Livsmedelsverket

Tillsyn NIS via självskattning

Syftet med självskattning

Livsmedelsverket utför en tillsyn för pågående informationssäkerhetsarbete i relation till NIS-direktivet och lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Tillsynen sker i form av en självskattning hos berörda aktörer. Självskattningen har ett antal syften, till exempel:

- Ett referensvärde för att längre fram kunna mäta effekt och förändringar som skett
- Ett ingångsvärde till utformning av föreskrifter
- Ett ingångsvärde till en riskbaserad tillsyn
- Eventuellt behov av informationsåtgärder

Självskattningen är också en hjälp till organisationer att komma igång med sitt säkerhetsarbete genom att reflektera över både organisation och teknisk miljö.

Självskattningen kan också ge viss statistik för att Livsmedelsverket ska få en helhetsbild av säkerhetsmedvetandet i Sverige inom vattensektorn.

Redovisning av resultat

Livsmedelsverket bedömer att svaren för varje enskild VA-huvudman kan komma att omfattas av sekretessbestämmelserna i 18 kap. 8 § 3 offentlighets- och sekretesslagen (2009:400). Sammanställning i form av statistik kan förmedlas vid konferenser och dylikt om Livsmedelsverket bedömer det möjligt ur ett sekretessperspektiv.

Innehåll

Områden som ingår i självskattningen är följande:

- Beskrivning av organisation
- Utgångsläget för er organisationen
    - Förutsättningar för säkerhetsarbete
    - Tekniskt utgångsläge
- En bedömning av den egna förmågan
- Skyddsbehov
- Risker och åtgärder
- Incidenthantering

Vad som omfattas av frågorna

Frågorna är i direkt relation till NIS-direktivet och rör således de styrsystem och system som kan påverka säkerheten i dricksvattenförsörjningen. Det gäller även för riskanalyser och åtgärder.

Mer i detalj innebär det att den IT som kan påverka säkerheten i styrsystemen för vattenproduktion och distribution också omfattas om den inte separeras från styrsystemen.

Frågorna eller frågeområdena föregås av motivet till att frågan/frågorna ställs. Svar sker genom kryssrutor för det alternativ som passar men det finns också utrymme att notera viss information i fritext efter frågeområdet.

Livsmedelsverket

Tillsyn NIS via självskattning

Beskrivning av er organisation

Organisationen ska beskriva sin kapacitet och storlek som den ser ut nu. Detta är relevant i bedömningen av den totala mognadsgraden hos olika aktörer där olika storlek på organisationen förmodligen har effekt på både förutsättningar och mognadsgrad avseende informationssäkerhet.

1. Uppgifter om verksamheten

Namn hos Bolagsverket	Organisationsnummer
Postadress	Postnummer och ort
Verksamhetens namn	Verksamhetens telefonnummer (vxl)

2. Hur många årsarbetskrafter arbetar inom er vattenverksamhet år 2019?

3. Hur är er verksamhet organiserad?

☐ Förvaltningsform - verksamheten är en del av kommunen.
☐ Kommunalt bolag – enbart VA bolag
☐ Kommunalt bolag – INTE enbart VA-bolag men s.k. multi-utility bolag
☐ Annan organisationsform, beskriv:

Livsmedelsverket

Tillsyn NIS via självskattning

Utgångsläge

Förutsättningar för informationssäkerhetsarbete

Syftet med dessa frågor är att klarlägga hur många VA-huvudmän som redan bedriver ett etablerat informationssäkerhetsarbete där styrsystem för vatten antingen ingår eller inte ingår. Frågorna syftar också till att klarlägga vem som styr säkerhetsarbetet och vilket mandat VA-verksamheten har att bedriva säkerhetsarbete samt vilka beroenden som finns till andra organisationer till exempel kommunen och andra yttre faktorer.

4. Vilken organisation styr förutsättningarna för informationssäkerhetsarbete inom er verksamhet?

- ☐ Kommunledningen
- ☐ Ägaren av bolaget
- ☐ VA- verksamheten
- ☐ Annat:

5. Var bedrivs det praktiska arbetet med ökad informationssäkerhet för vattenverksamheten?

- ☐ Det drivs av vattenverksamheten
- ☐ Det drivs av tillsammans med vattenverksamheten
- ☐ Det drivs av med lite medverkan av vattenverksamheten
- ☐ Det drivs av utan medverkan av vattenverksamheten
- ☐ Det är otydligt i vår organisation
- ☐ Annat, beskriv:

6. Har VA-verksamheten beslutanderätt avseende integration av styrsystem för vattenverksamhet med övrig IT-verksamhet, dvs är det er verksamhet som beslutar över graden av integration med övriga IT-system?

