamn och lösenord samt anmäler om användarnamnen blir utsatta för risk.<br>• Användningen av säkra och individuella användarnamn och lösenord kan främjas med hjälp av en lösenordshanterare.<br>• Aktören har identifierat system där starkare identifierings- och kontrollmetoder kan och ska tas i bruk, såsom multifaktorautentisering (multi-factor authentication MFA). |
| **Verifiering** |

1. Tillsynsmyndigheten verifierar att aktören har lösenordspraxis och har gett anvisningar om det. Praxisen innehåller anvisningar om hur man anmäler om användarnamnen blir utsatta för risk.

   Aktören har analyserat behovet av starka kontrollmetoder och tagit dem i bruk i den mån det är möjligt. Aktören har en förteckning över system som kräver en stark identifierings- och kontrollmetod för att användas. Aktören har en förteckning över system för vilka det inte krävs starka identifierings- och kontrollmetoder samt en motivering till varför starka identifierings- och kontrollmetoder inte har tagits i bruk i fråga om dem.

**Motiveringar**

Bra lösenord och kontrollmetoder som grundar sig på flera aktörer kan förhindra intrång i konton. Om samma användarnamn används på flera ställen ger stölden av ett användarnamn en angripare otillåten åtkomst till andra system. Sådana system kan till exempel vara sociala medieplattformar, varvid organisationens användarnamn kan missbrukas för skadliga syften. Med svaga lösenord är det möjligt att utsätta till exempel e-postanvändarnamn för risk, som kan användas för att sprida bluffmeddelanden eller skadliga program per e-post i aktörens namn. Med dessa användarnamn kan en angripare också få åtkomst till aktörens interna system.

**Källor**

CCB CYFUN Basic (PR.AC-1)

ISO/IEC 27002:2022 (5.15, 5.17, 8.5)

IEC 62443-2-1:2010 (4.3.3.6)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5, USER 1.11, DATA 1.1)

IEC 62443-2-4:2024 (SP.09.01)

IEC 62443-3-3:2013 (SR 1.1, SR 1.7)

NIST CSF 1.1 (PR.AC-1, PR.AC-7)

NIST CSF 2.0 (PR.AA-01, PR.AA-03)

**Verktyg**

Julkri (HAL-14, TEK-07, TEK-08)

Cybermätaren (ACCESS-1)

### 11.7 Aktören har i sina system differentierat huvudanvändarnamn och användarnamn med förhöjda rättigheter från andra användarnamn

| **Exempel på genomförande** |
|---|
| Denna grundläggande praxis för informationssäkerhet leder till punkt 7.5.<br>• Den personal hos aktören som utför huvudanvändar- eller underhållsuppgifter ska ha separata användarnamn för uppgifterna.<br>• Aktören ska ha praxis för beviljande och uppdatering av huvudanvändarnamn och användarnamn med förhöjda rättigheter. I praxisen bestäms hanteringen av användarnamnens livscykel, till exempel för beviljande, ändringar och borttagning.<br>• Användarnamn med förhöjda rättigheter och huvudanvändarnamn ska inte användas till grundläggande funktioner och grundläggande användarnamn ska inte användas för funktioner med förhöjda rättigheter eller huvudanvändarfunktioner.<br>• Onödigt omfattande åtkomsträttigheter ska undvikas. Användarna har till exempel endast grundläggande rättigheter till sina arbetsstationer om inte huvudanvändarrättigheter behövs för utförandet av arbetsuppgifterna. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har praxis för beviljande av huvudanvändarrättigheter eller användarnamn med förhöjda rättigheter, deras uppdatering och tillåtna användning. I praxisen har man beaktat att huvudanvändarnamn eller användarnamn med förhöjda rättigheter differentieras från grundläggande användarnamn.<br>Huvudanvändarrättigheter och användarnamn med förhöjda rättigheter beviljas endast vid behov och de tas bort eller ändras till exempel när arbetsuppgifterna ändrar eller när något annat behov i verksamheten ändras.<br>2. Tillsynsmyndigheten ber aktören att verifiera att huvudanvändarrättigheter endast innehas av de personer som behöver dem i sina arbetsuppgifter. Dessutom kan man jämföra dokumenterade och konfigurerade huvudanvändarrättigheter sinsemellan. |
| **Motiveringar** |
| Med huvudanvändarrättigheter är det möjligt att orsaka betydligt mer skada än med begränsade åtkomsträttigheter på grundläggande nivå.<br><br>Huvudanvändarnamnen är de mest eftertraktade objekten för angripare på grund av möjligheterna de ger. Därför är det särskilt viktigt att minimera hot som riktas mot dessa. |
| **Källor** |

| |
|---|
| CCB CYFUN Basic (PR.AC-4)<br>ISO/IEC 27002:2022 (5.15, 8.2)<br>IEC 62443-2-1:2010 (4.3.3.5)<br>IEC 62443-2-1:2024 (USER 1.4, USER 1.5)<br>IEC 62443-2-4:2024 (SP.09.04)<br>NIST CSF 1.1 (PR.AC-4, PR.AC-7)<br>NIST CSF 2.0 (PR.AA-05) |
| **Verktyg** |
| Julkri (TEK-04, TEK-07.2)<br>Cybermätaren (ACCESS-1, ACCESS-2, ACCESS-3, ARCHITECTURE-3) |

