Livsmedelsverket

Dnr 2023/01237

Vägledning till Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn produktion och distribution av dricksvatten

Författare:
Livsmedelsverket

Rekommenderad citering:
Livsmedelsverket. 2023. Citering: Vägledning till Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn produktion och distribution av dricksvatten. Livsmedelsverkets. Uppsala.

ISSN 1104-7089

Omslag: Livsmedelsverket

Innehåll

1. Inledning

Europaparlamentet och rådet antog 2016 ett direktiv om säkerhetsåtgärder avseende nätverks- och informationssystem, det så kallade NIS-direktivet (Europaparlamentet och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen). För genomförande av direktivet antogs i juni 2018 lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (i det följande benämnd som NIS-lagen) samt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen). Syftet med lagstiftningen är att uppnå en hög nivå av säkerhet i nätverk och informationssystem som används för tillhandahållandet av samhällsviktiga tjänster. Bestämmelserna kompletteras med föreskrifter från MSB och från respektive tillsynsmyndighet. Livsmedelsverket har i egenskap av tillsynsmyndighet på området leverans och distribution av dricksvatten meddelat Livsmedelsverkets föreskrifter (LIVSFS 2022:2) om *informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten*.

I december 2022 antogs det så kallade NIS2-direktivet (Europaparlamentet och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen), som ska ersätta det ursprungliga NIS-direktivet. Nationella bestämmelser som genomför direktivet ska börja tillämpas hösten 2024. Det medför att nuvarande lag, förordning och myndighetsföreskrifter, i åtminstone viss utsträckning, kommer att ersättas eller ändras framöver. Livsmedelsverkets nuvarande föreskrifter om säkerhetsåtgärder gäller tillsvidare och ska efterlevas tills att eventuella ändringar meddelas.

Detta dokument utgör en vägledning och ska ses som ett komplement till Livsmedelsverkets föreskrifter. Vägledningen utgör inte bindande regler, utan innehåller rekommendationer och förslag om hur de leverantörer som omfattas av NIS-lagen inom sektorn leverans och distribution av dricksvatten kan göra för att följa föreskrifterna.

1.1 Vägledningens målgrupp

Vägledningens primära målgrupp är de som aktivt arbetar med att upprätthålla IT- och informationssäkerheten i de nätverk och informationssystem som används för leverans och distribution av dricksvatten. Detta inkluderar roller som leder informationssäkerhetsarbetet, exempelvis informationssäkerhetssamordnare, CISO eller motsvarande.

1.2 Bakgrund till föreskrifterna

Dricksvattenförsörjningen är beroende av industriella informations- och styrsystem som av olika orsaker i allt högre grad kopplas samman med andra nätverk och informationssystem. Sådana sammankopplingar kan leda till ökad komplexitet och kan introducera nya risker och hot. Eftersom många IT-system idag har kopplingar mot Internet, externa leverantörer och

olika tjänsteleverantörer, kan antagonistiska hot vara lika relevanta som hot av mer intern karaktär, till exempel misstag eller oförmåga att hantera plötsligt ansträngda driftsförhållanden.

Komplexitet i informationssystem och nätverk, samt hot och risker varierar mellan olika leverantörer. Enligt NIS-lagen ska säkerhetsarbetet vara riskbaserat, vilket innebär att säkerhetsarbetet ska anpassas efter leverantörens verksamhet och därmed förknippade risker. Det betyder att leverantörer som omfattas av NIS-lagen, utöver de fall där NIS-lagen eller tillhörande föreskrifter ställer krav på specifika säkerhetsåtgärder, ska utgå från sina egna omständigheter i sitt informationssäkerhetsarbete.

2. Föreskrifternas inledande bestämmelser

1 § I dessa föreskrifter finns bestämmelser om informationssäkerhetsåtgärder som kompletterar 12-14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

2 § Dessa föreskrifter gäller leverantörer som omfattas av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster och som tillhandahåller sådana samhällsviktiga tjänster som identifierats inom sektorn leverans och distribution av dricksvatten i enlighet med 3 § förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
Enligt 8 och 9 §§ lagen om informationssäkerhet för samhällsviktiga och digitala tjänster gäller den lagen inte verksamhet som omfattas av säkerhetsskyddslagen (2018:585) och lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska, under vissa förutsättningar, inte heller tillämpas om det i annan lag eller författning finns bestämmelser om krav på säkerhetsåtgärder och incidentrapportering.

2.1 Vem föreskrifterna berör

De första två paragraferna i föreskrifterna är avsedda att tydliggöra vad föreskrifterna handlar om och vilka som berörs av den.

2.2 Förhållandet till annan lagstiftning

NIS-lagen gäller inte för verksamhet som omfattas av säkerhetsskyddslagen (2018:585) eller annan författning som innebär minst motsvarande krav på säkerhetsåtgärder och incidentrapportering (se 8 – 9 §§ NIS-lagen). Motsvarande gäller Livsmedelsverkets föreskrifter. För samhällsviktiga tjänster i sektorn leverans och distribution av dricksvatten är det primärt säkerhetsskyddslagen som överlappar med NIS-lagens tillämpningsområden.

Att en leverantör av samhällsviktiga tjänster bedriver verksamhet som omfattas av säkerhetsskyddslagens krav på säkerhetsskydd betyder inte nödvändigtvis att all verksamhet leverantören bedriver är undantagen från NIS-lagen. De delar av leverantörens verksamhet som inte är säkerhetskänslig kan fortfarande falla under NIS-lagen.

Det är leverantörens ansvar att avgöra om NIS-lagen är applicerbar, dvs. huruvida verksamhetens säkerhetsåtgärder och incidentrapportering ska anpassas enligt NIS-lagen. Det är också leverantörens ansvar att avgöra för vilka delar av verksamheten som kraven i NIS-lagen och tillhörande föreskrifter gäller.

2.3 Definitioner och uttryck i föreskrifterna

3 § Uttryck som används i dessa föreskrifter har samma innebörd som i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

I dessa föreskrifter avses med

1. leverantör: en aktör som tillhandahåller en samhällsviktig tjänst inom sektorn leverans och distribution av dricksvatten,
2. riskägare: person, organisatorisk enhet eller funktion som ansvarar för och har befogenhet att hantera en risk,
3. underleverantör: en aktör som förser en leverantör med produkter eller tjänster och som inte står under leverantörens direkta organisatoriska kontroll.

Definitionen av ”leverantör” fastställs av MSBs föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Riskägare har en central roll i hanteringen av risker. Se kapitel 3.10 för vägledning kring föreskriften om riskägarskap.

Underleverantörer är typiskt aktörer som inte är en del av leverantörens organisation. En underleverantör kan dock också vara en del av leverantörens organisation, t.ex. en IT-avdelning inom en kommun som står under en annan nämnds kontroll.

3. Riskanalyser och åtgärdsplaner

3.1 Förteckning av tillgångar

4 § Leverantören ska föra aktuella förteckningar över

- tillgångar i form av nätverksansluten hård- och mjukvara,
- förbindelser i form av kommunikationslänkar,
- beroenden till underleverantörer, och
- de organisatoriska enheter (delar av den egna organisationen) som kan påverka säkerheten i de nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten.