- ☐ Ja
- ☐ Nej
- ☐ Till viss del, beskriv:

7. Finns ett ledningssystem för informationssäkerhet som gäller för er verksamhet?

- ☐ Ja, det är anpassat till vattenverksamheten
- ☐ Ja, det är inte specifikt anpassat till vattenverksamheten
- ☐ Delvis, ett ledningssystem är under framtagande
- ☐ Delvis, ett ledningssystem med anpassning till vattenverksamheten är under framtagande
- ☐ Nej
- ☐ Vet ej

Svaren skickas med **rekommenderat brev** till Livsmedelsverket, ”NIS-tillsyn”, Box 622, 751 26 Uppsala

Livsmedelsverket

Tillsyn NIS via självskattning

8. Vilken/vilka standarder används för informationssäkerhetsarbetet inom vattenverksamheten?
☐ Vet ej ☐ Ingen ☐ ISO/IEC 27001 ☐ ISO/IEC 27002 ☐ ISO/IEC 27005 ☐ ISO/IEC 27019 ☐ IEC 62443 Andra, lista:

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Tekniskt utgångsläge

Frågorna nedan rör hur den tekniska miljön för styrsystemen för vattenproduktion/distribution är uppbyggd och hanteras samt i viss mån vilka säkerhetsåtgärder som redan finns. Detta ger Livsmedelsverket en samlad bild av utgångsläget och är underlag för prioritering av tillsyn samt som underlag till föreskriftsarbete.

Manuell styrning

9. Kan era styrsystem helt skärmas av från nätverk och system utanför styrsystemen, utan att det får konsekvenser för er vattenproduktion inklusive distribution, s.k. ö-drift/islanding?
☐ Ja, utan tidsbegränsning ☐ Ja, men endast under en viss tidsperiod, ange i antal timmar: ☐ Nej, följande externa beroenden finns:

10. Kan er vattenproduktion och distribution skötas manuellt utan det övergripande styrsystemet, dvs driva processen utan datorstöd men med fungerande PLC:er?
☐ Ja, utan tidsbegränsning ☐ Ja, men endast under en viss tidsperiod, ange i antal timmar: ☐ Nej, följande system är nödvändiga:

11. Vilka beroenden utöver era styrsystem finns för kontinuerlig drift?
☐ IP-telefoni ☐ Mobiltelefoni ☐ Internet ☐ 3G/4G ☐ Satellitkommunikation ☐ Andra, lista:

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Dokumentation av styrsystemens IT-miljö

12. Har er verksamhet aktuell dokumentation avseende:	
Verksamhetens nätverk (nätverkskarta mm)	☐ Ja ☐ Nej ☐ Ej färdigt men prioriterat
Verksamhetens system	☐ Ja ☐ Nej ☐ Ej färdigt men prioriterat
Systemberoenden	☐ Ja ☐ Nej ☐ Ej färdigt men prioriterat
Kommunikationsvägar till och från de industriella informations- och styrsystemen	☐ Ja ☐ Nej ☐ Ej färdigt men prioriterat
Informationsflöden till och från de industriella informations- och styrsystemen	☐ Ja ☐ Nej ☐ Ej färdigt men prioriterat

Övriga kommentarer:

Separation av IT-miljöer

13. Är verksamhetens industriella styrsystem segmenterade från andra IT-system (t.ex. kontorsnätverk som epostsystem etc och övrig verksamhets IT)?
Segmentering innebär att nätverket är fristående och att nätverkstrafik begränsas till det som är nödvändigt.

☐ Ja, de är logiskt segmenterade från all övrig verksamhet
☐ Ja, de är fysiskt segmenterade från all övrig verksamhet
☐ Delvis, beskriv vilken verksamhet som de sitter ihop med:
- ☐ Annan relaterad verksamhet, exempelvis avloppshanteringen
- ☐ Administrativ verksamhet som kontors och epostsystem
- ☐ Offentlig verksamhet som skola eller bibliotek
- ☐ Annat, beskriv:

☐ Nej

14. För de komponenter som delas med annan verksamhet och kan påverka IT-säkerheten för styrsystemen, styr ni över behörigheter, uppdateringar och konfigurationer för de komponenterna?