## 11.8 Aktören har säkerställt att konfidentiella uppgifter behandlas på ett säkert sätt

| **Exempel på genomförande** |
|---|
| Denna grundläggande praxis för informationssäkerhet leder till punkterna 2.3, 3.2, 5.2, 8.1 och 9.8.<br>• Aktören har praxis för att definiera informationens konfidentialitet. Aktörens praxis innehåller skriftliga anvisningar om informationshanteringen, såsom hur och var konfidentiell information förvaras, hanteras, överförs mellan olika system och elimineras.<br>• Organisationens arbetstagare, underleverantörer och andra parter som behandlar konfidentiell information har fått anvisningar om säker praxis.<br>• Konfidentiell information överförs i princip krypterad. Konfidentiell information i terminaler som aktören använder (datorer, telefoner, extern lagringsutrustning) är vid behov krypterad, till exempel med diskkryptering (se 11.10). |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har anvisningar där det framgår praxis för säker lagring, hantering, överföring och eliminering av konfidentiell information. Denna praxis gäller vid behov även underleverantörer och andra aktörer som hanterar konfidentiell information.<br>2. Tillsynsmyndigheten utnyttjar till exempel intervjuer och inspektioner för att granska funktionssätten i anknytning till konfidentiell information. Genom intervjuerna kontrolleras till exempel hur personalen hanterar konfidentiell in- |

formation. Dessutom kan man på plats inspektera förvaringsplatser, förvaringssätt och praxis för eliminering, eller utnyttja material som aktören lämnat in.

**Motiveringar**

Oavsam hantering eller överföring av information kan avslöja den för obehöriga användare. Det kan också finnas lagstiftningskrav på konfidentiell information, till exempel EU:s allmänna dataskyddsförordning (EU) 2016/679[12] eller sektorsspecifika krav. Om terminalutrustning och lagringsmedier försvinner till exempel vid stölder, är det viktigt att den stulna enheten är krypterad. Då kan inte obehöriga användare få tillgång till informationen i enheten.

**Källor**

CCB CYFUN Basic (PR.DS-1, PR.DS-2)

ISO/IEC 27002:2022 (5.12, 5.14, 5.33, 5.34, 7.1, 7.9, 7.10, 8.3, 8.24)

IEC 62443-2-1:2010 (4.3.4.4)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, NET 1.1, ORG 1.1, ORG 3.1, USER 1.11)

IEC 62443-2-4:2024 (SP.03.10)

IEC 62443-3-3:2013 (SR 4.1, SR 4.3)

NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.DS-5, PR.IP-6)

NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.DS-10)

**Verktyg**

Kartläggning av angreppsytan Hyöky.fi

Julkri (TEK-16, TEK-18)

Cybermätaren (THIRD-PARTIES-2, ARCHITECTURE-5, ARCHITECTURE-6)

## 11.9 Aktören har sett till att systemen uppdateras regelbundet och kritiska uppdateringar installeras utan dröjsmål

**Exempel på genomförande**

[12] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

Denna grundläggande informationssäkerhet leder till punkterna 3.2, 3.4 och 5.3.

- Aktören har praxis för att följa upp kritiska säkerhetsuppdateringar för operativsystem, applikationer och programvara som används och installera dem utan dröjsmål till exempel med automatiska uppdateringar. Praxisen kan också omfatta sårbarhetsskanningar.
- Aktören har utarbetat ändamålsenliga skriftliga anvisningar för kritiska säkerhetsuppdateringar.
- System som inte kan uppdateras ska skyddas med andra metoder och uppdateringarna ska installeras kontrollerat när det är möjligt.
- Även andra än kritiska säkerhetsuppdateringar görs med regelbundna intervaller, till exempel månatligen när systemleverantören publicerar nya uppdateringar.

## Verifiering

1. Tillsynsmyndigheten verifierar aktörens uppdateringspraxis och dokumenteringen av uppdateringarna. Dessutom inspekteras praxis för att upptäcka behovet av uppdatering. Tillsynsmyndigheten inspekterar även hur incidenter i uppdateringarna hanteras. Detta kan genomföras till exempel genom att dokumentera incidenter eller med riskhanteringsmetoder.

## Motiveringar

Sårbarheter i programvara är ett vanligt sätt att sprida skadliga program, och de kan möjliggöra till exempel missbruk av systemet eller otillåten åtkomst till systemet genom att utnyttja sårbarheten. Omfattande utnyttjande i synnerhet av kritiska sårbarheter sker ofta snabbt och därför är det mycket viktigt att installera kritiska säkerhetsuppdateringar utan dröjsmål. System som inte kan uppdateras kan vara mycket sårbara och de ska skyddas till exempel genom att differentiera dem från andra system.