Sådana förteckningar ska omfatta en aktuell kartläggning av logiska samband och kommunikationer till och från systemkomponenter.

Leverantören ska upprätthålla förteckningar över de förbindelser och tillgångar som kan påverka säkerheten i de nätverk och informationssystem som används för den samhällsviktiga tjänsten. Förteckningarna ska beskriva de komponenter som används i daglig drift för leverans av tjänsten samt beskriva beroenden till andra verksamheter i den egna organisationen eller till underleverantörer.

God kännedom om den tekniska och organisatoriska miljön samt ett dokumenterat underlag är en förutsättning för användbara riskanalyser och för att kunna vidta ändamålsenliga och tillräckliga säkerhetsåtgärder. Av förteckningarna ska framgå vilka IT-system, nätverksförbindelser, organisatoriska delar som måste anpassas till lagar och föreskrifter kopplade till NIS-lagen, samt underleverantörer som kan påverka säkerheten i de nätverk och informationssystem som används för den samhällsviktiga tjänsten.

Dokumentation av tekniska system

Leverantören ska ha en förteckning över nätverksansluten hård- och mjukvara. Det betyder att de system och den utrustning som används i verksamheten och som är ansluten till nätverk för leverans och distribution av dricksvatten som ska dokumenteras. En förteckning kan till exempel skapas med ett verktyg som skannar nätverket (se kapitel 3.2 gällande risker med skanning) eller genom manuell analys. Många verktyg kan konfigureras för att automatiskt skicka information om nya system eller ny mjukvara som identifieras i samband med skanningsprocessen. Kartläggning kan ske manuellt, men det kräver en noggrann analys av nätverket och en fysisk genomgång av samtliga komponenter som används för tillhandahållandet av den samhällsviktiga tjänsten.

Vidare är det av vikt att hålla förteckningarna uppdaterad och regelbundet kontrollera att den är korrekt. På så sätt ökar möjligheterna att upptäcka komponenter som ska tas bort, antingen från förteckningen eller från IT-miljön.

Kommunikationslänkar som används för tillhandahållandet av den samhällsviktiga tjänsten anses också som tekniska system som ska dokumenteras i förteckningen.

Dokumentation av beroenden till organisationer och leverantörer

Beroenden till underleverantörer kan till exempel vara direkta beroenden till tjänster och personal eller indirekta beroende till underleverantörer som kan påverka säkerheten i styrsystemen eller omkringliggande stödsystem. För att tydliggöra beroendet och vilka risker det medför behöver även den information och de system en underleverantör har tillgång till identifieras. Ett exempel kan vara källkod för system som används för leveransen av dricksvatten som en underleverantör kan ha i sina egna IT-system.

Beroenden till andra verksamheter utanför den samhällsviktiga tjänsten behöver också identifieras, till exempel IT-drift, nätverksadministratörer och fastighetsförvaltning men också underleverantörer som dessa verksamheter använder sig av. Det är inte alltid tydligt om en central IT-avdelning i en kommun ska betraktas som en underleverantör, men beroendet behöver identifieras, dokumenteras och förankras.

Föreskrifterna anger inte hur informationen ska dokumenteras och hela förteckningen behöver inte finnas i samma dokument. Till exempel kan nätverksanslutna komponenter finnas i en separat nätverkskarta. Det centrala är att förteckningen finns tillgänglig för den egna organisationen och att den hålls uppdaterad.

En kartläggning av logiska samband bör bestå av en sammanfattande beskrivning av vilka system som utbyter information och data med varandra, eftersom tekniska beskrivningar på port- och protokollnivå kan vara svåra att använda som underlag för riskanalysen. Kartläggningen ska även identifiera vilka system som utbyter information med system utanför egna nätverk och informationssystem.

Förslag på aktiviteter

För sådant som kan påverka säkerheten i de nätverk och informationssystem som används för den samhällsviktiga tjänsten;

- Kartlägg och dokumentera:
  - nätverksansluten hård- och mjukvara
  - verksamhetens informationsflöden
  - verksamhetens informationstillgångar
  - verksamhetens systemberoenden
  - förbindelser i form av kommunikationslänkar,
  - identifiera vilka system som utbyter information med system utanför egna nätverk
  - anslutningar till organisationens administrativa nätverk
- Identifiera och dokumentera:
  - verksamhetens åtkomst- och anslutningsmöjligheter
  - beroenden till organisationer som är viktiga; exempelvis IT-drift och nätverksadministratörer.
  - beroenden till externa organisationer som tjänsteleverantörer, nätverksleverantörer och konsulter
  - IT-avdelningens roll och möjlighet till att påverka säkerheten i dricksvattenproduktionen, eventuellt kan en IT-avdelning ses som en underleverantör beroende på organisationens utformning
  - beroenden till underleverantörer i andra verksamhetsområden som till exempel fastighetsskötsel, passagesystem, reservkraft, klimatanläggningar etc.
  - trådlösa anslutningar och kommunikationsvägar
- Säkerställ att:
  - De organisationer som identifierats förstår att dricksvattenförsörjningen är beroende av deras verksamhet
  - Avtal och överenskommelser speglar underleverantörers åtaganden

3.2 Sårbarheter

5 § För varje tillgång, förbindelse, underleverantör och organisatorisk enhet som förtecknas enligt 4 § ska kända och potentiella tekniska samt organisatoriska sårbarheter systematiskt kartläggas och dokumenteras, om de kan ha en negativ effekt på de nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten.

Leverantören ska aktivt arbeta med att identifiera sårbarheter som kan påverka säkerheten i informationssystem och nätverk som används för tillhandahållandet av dricksvatten.

Då styrsystem blir sammankopplade i nätverk blir de mer exponerade för hot. För att kunna överblicka vilka risker som finns för styrsystemen och dess stödsystem behöver sårbarheter identifieras i såväl de organisationer som hanterar systemen som i produkter och programvaror som används för att tillhandahålla dricksvatten.

Organisatoriska sårbarheter

Organisatoriska sårbarheter är exempelvis brister i dokumentation för viktiga rutiner eller att funktioner inom verksamheten inte är organisatoriskt separerade i tillräcklig utsträckning. Att separera funktioner i en liten organisation kan vara svårt, dock bör en sådan sårbarhet lyftas för att skapa en medvetenhet i organisationen samt möjliggöra en rimlig riskbedömning. Ett annat exempel på en organisatorisk sårbarhet är när arbetet med dokumentation, uppföljning eller regelefterlevnad blir så betungande att det helt enkelt inte utförs.

En typisk organisatorisk sårbarhet är personberoenden i kritiska roller som innebär att verksamheten får svårt att fortgå utan att dessa nyckelpersoner är tillgängliga. Andra exempel på en organisatorisk sårbarhet är att IT-säkerhetskompetens saknas i den egna organisationen eller att en viktig roll inte har bemannats.

Tekniska sårbarheter

Identifiering av sårbarheter av teknisk karaktär sker ofta genom nätverksskanningar, penetrationstester eller andra typer av tester. Nätverksskanningar och penetrationstester kräver stor försiktighet i miljöer med styrsystem eftersom sådana system kan vara känsliga för den nätverkstrafik som genereras av sådana aktiviteter. Skanningar och tester kan också göras mot testmiljöer när så är möjligt. Tekniska tester som sårbarhetskanning och penetrationstester kan visa på sårbarheter som tidigare har hanterats, men där den vidtagna åtgärden inte längre är effektiv eller tillräcklig. Vidare kan sårbarhetsanalyser visa på eventuella felkonfigurationer.

