Område Strategisk utveckling och stöd
NIS-tillsyn

Tillsyn

Livsmedelsverket kommer att genomföra tillsyn på säkerheten i nätverk och informationssystem som används för leverans och distribution av dricksvatten enligt Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen).

Mottagare	
Förmöte (distans)	
Tillsynsbesök	

Svar önskas
Senast 2020–xx–xx behöver vi uppgifter om:

- Namn, e-post och telefonnummer för er kontaktperson för tillsynen.
- Adress till och praktisk information om möteslokal
- Eventuella synpunkter på datum och tider

Svar samt eventuella frågor skickas till nistillsyn@slv.se

Särskilda förutsättningar med anledning av Corona/Covid19
Livsmedelsverket följer Folkhälsomyndighetens rekommendationer avseende bland annat lämpligheten i resor och fysiska möten. Detta möte kommer därför vara ett distansmöte, primärt via Skype. Om rekommendationerna avseende lämpligheten i resor ändras kan tillsynen istället ske som ett möte på plats hos er.

Tillsynen kan komma att ställas in om endera part har svårighet att bemanna mötet pga sjukdom. Detta kan från båda parterna ske med kort varsel.

Under punkten förberedelser (se nedan) beskrivs olika områden som ska presenteras för Livsmedelsverket under tillsynen. Den dokumentation som används vid presentationerna ska vara sådan att ni bedömer att den kan visas under ett eventuellt distansmöte, exempelvis så kan dokumentation av nätverksarkitektur vara i form av konceptuell nätverksritning. Det material ni visar kommer att vara underlag för fördjupade diskussioner och frågor.

Syfte och metod
Livsmedelsverket är enligt NIS-lagen tillsynsmyndighet för leverantörer inom sektorn leverans och distribution av dricksvatten. Syftet med NIS-lagen är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster.

Livsmedelsverket kommer att genomföra tillsyn hos er och de huvudsakliga ämnesområdena är:

- VA-huvudmannaskap, organisation, anläggningar
- Nätverksarkitektur, segmentering och fjärråtkomst
- Leverantörer
- Förutsättningar för införande av ett systematiskt informationssäkerhetsarbete
- Riskanalys och åtgärdsplan
- Andra frågeställningar baserade på era svar på självskattningsenkät, bl.a. er kapacitet och förberedelse för eventuell ö-drift

Tillsynen sker i huvudsak genom presentationer, intervjuer och fördefinierade frågor samt genomgång av dokumentation. Även tillsyn av utvalda lokaler, systemkomponenter och systeminställningar kan förekomma.

Agenda och förberedelser förmöte
Före tillsynsbesöket genomförs ett förmöte där tillsynsbesöket samt vilka roller/funktioner som bör medverka beskrivs närmare och ni har möjlighet att ställa frågor. Vi verifierar även er anmälan som leverantör enligt MSB:s föreskrifter (MSBFS 2018:7) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster under förmötet och vill att ni förbereder er med grunderna till ert beslut. Förmötet sker via Skype eller telefon.

Preliminär agenda för tillsynsbesök
Tillsynen sker under en heldag, agenda enligt nedan. Agendan kommer att anpassas efter förutsättningarna på plats, bland annat kan ämnesområden flyttas beroende på tidsåtgång och omfattningen av diskussionen samt bemanningsmöjligheter från er sida. Avslut sker senast klockan 16.

Förmiddag

- Introduktion
- Presentation av uppdrag, organisation, anläggningar, avtal
- Presentation av nätverksarkitektur
- Diskussion omfattning och avgränsning NIS-lagen

Eftermiddag

- Förutsättningar för införande av ett systematiskt informationssäkerhetsarbete
- Riskanalys och åtgärdsplan
- Frågeställningar baserade på självskattning
- Uppföljning och avslut

Postadress Box 622 751 26 Uppsala
Besöksadress Hamnesplanaden 5
Telefon 018-17 55 00
E-post livsmedelsverket@slv.se
Organisationsnummer 202100-1850
Internet www.livsmedelsverket.se

Förberedelser inför tillsynsbesök
En lämplig lokal för ändamålet är t. ex. ett konferensrum för ca 8 personer eller fler.

Följande ska presenteras muntligen. Om så önskas kan den muntliga presentationen stödjas av till exempel power point eller dylikt:

- VA-huvudmannaskap, uppdrag och övergripande om organisationen
- Översiktlig beskrivning av de fysiska anläggningar som används, ex vattenproduktion, reservoarer, datorhallar och övervakningscentraler.
- De avtalsparter som är nödvändiga för dricksvattenproduktion- och distribution. Detta kan exempelvis vara konsulter som arbetar i system, leverantörer av tjänster och kommunikationslösningar, samt leverantörer av hård- eller mjukvara. Beskriv hur leverantörens informationssäkerhetsarbete regleras i dessa avtal. Avtalen behöver finnas tillgängliga under tillsynstillfället.
- En utförlig beskrivning av den *nuvarande* nätverksarkitekturen som används för att realisera uppdraget. Presentationen avseende nätverksarkitektur ska beskriva principer, kritiska komponenter och väsentliga applikationer såsom industriella informations- och styrsystem (SCADA) samt deras beroenden till och uppbyggnaden av delad infrastruktur, nätverk- och kommunikations-infrastruktur, internet och externa tjänster. Beskriv om verksamhetens industriella styrsystem är segmenterade från andra IT-system. Beskriv även hur distansarbete i IT-miljön för styrsystemen sker och regleras, inkluderande hur autentisering och behörighetskontroll går till.
- En beskrivning av förutsättningarna för, samt hur ni avser arbeta med kraven i MSBFS 2018:8 för att etablera eller anpassa ett ledningssystemet som är tillämpbart på drickvattenproduktion- och distribution. Beskriv vilka standarder ni eventuellt använder.
- En beskrivning av hur arbete med riskanalys sker, i vilken omfattning och frekvens, vilka som deltar samt vilka riskområden som beaktas. Presentera även den resulterande åtgärdsplanen.
- Arbete med, förberedelser inför och konsekvenser vid en eventuell ö-drift.