## Källor

CCB CYFUN Basic (PR.MA-1)

ISO/IEC 27002:2022 (8.8, 8.19, 8.32)

IEC 62443-2-1:2010 (4.3.4.3.7)

IEC 62443-2-1:2024 (COMP 3.1, COMP 3.2, COMP 3.3, COMP 3.4, COMP 3.5, EVENT 1.9, ORG 2.4, CM 1.4)

IEC 62443-2-4:2024 (SP.11.01, SP.11.02, SP.11.03, SP.11.04, SP.11.05)

NIST CSF 1.1 (PR.IP-3, PR.MA-1)

NIST CSF 2.0 (PR.PS-01, PR.PS-02, PR.PS-03)

## Verktyg

| |
|---|
| Kartläggning av angreppsytan Hyöky.fi |
| Julkri (TEK-17, TEK-19) |
| Cybermätaren (ASSET-4, THREAT-1) |

## 11.10 Aktören har sett till att tjänsterna och enheterna är säkert konfigurerade

**Exempel på genomförande**

Denna grundläggande praxis för informationssäkerhet leder till punkt 3.3.

- Aktören har praxis för att ta bort onödiga egenskaper i sina system. De inbegriper bland annat avstängning av extra tjänster eller enheter eller att de tas ur bruk.
- Aktören har ändrat standardinställningar såsom standardlösenord i sina system eller enheter och förvarar de uppdaterade lösenorden säkert. Om aktören har skapat användarnamn för nödsituationer ska man se till att de att de skyddas, deras användningsgrund och tillgänglighet i anslutning till nödsituationer.
- Aktören har tagit i bruk de säkerhetsfunktioner som de använda systemen tillhandahåller. De kan till exempel vara automatiska programuppdateringar, säkra kontrollmetoder, kryptering och ibruktagande av händelseregistrering (logg).

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har praxis för att kontrollera enheternas konfiguration innan de tas i bruk och vid behov i samband med uppdateringar. Dessa förfaranden inbegriper borttagning av onödiga och osäkra egenskaper samt ändringar i osäkra standardinställningar. Många enheter har säkerhetsegenskaper som lätt kan tas i bruk som aktören som en del av denna process bör ta i bruk, till exempel kryptering av arbetsstationernas lagringsmedier, automatiska uppdateringar, säkra hanteringsförbindelser och protokoll som använder kryptering.

**Motiveringar**

Borttagning av onödiga egenskaper minskar angreppsytan och minskar angriparens möjligheter att komma in i aktörens system. Till exempel standardanvändarnamn och standardlösenord är sådana som utnyttjas i stor utsträckning i samband med automatiserad skanning. Vilken som helst enhet eller tjänst kan möjliggöra åtkomst även till kritiska system eller så kan enheten utnyttjas för brottslig verksamhet. Oskyddade enheter, såsom övervakningskameror kan avslöja konfidentiell information.

| Källor |
|---|
| ISO/IEC 27002:2022 (8.9, 8.27, 8.32) |
| IEC 62443-2-1:2024 (ORG 2.3, CM 1.4) |
| IEC 62443-2-4:2024 (SP.03.05) |
| IEC 62443-3-3:2013 (SR 7.6, SR 7.7) |
| NIST CSF 1.1 (PR.IP-1, PR.IP-3) |
| NIST CSF 2.0 (PR.PS-01, PR.PS-02, PR.PS-03) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi |
| Julkri (TEK-10) |
| Cybermätaren (ASSET-3, ARCHITECTURE-3, SITUATION-1) |

## 11.11 Aktören har sett till att kritiska tjänster och dataegendom är säkerhetskopierade

| Exempel på genomförande |
|---|
| Denna grundläggande praxis för informationssäkerhet leder till punkterna 10.2 och 10.3.<br>• Aktören har praxis för att göra säkerhetskopior, återhämtningspraxis och hantering av säkerhetskopiornas livscykel. Om säkerhetskopior innehåller data som omfattas av lagstadgade krav har aktören praxis även för att eliminera säkerhetskopior vid rätt tid.<br>• Kritiska datalager har säkerhetskopierats regelbundet. Säkerhetskopior har differentierats fysiskt och logiskt från de system de har säkerhetskopierats. Säkerhetskopior har skyddats minst med förfaranden på motsvarande nivå som ursprungligt data.<br>• Återställning av säkerhetskopior har testats regelbundet. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har praxis för att genomföra säkerhetskopiering av datalager som definierats som viktiga för verksamheten. Av praxisen framgår även hur säkerhetskopior har skyddats och hur de har differentierats från systemen som säkerhetskopieras. Aktören har även dokumenterat metoder för hur funktionen hos säkerhetskopior testas regelbundet. |

2. Tillsynsmyndigheten verifierar till exempel genom intervjuer, uppgifter som aktören lämnat in eller inspektion att praxis som gäller säkerhetskopior verkställs. Uppgifterna som lämnas in kan till exempel vara skärmdumpar, konfigurationer och händelseloggar i säkerhetskopiorna och deras praxis. Fysisk inspektion kan inbegripa till exempel inspektion av var säkerhetskopieringssystemet finns eller lagringsmediernas förvaringsplats och inspektion av dess säkerhet.