Omvärldsbevakning i form av prenumerationer på information om sårbarheter från tillverkare av utrustning och programvara eller tjänsteleverantörer fyller en viktig funktion för identifiering av sårbarheter. Viktigt är att omvärldsbevakningen utgår ifrån de nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten, men även omfattar de stödsystem som kan påverka säkerheten för den samhällsviktiga tjänsten. Arbetet med omvärldsbevakningen bör ske systematiskt och samverkan med andra verksamheter som också arbetar med omvärldsbevakning, exempelvis IT-organisationen, kan vara effektivt.

En medvetenhet om vilka sårbarheter en organisation har, oavsett om de är tekniska eller organisatoriska, är en av förutsättningarna för att utföra riskbedömningar och riskanalyser. Identifiering och dokumentation av sårbarheter bör därför vara en integrerad del av informationssäkerhetsarbetet.

Förslag på aktiviteter

- Genomför:
  - nätverksskanningar där så är möjligt
  - penetrationstester där så är möjligt
  - och/eller andra typer av tekniska analyser för kartläggning av sårbarheter
- Etablera processer för:
  - systematisk sårbarhetsanalys av de tillgångar som kartlagts enligt 4 §
  - att systematiskt identifiera produkter och programvaror som används
  - omvärldsbevakning i form av prenumerationer på sårbarhetsinformation
  - samverkan med andra verksamheter som utför omvärldsbevakning
- Identifiera:
  - personberoenden i kritiska roller
  - brister i dokumentation för viktiga rutiner
  - om funktioner som kan påverka säkerheten i dricksvattenproduktionen bör separeras

3.3 Riskanalysmetoder

6 § Leverantören ska ha minst en beslutad riskanalysmetod som är tillämpbar på tillgångar, förbindelser, underleverantörer och organisatoriska enheter som förtecknats enligt 4 §. Riskanalysmetoden ska vara utformad på ett sådant sätt att den med samma ingångsvärden, kompetens hos medverkande och avgränsning genererar konsekventa och sinsemellan jämförbara resultat.

Som en central del av det systematiska informationssäkerhetsarbetet ska en beslutad metod för riskanalys användas. Metoden kan ha sin utgångspunkt i etablerad standard, t.ex. ISO 31000 eller ISO 27005. Delar av MSB:s metodstöd och handböcker i ämnet kan också ge ett bra stöd. En beslutad riskanalysmetod medger ett systematiskt informationssäkerhetsarbete och om samma metod används återkommande blir resultaten jämförbara över tid. I början av ett riskanalysarbete kan i vissa fall mer eller mindre grova uppskattningar behövas och det är naturligt att vald metod förfinas eller förbättras för varje riskanalys som genomförs. Det är dock av vikt att metoden är utformad så att det inte är möjligt att godtyckligt nedvärdera risker för att undvika hantering.

Om olika riskanalysmetoder används kan resultatet av riskanalyserna variera och det blir svårare att arbeta systematiskt. Om metoden genererar olika typer av resultat eller beskriver resultaten med olika skalor, enheter etc. blir arbetet med, och framgång i hantering av risker, över tid svårt att mäta vilket ger sämre förutsättningar att bedriva arbetet systematiskt.

Föreskrifterna anger inte en metod eller standard utan lämnar öppet för leverantören att använda den riskanalysmetod som bäst passar dennes verksamhet. Leverantören behöver själv ha eller utveckla kompetens rörande de riskanalysmetoder som används samt säkerställa att inhyrd kompetens också använder en av verksamheten beslutad metod.

Förslag på aktiviteter
- Välj riskanalysmetod utifrån analysernas syfte, verksamhetens behov och förutsättningar, samt tillgänglig information
- Upprätta en dokumenterad process för hur riskanalyser ska genomföras
- Utbilda berörd personal i tillvägagångssätt och metod
- Etablera en process för att utvärdera och förbättra riskanalysmetoden

3.4 Riskanalyser

7 § Leverantören ska ha en plan för vid vilka tidpunkter och i vilka situationer leverantören ska genomföra riskanalyser.

NIS-lagen anger att riskanalys ska göras årligen. Utöver detta ska det finnas beslutade planer för vid vilka tidpunkter och i vilka situationer som riskanalyser ska genomföras. Föreskrifterna ställer också vissa krav på situationer då riskanalys ska ske.

Systematik i riskanalysarbetet innebär att det arbetet ska ske strukturerat och att riskanalyser ska genomföras vid bestämda situationer. Situationer som föranleder riskanalys kan vara olika beroende på leverantören och dess omständigheter. Det centrala är att leverantören avgör och beslutar om när riskanalyser ska genomföras, att detta dokumenteras samt att analyser faktiskt genomförs vid de tillfällen och de situationer som beslutats.

Återkommande riskanalyser kan utgå från tidigare utförda riskanalyser om avgränsningarna och omfattningen är desamma. På så vis kan en initial riskanalys ligga till grund för fortsatt riskanalysarbete vilket förenklar arbetet över tid. Med en tydligt definierad omfattning för riskanalysarbetet är det också möjligt att mäta förbättringar över tid.

Förslag på aktiviteter
- Etablera en process som säkerställer att riskanalys genomförs årligen
- Upprätta en plan för vid vilka andra tidpunkter och i vilka andra situationer riskanalys ska utföras
- Upprätta en process för att analysera och hantera risker som identifieras löpande
- Återkommande riskanalyser kan utgå från tidigare utförda riskanalyser

3.5 Planering av riskanalyser

8 § Leverantören ska, utöver den riskanalys som ska genomföras samt uppdateras årligen enligt 12 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, genomföra riskanalyser inför planerade förändringar i nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten, i samband med incidenter samt i övrigt när det är motiverat.

För att säkerställa kontinuiteten i dricksvattenförsörjningen ska riskanalyser genomföras innan förändringar införs i nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten.

Detta syftar till att minimera störningar och incidenter i samband med sådana förändringar.

När en händelse uppstått som orsakat någon form av incident för den samhällsviktiga tjänsten kan en riskanalys genomföras som en del av incidenthanteringen. En genomförd riskanalys i denna situation kan uppmärksamma behov av ytterligare åtgärder för att minska risken för att samma eller liknande händelser uppstår igen.

Förslag på aktiviteter

- Uppdatera processer för förändringshantering så att de innehåller krav på riskanalys
- Inför en CAB (Change Advisory Board) eller motsvarande för de nätverk och informationssystem som dricksvattenförsörjningen har beroenden till.
- Utbilda berörd personal
- Frågeställningar som kan ligga till grund för riskanalyser i samband med förändringar är:
    - alla brandväggsregler är dokumenterade och kopplade till en aktuell riskanalys
    - Hur omfattande är förändringen?
    - Har motsvarande förändringar orsakat störningar tidigare?
    - Vid vilken tid på dygnet ska förändring genomföras?
    - Finns det personal tillgänglig för att driva verksamheten manuellt i händelse av störning på grund av förändringen?
    - Vilka möjligheter finns att testa och kvalitetssäkra förändringen innan den införs i produktionsmiljö?
    - Vilka tester ska genomföras för att kontrollera att allt gått bra?
    - Finns det en plan för hur en förändring kan backas från produktion om större fel eller störningar upptäcks?