Bemanning vid tillsynsbesök
Vår erfarenhet är att vid diskussionerna om omfattning och avgränsning för NIS-lagen är det önskvärt att minst följande funktioner/roller/kompetenser eller motsvarande närvarar:

- Beslutande funktion för informationssäkerhet / informationssäkerhetsansvarig / CISO
- Drift och förvaltare av IT-infrastruktur samt nätverk- och kommunikationsinfrastruktur
- Drift och förvaltare av relevanta applikationer inklusive industriella informations- och styrsystem (SCADA).

Utöver dessa behöver specialister kunna beskriva olika ämnesområden, exempelvis styrsystem, fjärråtkomst, segmentering, genomförande av riskanalyser mm. Det är inte för Livsmedelsverket nödvändigt att dessa specialister är närvarande vid hela tillsynstillfället.

Postadress
Box 622
751 26 Uppsala

Besöksadress
Hamnesplanaden 5

Telefon
018-17 55 00

E-post
livsmedelsverket@slv.se

Organisationsnummer
202100-1850

Internet
www.livsmedelsverket.se

Tillämplig lagstiftning:
Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:7) om identifiering av leverantörer av samhällsviktiga tjänster
Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster
Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:9) om rapportering av incidenter för leverantörer av samhällsviktiga tjänster

Stödjande dokument:
- ISO/IEC 27001
- ISO/IEC 27002
- IEC 62443-2-1
- MSB Vägledning till ökad säkerhet i industriella informations- och styrsystem
- Svenskt Vattens checklista för ökad SCADA-säkerhet

Bilaga - Om sekretess

Ändamål och laglig grund för insamling

Livsmedelsverket utför tillsyn enligt lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Livsmedelsverkets undersökningsbefogenheter regleras i 24 – 27 §§ och förbinder den som står under tillsyn bland annat att på begäran tillhandahålla Livsmedelsverket den information som behövs för tillsynen. Livsmedelsverket får, vid behov, förelägga den som står under tillsyn att tillhandahålla information och ett sådant föreläggande får förenas med vite.

Sekretessavtal, sekretessförbindelse, non-disclosure agreements eller motsvarande

Livsmedelsverket och Livsmedelsverkets personal tecknar inga enskilda sekretessförbindelser eller motsvarande avtal med tillsynsobjekt. Sekretessen hos Livsmedelsverket och myndighetens personal, liksom verkets relation till tillsynsobjekt regleras i lag.

IT-säkerhet

Livsmedelsverket har vidtagit en rad organisatoriska, fysiska och tekniska åtgärder för att skydda den information som samlas in från tillsynsobjekt. Det är bara den personal som arbetar med Livsmedelsverkets NIS-tillsyn som kan ta del av den information som ni lämnar till Livsmedelsverket. För arbete med digital information som inkommer under tillsyn som innehåller uppgifter där någon sekretessregel från kapitel 18 i offentlighets- och sekretesslagen (OSL) kan vara tillämplig används särskilda datorer som inte är nätverksanslutna mot vare sig internet eller resten av Livsmedelsverkets nätverk; datorerna är tydligt märkta, krypterade, behörighetskontrollerade och skyddas med så kallat air gap.

Markering av känsliga handlingar vid tillsyn

Vid överlämnandet av uppgifter till Livsmedelsverket i samband med tillsyn är det bra om den som lämnar handlingar själv märker uppgifter som de bedömer som sekretessbelagd för att uppmärksamma detta. När allmänna handlingar begärs utlämnade från Livsmedelsverket föregås utlämningsärendet av en sekretessprövning av dokumentets innehåll.

Hantering av utlämningsärenden av allmän handling

Det flesta handlingar i ett tillsynsärende är antingen arbetshandlingar eller offentliga allmänna handlingar såvida inte någon sekretessregel är tillämplig. Det är Livsmedelsverket som prövar frågor om utlämning av allmänna handlingar som förvaras vid myndigheten; en sekretessmarkering från tillsynsobjektet utgör en varningssignal att handlingen kan innehålla uppgifter som omfattas av sekretess.

Särskilda begränsningar rörande kapitel 15 i OSL

Verksamhet som är säkerhetskänslig och omfattas av säkerhetsskyddslagen (2018:585) är explicit undantagen Livsmedelsverkets tillsyn. Handlingar som berörs av kapitel 15 i OSL, det vill säga information som rör Sveriges säkerhet, ska inte lämnas till Livsmedelsverket.

Gallring

Livsmedelsverket sparar inte mer information än nödvändigt. I samband med tillsynen kan det komma att samlas in mer information än vad som ligger till grund för ett beslut, exempelvis i form av nätverkskartor, rutiner och policydokumentation. I samband med att ärendet avslutas gallras anteckningar och den information och som inte ligger till grund för Livsmedelsverkets beslut. Ingen information eller dokumentation sparas utan att ha ett syfte.

Postadress
Box 622
751 26 Uppsala

Besöksadress
Hamnesplanaden 5

Telefon
018-17 55 00

E-post
livsmedelsverket@slv.se

Organisationsnummer
202100-1850

Internet
www.livsmedelsverket.se