**Motiveringar**

Säkerhetskopior skyddar mot avsiktlig eller oavsiktlig förlust av information. Med hjälp av säkerhetskopior kan systemet vid behov återställas även i en situation när till exempel hela systemet har krypterats av en angripare. I dessa fall är det i synnerhet viktigt att angriparen dessutom inte kan kryptera säkerhetskopior.

Det är bra att testa återställning regelbundet, eftersom det ofta finns fel i säkerhetskopiorna och återställningen misslyckas. Systemet behöver ofta återställas vid allvarliga störningssituationer. Det lönar sig att planera återhämtning från störningssituationer som en helhet, till exempel som en del av kontinuitets- och återhämtningsplaneringen.

**Källor**

CCB CYFUN Basic (PR.IP-4)

ISO/IEC 27002:2022 (5.30, 8.10, 8.13)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (AVAIL 1.1, AVAIL 2.1, AVAIL 2.3, DATA 1.4, EVENT 1.8)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02)

IEC 62443-3-3:2013 (SR 7.3)

NIST CSF 1.1 (PR.IP-4, PR.IP-6, PR.IP-9, PR.IP-10)

NIST CSF 2.0 (PR.DS-11)

NIST SP 800-82 rev 2

**Verktyg**

Julkri (TEK-20, TEK-22)

Cybermätaren (CRITICAL-1, CRITICAL-2, RESPONSE-4, RESPONSE-5, ASSET-2, ARCHITECTURE-5)

## 11.12 Aktören har förberett sig på hur verksamheten kan upprätthållas vid allvarliga incidenter

| **Exempel på genomförande** |
|---|
| Denna grundläggande praxis för informationssäkerhet leder till punkt 9.7.<br>• Aktören har skriftlig praxis för att fastställa ansvar och åtgärder i synnerhet med tanke på allvarliga incidenter.<br>• Aktören har skriftlig praxis för att göra en NIS-anmälan eller annan myndighetsanmälan vid incidenter. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har skriftlig praxis för incidenter. Av praxisen framgår anmälningsskyldigheter, aktuella och konkreta kontaktuppgifter och kontaktkanaler till interna och externa kontakter, ansvar och skyldigheter, eventuella användarnamn vid nödsituationer samt verksamhetsanvisningar.<br>2. Om aktören har haft incidenter kontrollerar tillsynsmyndigheten praxisen för aktörens incidenthantering till exempel med hjälp av intervjuer och dokumentation i anknytning till incidenthanteringen. Det ska särskilt kontrolleras att incidenthanteringen har varit tillräcklig och att man utrett hotet eller typen av grundläggande orsak som sannolikt har orsakat incidenten och att lagstadgade skyldigheter har genomförts i incidenthanteringen, såsom incidentanmälningar. De kan kontrolleras till exempel i material som aktören lämnat in, såsom slutrapporten över incidenten. |
| **Motiveringar** |
| Välplanerade tillvägagångssätt och praxis vid incidenter förkortar återhämtningstiden. Praxis i fråga om anmälningsskyldigheter säkerställer att lagstadgade anmälningar till exempel enligt NIS 2-direktivet inte glöms bort vid en incident. |
| **Källor** |
| CCB CYFUN Basic (RS.RP-1, RC.RP-1, RC.CO-3)<br>ISO/IEC 27002:2022 (5.5, 5.24, 5.26)<br>IEC 62443-2-1:2010 (4.3.4.5)<br>IEC 62443-2-1:2024 (ORG 1.3, EVENT 1.8)<br>IEC 62443-2-4:2024 (SP.01.05, SP.01.06, SP.12.09)<br>NIST CSF 1.1 (RS.RP, RC.RP, RC.CO-3)<br>NIST CSF 2.0 (RS.MA-05, RC.RP-02, RC.CO-03) |

| **Verktyg** |
| --- |
| Julkri (HAL-08)<br>Cybermätaren (RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-5) |

### 11.13 Aktören har i bruk registrering av händelser (logg) i fråga om kritiska funktioner

| **Exempel på genomförande** |
| --- |
| Denna praxis för grundläggande informationssäkerhet leder till punkt 9.3<br>• Aktören har säkerställt att händelser i anknytning till kritiska funktioner registreras.<br>• Händelseregistreringar uppkommer till exempel av huvudanvändarnas åtgärder och ändringar i anknytning till åtkomsträttigheter samt i mån av möjlighet av alla händelser som hänför sig till säkerhet i hela kommunikationsnätet och informationssystemet.<br>• Händelseregistreringar uppkommer också vid hantering av konfidentiell information som grundar sig till exempel på krav i lagstiftningen.<br>• Det skulle vara bra om händelseregistreringen åtminstone besvarar följande frågor i mån av möjlighet: vem, vad, varifrån, när, vart.<br>• Händelseloggen är skyddad från ändringar och den hanteras med separata användarnamn. Händelseloggen har säkerhetskopierats med regelbundna intervaller eller kopierats till ett separat system. |
| **Verifiering** |
| 1. Tillsynsmyndigheten verifierar att aktören har bestämt behovet av loggar och vid behov informationssystemets och kommunikationsnätets loggarkitektur. Loggsystemets omfattning har relaterats till aktörens behov.<br>2. Tillsynsmyndigheten verifierar till exempel i material som aktören lämnat in eller genom inspektion att loggen skapas minst för objekt och funktioner som är centrala för verksamheten och att den förvaras säkert så att loggen inte kan ändras utan tillstånd. |
| **Motiveringar** |
| Händelseregistreringar (loggar) är väsentliga vid störningssituationer för att utreda händelseförloppet. Utan ordentliga händelseregistreringar kan det vara omöjligt att utreda den grundläggande orsaken till störningen.<br><br>Säkerhetskopiering av händelseregistreringar är viktigt särskilt när det gäller utpressningsprogram, eftersom de ofta krypterar hela lagringsmediet. Om det blir |