3.6 Omfattning av samtliga riskanalyser

9 § De riskanalyser som genomförs ska sammantaget omfatta åtminstone de tillgångar, förbindelser, underleverantörer och organisatoriska enheter som förtecknats enligt 4 §.
För varje enskild riskanalys ska det finnas en dokumenterad beskrivning av vilka tillgångar, förbindelser underleverantörer och organisatoriska enheter den omfattar.

Alla delar av de nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten omfattas av kravet på riskanalyser. Analyserna ska inte begränsas till endast nätverk och informationssystem som omedelbart förknippas med dricksvattenproduktionen. Kringliggande stödsystem och organisatoriska enheter som kan påverka säkerheten för dricksvattenproduktionen ska också omfattas av riskanalyserna, eftersom de används för tillhandahållandet av tjänsten. Omständigheter som ligger utanför verksamhetens omedelbara ansvarsområde och kontroll, exempelvis externa tjänster, ska inkluderas i analysen om de kan påverka säkerheten i de nätverk och informationssystem som används för den samhällsviktiga tjänsten.

En uppdelning till flera mindre riskanalyser kan vara fördelaktig om en riskanalys för helheten blir för omfattande, under förutsättning att alla relevanta nätverk och informationssystem omfattats när samtliga riskanalyser är genomförda. Om en uppdelning i flera riskanalyser sker, behöver resultaten av genomförda riskanalyser möjliggöra en övergripande prioritering av hantering av risker som identifierats.

Noggrann dokumentation av vad respektive riskanalys omfattar utgör en förutsättning dels för en systematisk uppföljning av säkerhetsarbetet, dels för den egna organisationens kontroll av vilka riskbedömningar som gjorts. Utan en sådan beskrivning är det lätt att riskanalysen blir för omfattande eller för avgränsad. Utan en noggrann dokumentation är det även svårt att avgöra om hela eller endast delar av relevanta tillgångar, förbindelser, underleverantörer och organisatoriska enheter har analyserats.

För en viss typ av utrustning där det finns många enheter av samma sort och med likartat användningsområde, exempelvis mobiltelefoner, jour-pc, undercentraler, nätverksutrustning och kommunikationslänkar kan en riskanalys per kategori och användningsområde vara tillräckligt. Likvärdiga system och förbindelser kan alltså analyseras i grupp så länge det säkerställs att samtliga tillgångar och förbindelser omfattas av riskanalysen.

<u>Förslag på aktiviteter</u>
- Dela upp riskanalysarbetet i mindre delar
- Dokumentera tydligt vad varje riskanalys omfattar
- Gruppera likvärdiga system och analysera dem tillsammans
- Identifiera och analysera risker förknippade med system och nätverk som ligger utanför leverantörens direkta kontroll separat
- Utbilda berörd personal

3.7 Grundläggande krav på riskanalysens omfattning

10 § En riskanalys ska omfatta följande delar:

1. identifiering av risker, dvs. av rimligen identifierbara omständigheter eller händelser med en potentiell negativ inverkan på säkerheten i de nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten (riskidentifiering),
2. kvalificerade bedömningar av tänkbara konsekvenser av att identifierade risker inträffar (konsekvensbedömning),
3. kvalificerade bedömningar av sannolikheten för att sådana omständigheter inträffar (sannolikhetsbedömning), samt
4. kvalificerade sammanvägda bedömningar av sannolikheten för att omständigheterna inträffar och de negativa konsekvenser detta kan medföra (riskutvärdering).

Rimligen identifierbara omständigheter

En förutsättning för att genomföra riskanalyser är att först identifiera samtliga rimligen identifierbara omständigheter som kan ha en negativ inverkan på de nätverk och informationssystem som används för leverans och distribution av dricksvatten.

Riskanalyserna enligt NIS-lagen ska inte sammanblandas med de risk- och sårbarhetsanalyser (RSA) som avses i lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. NIS-lagens definition av risk är bred och avser samtliga identifierbara händelser, inte enbart extraordinära händelser som avses i lagen (2006:544).

En uttömmande lista

Kravet på att identifiera samtliga rimligen identifierbara omständigheter är ett krav på att identifiera sådant som vid en objektiv bedömning baserat på den kompetens som krävs kan identifieras. Uttrycket är kopplat till definitionen av ”risk” i 2 § NIS-lagen. Att identifiera samtliga omständigheter innebär att skapa en uttömmande lista över omständigheter som kan ha en negativ inverkan på de nätverk och informationssystem som används för leverans och distribution av dricksvatten.

Även omständigheter utanför den egna verksamheten ska beaktas. Om störningar som uppstår i nätverk och informationssystem som ligger utanför leverantörens kontroll eller omedelbara ansvarsområde, men som kan ha en negativ inverkan på de nätverk och informationssystem som används för leverans och distribution av dricksvatten, måste risken förknippad med dessa störningar analyseras. Riskanalysen ska i sådana fall även omfatta de nätverk och informationssystem som leverantören själv inte har rådighet över eftersom risker förknippade med dessa kan ha en negativ inverkan på de nätverk och informationssystem som används för leverans och distribution av dricksvatten.

Kvalificerade bedömningar av konsekvenser och sannolikheter

En kvalificerad bedömning innebär att bedömningen ska vara genomförd baserad på relevant information och av personal med kompetens inom området. Det innebär även att de som medverkar ska ha nödvändig kompetens för att kunna använda den metod som valts.

Gällande konsekvenser så är det endast konsekvenser som är relevanta för leverantörens förmåga att leverera den samhällsviktiga tjänsten som behöver beaktas inom ramen för NIS-lagen.

Sammanvägda bedömningar (riskutvärdering)

Det är ofta den sammanvägda bedömningen som traditionellt kallas för en riskutvärdering, d.v.s. när sannolikhet och konsekvens vägs samman till en gemensam riskutvärdering. Processen för en sammanvägd riskutvärdering ingår normalt i den riskanalysmetod som beslutats enligt 6 §.

Förslag på aktiviteter

- Tillsätt en grupp med uppgiften att först identifiera samtliga rimligen identifierbara omständigheter eller händelser i nätverk och informationssystem
- Utforma krav på vilken kompetens och vilka roller som ska ingå vid olika riskanalyser beroende på avgränsning
- Utforma krav på hur riskanalysernas resultat ska dokumenteras
- Utse vilken roll som ska följa upp att riskanalyser genomförs
- Utbilda berörd personal

3.8 Ytterligare faktorer

11 § Vid genomförandet av riskanalyser ska leverantören beakta bland annat erfarenheter av inträffade incidenter, resultatet av aktuell omvärldsbevakning, sårbarheter som kartlagts enligt 5 §, sammankoppling med nätverk och informationssystem som används i annan verksamhet, och eventuellt behov av att uppdatera eller förstärka tidigare vidtagna säkerhetsåtgärder.

Erfarenheter från inträffade incidenter

Som ingångsvärde till riskanalysarbetet behöver tidigare inträffade incidenter som påverkade eller kunde ha påverkat tjänsten analyseras för att identifiera om behovet av säkerhetsåtgärder är förändrat med beaktande av det inträffade. Avsikten är att genom den analysen minska risken för att en liknande incident inträffar igen. Incidenter som används som underlag till riskanalyser behöver inte enbart vara sådana som påverkat den egna leveransen, med fördel kan även incidenter från andra organisationer eller organisatoriska enheter tas i beaktande för att dela lärdomar och erfarenheter. Det kan också vara värdefullt att beakta händelser som kunde ha utvecklats till en incident, men där så inte skedde.

Omvärldsbevakning

Omvärldsbevakning kan leda till att nya risker identifieras samt påverka bedömningen av risker, till exempel om sårbarheter för den programvara och utrustning som används i verksamheten identifieras. Leverantören behöver bedriva en aktiv omvärldsbevakning som syftar till att inhämta information som kan användas för att värdera och bedöma risker, exempelvis allmänna trender inom IT- och informationssäkerhetsområdet eller tekniska trender specifika för säkerhet avseende industriella styrsystem.

Vanligtvis fångas information om risker och sårbarheter upp genom aktivt uppsökande omvärldsbevakning, veckobrev eller blixtmeddelande från exempelvis CERT-SE. Med en etablerad process för omvärldsbevakning är det möjligt att använda omvärldsinformation i genomförandet av riskanalys för att identifiera behovet av åtgärder.

Tekniska och organisatoriska sårbarheter

Sårbarheter som identifierats enligt 5 §, oavsett om det är tekniska eller organisatoriska sårbarheter, påverkar risk och ska användas som ingångsvärden i genomförande av riskanalyser. Ny information kan också påverka bedömningen av effektiviteten i redan vidtagna åtgärder. Ett exempel är att en rutin behöver justeras eller att en säkerhetsåtgärd behöver förstärkas.

Sammankopplingar med andra nätverk och informationssystem

I 16 § anges att nätverk och informationssystem som används för leverans och distribution av dricksvatten ska separeras från nätverk och informationssystem som används för annan verksamhet. Sammankopplingar mellan nätverkssegment kan vara motiverat, men det kan också introducera nya risker eller påverka befintliga risker och behöver därför beaktas i en riskanalys. Vid en ökad grad av integration bör risker värderas högre och kan därmed kräva ytterligare säkerhetsåtgärder till exempel via förstärkt övervakning av trafik och säkerhetsloggar.

Ändringar i regler i en nätverkskomponent som styr tillåten kommunikation bör gå att spåra till en aktuell riskanalys och riskbedömning.

Tidigare införda åtgärder

Tidigare införda säkerhetsåtgärder kan vid ett senare tillfälle bedömas som otillräckliga. Befintliga säkerhetsåtgärders effektivitet måste därför bedömas kontinuerligt samt när riskanalyser genomförs. Det förekommer att åtgärder behöver förstärkas eller att åtgärden i sig har en sårbarhet som upptäckts vid exempelvis omvärldsbevakning eller sårbarhetsskanning.

Förslag på aktiviteter
- Etablera
  - en aktiv omvärldsbevakning
  - samverkan med andra liknande verksamheter för erfarenhetsutbyte
- Säkerställ att
  - alla brandväggsregler är dokumenterade och kopplade till en aktuell riskanalys
  - alla ändringar av brandväggsregler eller annan konfiguration av nätverk sker kontrollerat och föregås av riskanalys
  - alla sårbarheter som identifierats enligt 5 § har ingått i en riskanalys
  - erfarenhet och lärdomar från egna och andras incidenter ges utrymme i riskanalysarbetet
  - tidigare införda säkerhetsåtgärder följs upp regelbundet

3.9 Dokumentation av riskanalyser

12 § Resultatet av riskanalyser ska dokumenteras tillsammans med uppgifter om vilka som deltagit vid genomförandet av analyserna.

Dokumentation av riskanalyserna är en förutsättning för ett ändamålsenligt och systematiskt säkerhetsarbete, där arbetets effektivitet och verkan bör vara mätbar. Dokumentation av riskanalysen är också grundläggande för åtgärdsplanen. Dokumentation av deltagande vid genomförandet av riskanalysen kan vara väsentligt ur flera aspekter; om deltagarna byts ut så kan de tidigare deltagarna bli tillfrågade i efterhand, nya deltagare kan få lärdomar av dem som var med tidigare, och det blir transparent vilka som var ansvariga.

Förslag på aktiviteter
- Dokumentera och spara underlaget till alla riskanalyser
- Dokumentera och spara resultatet av alla riskanalyser
- Dokumentera och spara vilka som deltagit i arbetet med att genomföra riskanalyserna
- Säkerställ att dokumentation finns tillgänglig för uppföljning av informationssäkerhetsarbetet

3.10 Riskägare

13 § För varje identifierad risk ska det finnas en beslutad och dokumenterad riskägare som har befogenhet att fatta beslut om riskhanteringsåtgärder.

Riskägare som har befogenhet fatta beslut

När riskanalys är genomförd ska leverantören besluta om en ägare för respektive identifierad risk. Riskägare har ansvar för att deras risker hanteras, samt för valet av åtgärder för hantering av enskilda risker. Riskägarskap ska tilldelas aktivt till relevant personal, dvs. det ska inte per automatik vara en del i en viss rolls ansvar att agera riskägare.

Riskägaren får heller inte enbart bli en ansvarstagare som saknar nödvändigt inflytande. Riskägaren behöver inte vara den som utför åtgärder för att hantera risken, men ska vara den som kan besluta om åtgärd och ambitionsnivå, prioritering, resurser, beställningar m.m. Att utse en riskägare som inte har möjlighet, eller det mandat som krävs, för att fatta beslut kring åtgärder gör säkerhetsarbetet ineffektivt.

Vidare kan en åtgärd vara att acceptera risken under förutsättning att riskägaren förstår vad det innebär. Den som fattar beslut relaterat till en risk måste förstå konsekvensen av risken, inklusive risker kopplade till beroenden till extern infrastruktur eller underleverantörer. Om riskägaren inte direkt kan påverka risknivån i extern infrastruktur eller hos en underleverantör kan kompenserande eller alternativa åtgärder vara nödvändiga.

Ägarskap för risk respektive åtgärd kan ligga i olika delar av en organisation. Som exempel är det tveksamt om en utpekad riskägare, som via ägardirektiv tvingas använda en specifik infrastrukturlösning, är den faktiska riskägaren. För betydande risker som kräver långtgående åtgärder kan det vara nödvändigt att eskalera riskägarskapet i organisationen. I detta exempel kan den faktiska riskägaren vara utfärdaren av ägardirektivet.

Förslag på aktiviteter
- Identifiera en riskägare till varje risk
- Säkerställ att riskägare har mandat att fatta beslut så att riskägaren inte enbart är ansvarstagare
- Säkerställ att riskägare förstår konsekvensen av att avstå från att införa åtgärder
- Besluta vem inom den egna organisationen som följer upp åtaganden
- Utveckla en process för att följa upp och bedöma risker hos underleverantörer löpande
- Utbilda relevant personal

4. Åtgärdsplan

14 § Leverantören ska upprätta och dokumentera en åtgärdsplan som baseras på resultatet av genomförda riskanalyser.