| |
|---|
| verklighet kan inte händelseloggen längre läsas om den inte separat har säkerhetskopierats eller överförts till ett system som angriparen har åtkomst till. |
| **Källor** |
| CCB CYFUN Basic (PR.PT-1, DE.AE-3)<br>ISO/IEC 27002:2022 (5.28, 5.34, 8.15)<br>IEC 62443-2-1:2010 (6.10.1, 6.10.3)<br>IEC 62443-2-1:2024 (EVENT 1.4, DATA 1.1, DATA 1.2)<br>IEC 62443-2-4:2024 (SP.08.02, SP.08.03)<br>NIST CSF 1.1 (PR.PT-1, DE.AE-3)<br>NIST CSF 2.0 (PR.PS-04, DE.CM-01)<br>Transport- och kommunikationsverkets anvisning om dokumentation av uppgifter som gäller behandling av förmedlingsuppgifter (Traficom/376384/03.04.05.01/2022) |
| **Verktyg** |
| Kartläggning av angreppsytan Hyöky.fi<br>Julkri (TEK-12)<br>Cybermätaren (ASSET-4, ACCESS-3, SITUATION-1, RESPONSE-4) |

# 12 Åtgärder för att säkerställa den fysiska miljön, lokalsäkerheten och nödvändiga resurser i fråga om kommunikationsnät och informationssystem

Rekommendationerna grundar sig på artikel 21.2 i NIS 2-direktivet i fråga om åtgärder för att skydda den fysiska miljön i kommunikationsnät och informationssystem. Om nationellt genomförande av denna föreskrivs i 9 § 2 mom. 12 punkten i cybersäkerhetslagen och 18 c § 1 mom. 12 punkten i informationshanteringslagen.

1. **Lokalsäkerhet och fysisk åtkomstövervakning:** Aktören ska identifiera faktorer i den fysiska miljön vars säkerhet är viktig med tanke på kommunikationsnätens och informationssystemens funktion och skydda dem mot effekterna och störningarna av dessa fysiska hot. Aktören ska också beakta fysiska miljöer som påverkar kommunikationsnät och informationssystem. Dessa kan vara mycket olika och till exempel geografiskt omfattande eller begränsade. (Se punkt 12.1).

2. **Skydd mot fysiska hot och hot som miljön orsakar:** Fysiska hot är miljöfaktorer och illvilliga aktörer. Kommunikationsnäten och informationssystemen kan till exempel övervakas och skyddas mot obehörig fysisk åtkomst, skada och störning. Dessutom måste man skydda sig mot naturrelaterade och sociala händelser, såsom eldsvådor, översvämningar och oroligheter. (Se punkt 12.2).

3. **Säkerställande av kontinuiteten för resurser som är nödvändiga för verksamheten:** Aktören ska förbereda sig på störningar i de nödvändiga resurserna, såsom eldistributionen, datakommunikationsförbindelserna och kylningen, och förhindra att kommunikationsnät och informationssystem förstörs eller skadas eller att aktörens kritiska funktioner avbryts på grund av brist på nödvändiga resurser eller på grund av störningar. (Se punkt 12.3).

## 12.1 Lokalsäkerhet och fysisk åtkomstövervakning

| **Exempel på genomförande** |
|---|
| • Aktören har identifierat de mest kritiska områdena för kommunikationsnät och informationssystem. Aktören har skyddat områden som är kritiska för säkerheten mot obehörig åtkomst samt mot andra skador och störningar.<br>• Kritiska områden kan till exempel vara kontorslokaler, serverlokaler och andra tekniska lokaler. Beroende på aktören kan det till exempel vara nödvändigt att avgränsa gårdsområdet i närheten av aktörens lokaler till exempel med staket. Till exempel kan energi-, datakommunikations- och trafikförbindelser täcka geografiskt mycket stora områden och har kunnat byggas under årtionden. Effekterna av riskhanteringen inom lokalsäkerheten och storleken på de kvarstående riskerna bör särskilt följas upp. |