Åtgärdsplanen ska innehålla uppgift om följande:
- vilka risker som respektive säkerhetsåtgärd syftar till att hantera och en redogörelse för det sätt på vilket risker hanteras genom valda åtgärder,
- redan vidtagna säkerhetsåtgärder och hanterade risker,
- planerad sluttid för införande eller genomförande av respektive säkerhetsåtgärd,
- vem inom den egna organisationen som ansvarar för genomförande av respektive säkerhetsåtgärd, och
- i vilken utsträckning underleverantörer anlitats för genomförandet av säkerhetsåtgärder.

4.1 Upprätta åtgärdsplan

Åtgärdsplanen ska vara relaterad till riskanalyser som gjorts och kan bestå av flera dokument, men det måste gå att få en överblick över åtgärder som genomförts och arbetet som återstår.

Leverantören bör besluta om gränsvärden för när en risk kräver en åtgärd. För att möjliggöra prioritering mellan risker, samt för att göra en tidplan för införande av åtgärd, bör organisationen även fastställa riktlinjer för prioritet baserat på sammanvägd riskbedömning. Gränsvärden och riktlinjer kan på så sätt relateras till den sammanvägda riskutvärderingen som framkommit i riskanalysen, dvs. riskens allvarlighetsgrad ska styra om och när en åtgärd är nödvändig att införa. På så sätt kan leverantören säkerställa att resurser konsekvent och systematiskt läggs på att hantera risker som är relevanta.

Risker som respektive åtgärd avser hantera

En åtgärd kan av naturliga skäl hantera fler risker och en risk kan hanteras av flera olika åtgärder. Av detta skäl ska en vald åtgärd kunna kopplas till den risk som åtgärden avser hantera. Vidare ska det av åtgärdsplanen framgå hur leverantören anser att valda åtgärder hanterar risken på det sätt som avsetts.

Redan införda åtgärder

Det finns många situationer där en redan införd säkerhetsåtgärd helt eller delvis hanterar nya identifierade risker. Att dokumentera redan införda åtgärder och koppla dessa till nya identifierade risker kan påvisa framsteg i informationssäkerhetsarbetet.

En annan aspekt att ta hänsyn till vid dokumentation av sedan tidigare införda åtgärder är att många åtgärder redan är införda sedan länge. Dokumentationen kan visa vilken risk som eventuellt kvarstår för redan införda åtgärder eller om en sådan åtgärd kan behöva förstärkas. Dokumentationen är också ett verktyg för leverantören att uppmärksamma varför vissa åtgärder vidtagits. På så vis kan åtgärder motiveras så de inte avskaffas med följden att risker

återuppstår. Det kan också uppstå tillfällen när en tidigare vidtagen åtgärd blir inaktuell efter att en annan mer effektiv åtgärd införts, vilket då kan framgå av åtgärdsplanen.

Planerad sluttid för införande

För att åtgärdsplanen ska ha en reell effekt måste säkerhetsåtgärderna som tas upp i den införas. En vanligt förekommande situation gällande åtgärder är att om ingen tidsplan anges så tenderar de att inte införas. En tidplan knuten till åtgärdsplanen möjliggör för leverantören att följa upp sitt eget införande och säkerställa slutförande av uppgiften.

Peka ut ansvar för genomförande

Åtgärdsplanen ska ange vem som ansvarar för införandet eller genomförandet av åtgärden. Åtgärder tenderar att utebli om ansvar för införande av åtgärd är otydligt, liksom om ingen uppföljning på införandet utförs. Särskilt angeläget blir uppföljning och ansvar om åtgärden ska utföras av en annan organisation än den egna verksamheten. Notera att ansvar för införande av en åtgärd inte är samma roll som riskägare som fattat beslut om vilken åtgärd det är som ska införas.

Underleverantörers åtaganden

Leverantören har ansvar för regelefterlevnad och behöver därför ställa krav på säkerhet i såväl egna nätverk och informationssystem som de som tillhör en underleverantör. Därmed bör åtgärder som eventuellt införs av eller hos en underleverantör också inkluderas i åtgärdsplanen och följas upp av leverantören.

Förslag på aktiviteter

- Besluta om krav på om och när en risk ska hanteras, med utgångspunkt i den sammanvägda riskutvärderingen
- Upprätta en åtgärdsplan
- Identifiera vilka risker som respektive åtgärd avser hantera och hur
- Dokumentera redan införda åtgärder och hanterade risker
- Besluta alltid planerad sluttid för genomförande
- Besluta vem inom den egna organisationen som ansvarar för genomförandet av respektive åtgärd
- Dokumentera underleverantörers åtaganden för genomförande av åtgärder
- Besluta vem inom den egna organisationen som följer upp underleverantörers åtaganden

5. Obligatoriska säkerhetsåtgärder

15 § I 16–18 §§ uppställs krav på grundläggande säkerhetsåtgärder som leverantören måste vidta för att hantera risker i de nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten. Dessa säkerhetsåtgärder ska vidtas oavsett vilka ytterligare åtgärder som bedöms lämpliga utifrån leverantörens riskanalys.

Leverantörer ska vidta säkerhetsåtgärderna i 16-18 §§, oavsett vilka säkerhetsåtgärder som i övrigt bedöms som lämpliga baserat på genomförda riskanalyser. Syftet med de obligatoriska säkerhetsåtgärderna är att garantera en allmän lägsta säkerhetsnivå.

5.1 Logisk eller fysisk separation

16 § Leverantören ska se till att nätverks- och informationssystem som används för tillhandahållande av den samhällsviktiga tjänsten är logiskt eller fysiskt separerade från nätverk och informationssystem som används för tillhandahållandet av andra tjänster.
Separation enligt första stycket krävs inte i förhållande till nätverk och informationssystem som används för tillhandahållandet av andra tjänster nära förknippade med den samhällsviktiga tjänsten, förutsatt att säkerheten i anslutna nätverk och informationssystem motsvarar den i de nätverk och informationssystem som används för tillhandahållande av den samhällsviktiga tjänsten.

Behovet av segmentering

Med separation av nätverk menas att de nätverk och de komponenter som styr produktion och distribution av dricksvatten samt liknande verksamhet, t.ex. styr- och kontrollsystem för avloppsverksamhet, ska vara åtskilda från system och nätverk som används för övrig verksamhet. Med övrig verksamhet menas till exempel kontorsnätverk, annan kommunal verksamhet, skola eller IT-system som inte rör styr- och kontrollsystemen. De verksamheter som är snarlika dricksvattenproduktionen, till exempel avloppshantering, använder ofta samma system och nätverk och hanteras av samma personal. System som används för syften som är relaterade till dricksvattenproduktion kan därför finnas i samma segment, så länge de håller samma säkerhetsnivå. Syftet med segmentering är att minska styrsystemens exponering för risker.

En högre grad av integration mellan olika verksamheters nätverk och system medför att styrsystemen kan exponeras för risker de inte är designade för att hantera. Störningar (t.ex. IT-haverier, strömavbrott eller angrepp) i leverantörens IT-infrastruktur riskerar att påverka även styrsystemens funktion om miljön är integrerad.

Hur separation av system ska uppnås

Nätverkssegmentering och begränsning av nätverkstrafik mellan olika nätverkssegment kan realiseras på olika sätt. Att bygga ett helt separat fysiskt nätverk, med egen nätverksutrustning

och kablage, skapar en mycket bra separation, ger god säkerhet och kontroll men kan vara kostnadsdrivande. Ett alternativ kan vara att bygga logisk trafikreglering i form av virtuella lokala nätverk (VLAN) vilket idag kan åstadkommas med standardfunktionalitet i brandväggar och nätverksutrustning. Separation av nätverk skulle t.ex. kunna innebära en avancerad säkerhetsarkitektur för zon-indelning i ett delat nätverk. Ur ett rent säkerhetsperspektiv är fysisk separation oftast att föredra framför logisk separation och traditionellt sett har industriella kontrollsystem ofta varit fysiskt isolerade. Föreskriften anger inte hur separation ska uppnås, valet av metod för separation bör vara baserat på organisationens egen riskanalys och behov.

Vid nätverksdesign och val av teknik ska hänsyn tas till befintliga och framtida integrationer så att kommunikation mellan olika segment kan ske på ett säkert sätt.

Behov av särskild försiktighet vid logisk separation

Separation som är helt baserad på exempelvis VLAN eller teknik för virtuell routing (VRF) kan resultera i lösningar med ökad komplexitet. Avancerad säkerhetsarkitektur för logisk zon-indelning ställer höga krav på kunskap som på sikt kan vara dyr och svårtillgänglig. Ökad komplexitet leder också till ett behov av en mer omfattande riskanalys.

Integrationer och kommunikation mellan nätverkssegment.

I vissa fall, exempelvis för fjärråtkomst, 4G-kommunikation med yttre anläggningar eller export av data, kan det krävas någon form av integration eller kommunikation med andra nätverk och informationssystem. Sådan kommunikation bör regleras med en logisk eller fysisk skyddskomponent som till exempel brandvägg, datadiod, dmz, proxy eller motsvarande.

Stödsystem (AD, virtualisering, SAN, backup)

En relativt vanlig anledning till att öppna för datakommunikation mellan system som används för produktion och distribution av dricksvatten och andra IT-system är behovet av att nyttja gemensamma IT-resurser och stödsystem, till exempel virtualiseringslösningar eller behörighetskontrollsystem. Det finns dock ofta goda skäl för att undvika att använda gemensamma stödsystem till flera olika zoner parallellt, då det kan introducera brister i zonuppdelningen och aktivt motverka nätverksseparation som säkerhetskoncept.

En separation av stödsystem kan innebära att funktioner som behörighetskontrollsystem, backup och lagringslösningar behöver dupliceras till respektive nätverkszon. Lösningarna i sig kan vara byggda på en identisk teknisk plattform och förvaltas av gemensam personal, så länge IT-systemen i sig är separata och inte integreras. Målet är att säkerställa att ett intrång, eller IT-haveri, i gemensam IT-infrastruktur inte får en spridningseffekt i nätverk och informationssystem som används för tillhandahållande av den samhällsviktiga tjänsten. Här är det även viktigt att beakta de arbetsstationer som används av IT-personal för att administrera IT-system, så inte ett intrång i en IT-arbetsstation möjliggör intrång i andra IT-miljöer.

Andra anslutningsvägar

Det är lätt att av misstag introducera brister i segmenteringen. Till exempel kan ett 4G-modem som en underleverantör av någon utrustning installerar för fjärråtkomst under garantitiden eller en felaktig tillfällig internetkoppling utgöra sådana brister.

Industriella informations- och styrsystem har höga krav på tillförlitlighet och tillgänglighet. Det finns ofta supportkontrakt och garantiåtagande för både utrustning och mjukvara från leverantören vilket ibland kan leda till att det finns en förväntan från leverantörer, integratörer och supportorganisationer att de på distans ska ha möjlighet övervaka och diagnostisera och även i viss mån konfigurera och utföra underhåll på mjukvara och komponenter. Denna typ av anslutning kan innebära en brist i segmenteringen.

Särskilda överväganden avseende mobilkommunikation (3G/4G/5G) till ytterstationer (och motsvarande)

När mobilnätet används för att kommunicera med ytterstationer behövs åtgärder för att säkerställa att endast betrodda enheter får kommunicera med ytterstationen, mellan ytterstationer och med centralsystem. I praktiken kan detta vara svårt att åstadkomma utan aktiv utrustning med stöd för VPN och brandväggsregler.

Vid kommunikation med ytterstationer via 3G/4G/5G (eller motsvarande teknik) behövs åtgärder för att säkerställa att kommunikationen regleras så att endast trafikflöden nödvändiga för verksamheten accepteras. Normalt regleras detta i en brandvägg så att ytterstationer endast kan kommunicera på de portar, med de protokoll och i de riktningar som är avsett.

Förslag på aktiviteter

- Separera alla system som används för leverans och distribution av dricksvatten och näraliggande tjänster (styrsystem för avlopp)
- Säkerställ att all kommunikation med andra nätverk och informationssystem regleras via en brandvägg, datadiod, proxy eller motsvarande nätverkskomponent
- Kontrollera att alla delar av den separerade infrastrukturen uppfyller minst de IT- och informationssäkerhetskrav som gäller för leverans och distribution av dricksvatten
- Gör en dokumenterad riskanalys för varje brandväggsöppning och sammankoppling med andra system
- Inventera och övervaka användning av kommunikationsutrustning som används för fjärruppkoppling
- Begränsa uppkopplingstid för fjärruppkopplade sessioner
- Avinstallera mjukvarulösningar för fjärrinloggning om möjligt
- Testa regelbundet att separation från internet finns för in- och utgående trafik.

5.2 Behörighetskontroll

17 § Åtkomst till nätverks- och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten ska endast medges till den person eller det system som behöver sådan åtkomst för att kunna utföra sina arbetsuppgifter respektive fylla sin funktion. Tilldelad behörighet ska begränsas till vad som är nödvändigt.
Leverantören ska upprätta och tillämpa regler för tilldelning, ändring och uppföljning av åtkomst och behörighet enligt första stycket.

Åtkomst ska medges endast för att tillåta utförande av arbetsuppgifter

Kraven om tilldelning av åtkomst omfattar utöver vanliga användare, som ofta tolkas som individer, även åtkomst som tilldelas utrustning, applikationer, kommunikationslänkar etc. Det finns till exempel ofta servicekonton som används när applikationer loggar in i en databas eller om utrustning, till exempel ytterstationer som ansluter via VPN, som har någon form av behörighet tilldelad i form av ett certifikat med krypteringsnyckel eller genom att utrustningen tilldelats ett SIM-kort med åtkomst till ett speciellt APN. Tilldelning av SIM-kort, certifikat eller motsvarande till utrustning är också en form av behörighet som endast ska medges när det är nödvändigt.