- Tillträde till kritiska områden är begränsad endast till behöriga personer med hjälp av åtkomstövervakning. Åtkomstövervakning kan genomföras till exempel genom att låsa dörrar, strukturella hinder, larm och bevakning.
- I mån av möjlighet har händelselogg använts för åtkomstövervakningen. Av händelseregistreringen ska framgå vem som har passerat en viss dörr eller passage, vilken tid och på vilket sätt till exempel en eventuell dörrlåsning har öppnats. Händelseregistreringarna kan vara automatiska eller på papper.
- De viktigaste dörrarna och passagen har vid behov övervakats med inspelningsbar kameraövervakning. Behovet av övervakning grundar sig på riskbedömning av aktören (se 1).
- Aktören har särskilt beaktat åtkomstövervakning för tredje parts personer.
- Aktören har praxis som fastställer hur besökare ska gå till ett säkerhetskritiskt område, hur de ska röra sig på och lämna området.
- Aktören har vid behov bestämt annan praxis i anknytning till lokalsäkerheten, såsom principerna rent bord och skärm, synliggörande av identifikationer och förhindrande av att besökare kommer in i lokalen i samband med dörröppning (tailgating).
- Aktören har praxis för säker återanvändning, återvinning eller annan eliminering av föråldrad eller annan utrustning som tagits ur bruk eller lagringsmedier. Mer information i punkt 5 Tillgångsförvaltning.

## Verifiering

1. Tillsynsmyndigheten verifierar att aktören har dokumenterat de mest kritiska områden med tanke på kommunikationsnätens och informationssystemens säkerhet och principerna för deras åtkomsthantering. Av principerna framgår fastställandet av kritiska områden i enlighet med riskbedömningen samt till exempel praxis för passerkontroll och andra principer i anknytning till lokalsäkerheten, principer för loggregistrering och eventuell kameraövervakning. Principerna ska i mån av möjlighet omfatta aktörens alla lokaler där det finns kommunikationsnät och informationssystem.
2. Tillsynsmyndigheten verifierar aktörens lokalsäkerhet och skydd när det gäller kommunikationsnät och informationssystem genom att inspektera till exempel förmågan hos den fysiska passerkontrollen i aktörens lokaler. Myndigheten kan till exempel fästa uppmärksamhet vid kameraövervakning och dess omfattning, passerkontroll och serverutrustningens placering samt deras fysiska skydd.

## Motiveringar

Tillträde av obehöriga personer till aktörens kritiska lokaler kan äventyra verksamhetens konfidentialitet, riktighet eller tillgänglighet. I synnerhet lokaler där aktören förvarar skyddade tillgångar, personuppgifter eller säkerhetsklassificerad information ska skyddas från utomstående personer.

## Källor

| |
|---|
| ISO/IEC 27002:2022 (7.1, 7.2, 7.4)<br>IEC 62443-2-1:2024 (ORG 3.1, AVAIL 1.1, AVAIL 1.2, EVENT 1.1)<br>NIST CSF 1.1 (PR.AC-2, DE.CM-2)<br>NIST CSF 2.0 (PR.AA-06, DE.CM-02)<br>”Digital säkerhet i byggnader” anvisningar (RT 103206 [ST 70.40], RT 103207 [ST 70.41] och RT 103208 [ST 95.12])<br>NIS CG Reference document (3.13.1 Perimeter and physical access control)<br>NIS CG Implementing guidance (13.3. Perimeter and physical access control) |
| **Verktyg** |
| Julkri (FYY-02, FYY-07, TEK-09)<br>Cybermätaren (CRITICAL-1, ACCESS-3, ARCHITECTURE-3) |

## 12.2 Skydd mot fysiska hot och hot som miljön orsakar

**Exempel på genomförande**

- Aktören har i sin verksamhet beaktat både fysiska och miljörelaterade hot mot kommunikationsnät och informationssystem och dimensionerat sina riskhanteringsåtgärder i relation till den egna verksamheten i rådande förhållanden, genom att övervaka och skydda dem mot olovlig fysisk åtkomst, skador och störningar. Dessa hot kan uppkomma genom avsiktliga eller oavsiktliga fysiska handlingar eller naturkatastrofer. Sådana risker kan till exempel vara bränder, översvämningar, stormar, vandalism eller terrorism.
- Åtgärder som bidrar till att minska riskerna och skydd mot fysiska och hot som orsakas av miljön kan till exempel vara automatiska släckningssystem, brandsektionering, säkerställande och rätt dimensionering av byggnadens strukturella styrka, skydd i anslutning till husteknik och fastighetsautomation, såsom uppföljning av temperaturen och fuktigheten, överspänningsskydd. Om risken hanteras genom att mäta storheter (t.ex. värme eller luftfuktighet) bör tydliga gränsvärden fastställas för dem. Om dessa överskrids eller underskrids utlöses larm eller andra åtgärder.
- Aktörens riskhantering ska hantera de ovannämnda hoten utifrån ett tillvägagångssätt som beaktar alla riskfaktorer. Läs mer i punkt 1.2 Förhållningssätt som beaktar alla riskfaktorer.
- I händelse av olyckor eller andra störningar har aktören utvärderat sin riskhantering i anknytning till det och att den är proportionerlig. Aktören har vid behov uppdaterat sina tillvägagångssätt för att förhindra att händelserna i fråga inte sker på nytt.