Åtkomst till fysisk utrustning

Styrning och begränsning av fysisk åtkomst till utrustning kan ske med till exempel elektronisk passagekontroll eller att nycklar till anläggningar som innehåller utrustning ges till personer som behöver det för sitt arbete. För utrustning som är placerad i allmänna utrymmen, utomhus eller på annan plats där obehöriga regelbundet vistas innebär det att utrustningen i sig kan behöva ett förstärkt fysiskt skydd.

Tilldelad behörighet ska begränsas till det som är nödvändigt.

Den behörighet som tilldelas ska vara begränsad till det som är nödvändigt för användarens möjlighet att utföra sin arbetsuppgift. Generellt finns en tendens att konton ges högre behörighet än nödvändigt. Begränsningen av behörigheter avser såväl fysisk som logisk åtkomst till nätverk och informationssystem som har betydelse för leverans och distribution av dricksvatten.

I möjligaste mån ska tidsbegränsade konton och behörigheter användas. En användare som har ett tidsbegränsat uppdrag bör också ha ett tidsbegränsat konto som automatiskt stängs när tiden för uppdraget löpt ut.

Uppföljning av åtkomst

För att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring i de digitala system som används för leverans och distribution av dricksvatten bör regelbunden kontroll/revision av åtkomst och behörigheter göras. Det är särskilt angeläget med regelbunden kontroll/revision för system som är åtkomliga via fjärråtkomst eller motsvarande.

Leverantören bör besluta om en rutin och periodicitet för genomgång och uppföljning av användares behörigheter, där behörigheter kontrolleras mot personers och systems aktuella arbetsuppgifter och funktion. Protokoll från genomförd uppföljning behöver upprättas och bevaras för att kunna visa en spårbarhet i att kontrollen är genomförd.

Fastställda regler

Det är upp till varje leverantör att själv avgöra vilka åtgärder som behövs för att följa föreskrifterna. I de flesta fall innebär det att det finns behov av att använda ett identitets- eller åtkomstsystem. I andra fall kan det räcka med att dokumentera tilldelade behörigheter i en förteckning. För hantering och utdelning av nycklar kan det till exempel vara vanligt med en skriftlig förteckning.

En strukturerad process för tilldelning, ändring och uppföljning av tilldelade behörigheter och nycklar utgör ett stöd för att leverantören ska ha kontroll av åtkomst till de komponenter som används för den samhällsviktiga tjänsten samt lägger grunden för verksamhetens egen uppföljning och kontroll av vilka behörigheter som tilldelats.

Förslag på aktiviteter

- Kartlägg vilka identitets- och åtkomstsystem som används
- Utforma regler för tilldelning, ändring och uppföljning av åtkomst och behörighet
- Etablera en process för att skyndsamt ta bort åtkomst som inte behövs
- Inför en process för regelbunden kontroll och revision av åtkomst och behörigheter.
- Kontrollera särskilt vilka användare som har
  - Möjlighet till fjärråtkomst
  - Högre behörigheter (exempel ”domän admin” behörighet i AD)
  - Åtkomst till brandväggar
- Utbilda berörd personal

5.3 Flerfaktorsautentisering

18 § Leverantören ska se till att autentisering vid fjärråtkomst till informationssystem som har betydelse för den samhällsviktiga tjänsten baseras på flera faktorer (flerfaktorautentisering).

Behovet av stark åtkomstkontroll för fjärråtkomst

Flerfaktorsautentisering vid fjärråtkomst är en grundläggande säkerhetshöjande åtgärd för industriella kontrollsystem. Det finns en betydande risk för allvarliga störningar om obehöriga får fjärråtkomst till nätverks- och informationssystem som används för leverans och distribution av dricksvatten. Vid fjärråtkomst till viktiga system, primärt via Internet, är användarens identitet central.

Traditionell åtkomstkontroll baserad på enbart användarnamn och lösenord för autentisering har ett flertal olika brister, exempelvis att användare kan dela lösenord med andra användare eller att användarna väljer enkla lösenord eller samma lösenord på flera ställen.

Tekniska lösningar för fjärråtkomst begränsar möjlighet att kontrollera att den som loggar in faktiskt är den person den utger sig för att vara. Skalskydd och kollegor som delvis fungerar som en kontrollmekanism saknas helt vid fält- eller distansarbete.

Det förekommer att underleverantörer med fjärråtkomst inte alltid har användarunika konton för sina användare utan delar ett gemensamt leverantörskonto med ett gemensamt lösenord som delas av flera personer. Det innebär att lösenord och användarnamn för fjärråtkomst med tiden kan spridas i vida kretsar och att de inte byts när underleverantörens anställda byter jobb eller befattning.

Flerfaktorsautentisering

Flerfaktorsautentisering ska användas vid fjärråtkomst till nätverk och informationssystem som används för produktion och distribution av dricksvatten. Syftet är att säkerställa stark identitetskontroll för de användare som tilldelas behörighet till fjärråtkomst till nätverk och informationssystem.

Flerfaktorsautentisering innebär extra krav på användaren att presentera ytterligare bevis på sin identitet (två eller flera) utöver lösenord för att kunna logga in. Autentiseringen kan bestå av en kombination av olika faktorer inom ”något som man vet”, exempelvis lösenord och ”något som man har”, exempelvis ett smart kort.

Flerfaktorsautentisering minskar risken för att lösenord som stjäls kan användas för obehörig fjärråtkomst vid ett senare tillfälle.

Vidare bör kraven på flerfaktorsautentisering vara implementerade så att de följer hela livscykeln för ett konto. Det vill säga att kravet för flerfaktorsautentisering kvarstår vid inaktivering/aktivering av ett konto.

Utvärdera beroenden och risker vid val av lösning

Det finns fördelar ur säkerhetssynpunkt om flerfaktorsautentisering för fjärråtkomst till nätverk och informationssystem inte är beroende av externa tredjepartstjänster, exempelvis SMS. Anledningen är att verifieringen av användarens identitet sker utanför verksamhetsutövarens kontroll, vilket kan introducera sårbarheter i åtkomstkontrollen. Beroende till en tredjepartstjänst kan även försvåra eller omöjliggöra inloggning i krissituationer då det kräver flera tjänster som samtidigt ska fungera.

Vilka system som berörs

Kravet på flerfaktorsautentisering vid fjärråtkomst omfattar alla informationssystem som är av betydelse för leverans och distribution av dricksvatten, inte enbart de informationssystem nätverk och informationssystem som används för dricksvattenproduktionen. Exempel på informationssystem som kan omfattas är skyddsmekanismer som brandväggar, nätverksinfrastruktur, virtualiseringsinfrastruktur och behörighetskontrollsystem.

Förslag på aktiviteter
- Kartlägg vilka system som kan påverka leverans och distribution av dricksvatten
- Välj en robust autentiseringslösning som fungerar även i kris och störda förhållanden
- Inför flerfaktorsautentisering vid fjärruppkoppling för distans och fältarbete
- Utbilda berörd personal

Sammanfattningen ska ge läsaren en snabb uppfattning om de huvudsakliga slutsatserna i ett PM och i förekommande fall de åtgärder som föreslås. Målet är att alla ska förstå din sammanfattning – skriv enkelt och begripligt så att så många som möjligt förstår.

Du kan radera den här sidan om det inte finns någon sammanfattning.


Livsmedelsverket