| **Verifiering** |
|---|
| 1. Tillsynsmyndigheten verifierar att aktören i sin riskhantering och kontinuitetsplanering har beaktat fysiska och hot som miljön orsakar mot kommunikationsnät och informationssystem. Risker som direkt äventyrar verksamheten har hållits i styr med lämpliga hanteringsmetoder. Aktören ska uppfylla eventuella lagstadgade krav till exempel när det gäller brandskyddet. |
| **Motiveringar** |
| Fysiska hot och hot som miljön orsakar kan utgöra en risk för verksamhetens kontinuitet. I värsta fall kan hoten påverka aktören så att affärsverksamheten inte längre kan fortsätta. |
| **Källor** |
| ISO/IEC 27002:2022 (7.3, 7.5)<br>IEC 62443-2-1:2024 (ORG 3.1, AVAIL 1.2)<br>NIST CSF 1.1 (PR.IP-5)<br>NIST CSF 2.0 (PR.IP-02)<br>”Digital säkerhet i byggnader” anvisningar (RT 103206 [ST 70.40], RT 103207 [ST 70.41] och RT 103208 [ST 95.12])<br>NIS CG Reference document (3.13.2 Protection against physical and environmental threats)<br>NIS CG Implementing guidance (13.2. Protection against physical and environmental threats) |
| **Verktyg** |
| Julkri (FYY-02)<br>Kybermittari (CRITICAL-2, THREAT-2, RISK-2, RISK-3, RISK-4, ACCESS-2, RESPONSE-3) |

## 12.3 Säkerställande av kontinuiteten för resurser som är nödvändiga för verksamheten

| **Exempel på genomförande** |
|---|

- Aktören har beaktat kontinuiteten för resurser som är nödvändiga för kommunikationsnäten och informationssystemens funktion (stödtjänster). Dessa omfattar till exempel elförsörjning, vatten- och gasdistribution, kylning, avlopp och telekommunikationsförbindelser.
- Aktören har ställt risker, som orsakas av störningar i stödtjänsterna, i relation till sin verksamhet och kompenserat dem vid behov till exempel i händelse av elavbrott med reservkraftsgenerator, batteribackup eller alternativa kraftkällor. Telekommunikationsförbindelserna ska vid behov vara feltoleranta, till exempel genom reservförbindelser. Undantagsarrangemangen kan vid behov stödas med hjälp av externa partners avtalsförhållanden, till exempel för att säkerställa tillgången till bränsle för reservkraftgeneratorer.
- Aktören har uppdaterat och upprätthållit sina instruktioner regelbundet och vid behov efter en störning för att man i fortsättningen kan undvika störningar eller följderna av dem.
- Aktören har tydliga instruktioner för allvarliga störningssituationer.
- Aktören har övervakat stödtjänsternas situation och följt störningsmeddelanden i anknytning till dem. Aktören ska ha uppdaterade kontaktuppgifter till leverantörer av stödtjänster i händelse av störningssituationer.
- Aktören bör öva och testa sina reservsystem regelbundet. Övningarna har planerats omsorgsfullt och i övningarna har man säkerställt att simulering av en störningssituation inte medför verklig fara för verksamheten eller miljön.

**Verifiering**

1. Tillsynsmyndigheten verifierar att aktören har beredskap för störningar i fråga om de nödvändiga resurserna, såsom eldistributionen, telekommunikationsförbindelserna och kylningen, och förhindrat att kommunikationsnät och informationssystem förstörs eller skadas eller att aktörens kritiska funktioner avbryts på grund av brist på nödvändiga resurser eller på grund av störningar. Aktören har uppskattat nödvändiga resurser som behövs för verksamheten och kontinuiteten och vid behov bestämt hanteringsmetoder för att kompensera de risker som är förenade med dem. Hanteringsmetoderna kan till exempel vara behövliga avtal om reservarrangemang, separata reservförbindelser och planer för att ta dem i bruk.
2. Tillsynsmyndigheten verifierar att reservarrangemangen för resurser som är nödvändiga för aktörens verksamhet har testats eller att man i praktiken övat verksamhet utifrån reservarrangemangen.

**Motiveringar**

Störningar i stödtjänsterna kan orsaka även långa avbrott eller störningar för aktörens verksamhet, som kan skada ryktet eller äventyra verksamhetens kontinuitet. Avvikande situationer är mycket olika och kan orsaka förlust av information eller andra skador. Avvikande situationer kan till exempel vara elavbrott, problem i utrustningens kylning och vattenskador.

| **Källor** |
| --- |
| ISO/IEC 27002:2022 (7.11) |
| IEC 62443-2-1:2024 (AVAIL 1.2, ORG 1.6) |
| IEC 62443-2-4:2024 (SP.08.04) |
| NIST CSF 1.1 (ID.BE-1, ID.BE-2, ID.SC-2) |
| NIST CSF 2.0 (GV.OC-01, GV.OC-05, GV.SC-03, PR.IR-03, PR.IR-04) |
| ”Digital säkerhet i byggnader” anvisningar (RT 103206 [ST 70.40], RT 103207 [ST 70.41] och RT 103208 [ST 95.12]) |
| NIS CG Reference document (3.13.3 Supporting utilities) |
| NIS CG Implementing guidance (13.1. Supporting utilities) |
| **Verktyg** |
| Julkri (VAR-05, VAR-07) |
| Cybermätaren (CRITICAL-3, RESPONSE-3, RESPONSE-4, RESPONSE-5, THIRD-PARTIES-1, THIRD-PARTIES-2, Allmänna förvaltningsåtgärder) |

# III Källor

## Författningar och anvisningar som hänför sig till rekommendationen

Nationella

Lag om riskhantering inom cybersäkerhet (124/2025)

Lag om ändring av lagen om informationshantering inom den offentliga förvaltningen(125/2025)

Lag om informationshantering inom den offentliga förvaltningen (906/2019, informationshanteringslagen)

Transport- och kommunikationsverkets föreskrift om televerksamhetens informationssäkerhet (M67) (TRAFICOM/248815/03.04.05.00/2022)

Anvisning av Myndigheten för digitalisering och befolkningsdata: Handbok om säker applikationsutveckling (på finska). Publicerad 19.5.2020.

Transport- och kommunikationsverkets anvisning om dokumentation av uppgifter som gäller behandling av förmedlingsuppgifter (Traficom/376384/03.04.05.01/2022)

Finansministeriets publikationer 2023:54: Handbok för riskhantering för aktörer inom statsförvaltningen (på finska): https://urn.fi/URN:ISBN:978-952-367-633-6

Finansministeriets publikationer 2023:57: Rekommendation om informationssäkerhet vid upphandling, målgrupp informationshanteringsenheter och myndigheter: https://urn.fi/URN:ISBN:978-952-367-647-3

Internationella

Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet, cybersäkerhetsdirektivet)

NIS Cooperation Group: NIS CG Reference document (on security measures for important & essential entities

## Standarder och referensramar som hänför sig till rekommendationen

Nationella

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri): Rekommendation och kriterier: http://urn.fi/URN:ISBN:978-952-367-462-2

Transport- och kommunikationsverkets Cybermätare: cybermataren.fi

Internationella

CCB CYFUN (CyberFundamentals) Framework Basic

COSO Enterprise Risk Management Framework

IEC 62443-2-1:2013 Telekommunikationsnät inom industrin. Informationssäkerhet i nätverk och system. Del 2-1: Grundande av informationssäkerhetsprogram för industriautomations- och styrningssystem

IEC 62443-2-4:2019 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

IEC/TR 62443-3-1:2013 Telekommunikationsnät inom industrin. Informationssäkerhet i nätverk och system. Del 3-1: Informationssäkerhetsteknik för industriautomations- och styrningssystem

IEC 62443-3-3:2019 Industrial communications networks - Network and system security - Part 3-3: System security requirements and security levels

IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

ISO/IEC 27001:2022 Informationssäkerhet, cybersäkerhet och dataskydd. Ledningssystem för informationssäkerhet. Krav

ISO/IEC 27002:2022 Informationssäkerhet, cybersäkerhet och dataskydd. Metoder för hantering av informationssäkerhet.

ISO/IEC 27003:2018 Informaatioteknologia. Säkerhetsteknik. Ledningssystem för informationssäkerhet. Instruktioner

ISO/IEC 27005:2022 Informationssäkerhet, cybersäkerhet och dataskydd. Instruktioner för hantering av datasäkerhetsrisker

ISO/IEC 27035-1:2023 Information technology - Information security incident management - Part 1: Principles and process

ISO/IEC 27035-2:2023 Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response

ISO 31000:2018 Riskhantering. Anvisningar

NIST CSF 1.1 Cybersecurity framework 1.1

NIST CSF 2.0 Cybersecurity framework 2.0

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: https://doi.org/10.6028/NIST.SP.800-53r5

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide: https://doi.org/10.6028/NIST.SP.800-61r2

NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security: https://doi.org/10.6028/NIST.SP.800-82r3

OWASP Application Security Verification Standard

OWASP Top Ten

The STRIDE Threat Model

The DREAD risk assessment model

### Övriga publikationer

Cybersäkerhetscentret vid Transport- och kommunikationsverket: Sårbarheter – att anmäla sårbarheter på korrekt sätt

Cybersäkerhetscentret vid Transport- och kommunikationsverket: Så här samlar du in och använder loggdata

Cybersäkerhetscentret vid Transport- och kommunikationsverket: Anvisning om cyberövningar

Cybersäkerhetscentret vid Transport- och kommunikationsverket: Process för samordnad publicering av sårbarhetsinformation CVD

NSA, CISA: Identity and Access Management: Recommended Best Practices for Administrators

## Bilaga 1 Korsreferenstabel

Korsreferenstabel med exempel på välkända standarder, ramverk och riktlinjer med ankytning till denna rekommendation