☐ Det finns inga delade komponenter

Behörigheter	Uppdateringar	Konfigurationer
☐ Ja ☐ Ja, för flertalet ☐ Nej	☐ Ja ☐ Ja, för flertalet ☐ Nej	☐ Ja ☐ Ja, för flertalet ☐ Nej

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Fjärruppkoppling

15. Kan någon extern part godtyckligt koppla upp sig för distansarbete till IT-miljön för styrsystemen?
☐ Ja ☐ Nej, vi tillåter inte fjärruppkoppling ☐ Nej, vi har teknisk styrning på när fjärranslutning kan användas

16. Om sk fjärruppkoppling eller distansarbete sker; används då alltid två-faktors-autentisering för samtliga användare?
☐ Ja ☐ Nej

17. Om sk fjärruppkoppling eller distansarbete sker; används då alltid användarunika inloggningsuppgifter för samtliga användare?
☐ Ja ☐ Nej

Övriga kommentarer:

Behörighetskontroll

18. Hanterar verksamheten själv all behörighetstilldelning till styrsystemen?
☐ Ja ☐ Nej, den hanteras av:

19. Har vattenverksamheten kontroll över behörighetstilldelning till system som kan påverka säkerheten i styrsystemen?
☐ Ja ☐ Nej, den hanteras av:

20. Med vilken regelbundenhet kontrolleras relevansen av alla användares behörigheter och åtkomsträttigheter till styrsystemen?
☐ Oftare än årsvis ☐ Årsvis ☐ Vartannat år ☐ Mer sällan än vartannat år

Svaren skickas med **rekommenderat brev** till Livsmedelsverket, ”NIS-tillsyn”, Box 622, 751 26 Uppsala

Livsmedelsverket

Tillsyn NIS via självskattning

21. Med vilken regelbundenhet kontrolleras relevansen av alla användares behörigheter och åtkomsträttigheter system som kan påverka säkerheten i styrsystemen?
☐ Oftare än årsvis ☐ Årsvis ☐ Vartannat år ☐ Mer sällan än vartannat år

Övriga kommentarer:

Virusskydd

22. Finns antivirus installerat på datorer som kan drabbas av virusangrepp eller annan skadlig kod som kan påverka vattenproduktionen/distributionen?
☐ Ja ☐ På färre än 50% ☐ På flertalet ☐ Nej, beskriv varför

23. Har ytterligare åtgärder vidtagits för att minska spridning och effekten av oavsiktligt införd skadlig kod (t ex datavirus och ransomware)?
☐ Ja, vilka: ☐ Nej, varför:

Övriga kommentarer:

Backuper/återställning

24. Med vilken regelbundenhet testar ni att återställning av alla styrsystem och konfigurationsdata från utförd säkerhetskopiering (backup) verkligen fungerar i praktiken?
☐ Oftare än årsvis ☐ Årsvis ☐ Vartannat år ☐ Mer sällan än vartannat år ☐ Vi har aldrig testat att styrsystemen fungerar efter återställning

Övriga kommentarer:

Svaren skickas med **rekommenderat brev** till Livsmedelsverket, ”NIS-tillsyn”, Box 622, 751 26 Uppsala

Livsmedelsverket

Tillsyn NIS via självskattning

Externa leverantörer och molntjänster

25. Har ni avtal med leverantörer, som kan påverka styrsystemens säkerhet, om deras åtaganden om IT-säkerhet?
☐ Ja, med alla leverantörer ☐ Ja, med flertalet leverantörer ☐ Nej

26. Följer ni upp att leverantörerna håller den IT-säkerhet som utlovats i avtal?	
Kritiska leverantörer	Övriga leverantörer
☐ Ja, oftare än årsvis ☐ Ja, årsvis ☐ Ja, vartannat år ☐ Nej	☐ Ja, oftare än årsvis ☐ Ja, årsvis ☐ Ja, vartannat år ☐ Nej

Övriga kommentarer:

Utvärdering/tester av miljön för styrsystemen

27. Vilka säkerhetstester utförs i styrsystemen?
☐ Vi utför inga tester ☐ Sårbarhetsscanningar ☐ Penetrationstester ☐ Andra/fler, lista:

Övriga kommentarer:

Framtida uppgraderingsprojekt

28. Kommer ni att behöva uppgradera ert nuvarande styrsystem eller delar av det?
☐ Ja, pågår nu, under 2019. ☐ Ja, inom 1-3 år ☐ Ja, inom 4-5 år ☐ Ja, inom 6-9 år ☐ Om 10 år eller senare

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Den egna förmågan

Följande frågor syftar till att ni ska skatta er förmåga att arbeta för att höja säkerheten inom vattenproduktionen/distributionen samt att klarlägga kompetensen som finns inom vattenverksamheten.

29. Anser ni att ni har förmågan att höja informations- och IT-säkerheten i er styrsystemsmiljö?
☐ Ja ☐ Nej Om nej, beskriv kort vad som saknas:

30. Finns det informationssäkerhetskompetens och erfarenhet i den egna organisationen?
☐ Ja ☐ Nej Om nej, beskriv kort hur ni går tillväga för att tillse tillgång på kompetens:

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Skyddsbehov, riskanalyser och åtgärder

Innan säkerhetsåtgärder införs bör organisationen ha rett ut vilka skyddsbehov som föreligger. Med det menas hur känslig informationen/trafiken är och vad som kan hända om störningar i de aktuella styrsystemen sker eller vid röjande av känslig information. Nedan frågor klarlägger om en bedömning av känslighet har utförts, om riskanalyser har utförts samt vilka riskområden och åtgärder ni ser och prioriterar.

Informationssäkerhetsklassning

31. Har ni identifierat vilken information/vilka system/vilken nätverkskommunikation som är viktig(a) avseende driftssäkerhet?
☐ Ja ☐ Ej färdigt men prioriterat ☐ Nej

32. Har resultatet av ovan dokumenterats?
☐ Ja ☐ Ej färdigt men prioriterat ☐ Nej

Övriga kommentarer:

Riskanalyser

33. Har riskanalys genomförts avseende den information/de system/den trafik som identifierats som viktiga avseende driftssäkerhet?
☐ Ja ☐ Vi har analyserat mer än 50% av det som identifierats som viktigt ☐ Vi har analyserat mindre än 50% av det som identifierats som viktigt ☐ Nej

34. Medverkar verksamheten vid riskanalyserna för styrsystemen?
☐ Ja, tillsammans med riskanalysexpert ☐ Ja, på egen hand ☐ Nej, den utförs av: ☐ Vi har inte påbörjat något riskanalysarbete

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Risker och Åtgärder

35. Har en åtgärdsplan för att hantera risker från riskanalysen tagits fram?
☐ Ja ☐ Framtagning är pågående ☐ Nej

De tre tabellerna nedan syftar till bland annat att identifiera vilka risker/riskområden som branschen ser är prioriterade, om vissa risker inte hanteras och vad det kan bero på samt åtgärder som redan är införda eller under införande. Detta är även ingångsvärden för kommande tillsyner som sker på plats.

För att svaren ska bli jämförbara så föreslår vi att ni vid behov använder liknande uttryck/nivå på beskrivning som nedan för att beskriva era riskområden och åtgärder:

Exempel riskområden:

- Bristande separation: styrsystemen sammankopplade med till exempel kontorsnätverk
- Bristande kontroll över fjärråtkomst
- Bristande kontroll av externa parter
- Ransomware
- Diskkrasch
- Översvämning/inbrott/brand i miljön för styrsystemen

Exempel åtgärder:

- Tvåfaktors autentisering för fjärråtkomst
- Separation av styrsystemen från kontorsnätverket
- Utbildning inom informationssäkerhet
- Införande av DMZ för kommunikation

Valbara tidsspann: 3-5 mån, 6-8 mån, 1 år, 2 år, 3 år.

36. Lista upp till 10 högt prioriterade säkerhetsåtgärderna och ange inom vilket tidsspann de kommer att införas. Notera att tidsspannet inte nödvändigtvis avgör prioriteten.		
Prioritets ordning	Åtgärd	Tid
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Livsmedelsverket

Tillsyn NIS via självskattning

37. Lista upp till 5 risker med högst konsekvens, enligt er bedömning, som inte kommer att hanteras inom 3 år samt av vilken orsak.
Med detta menas till exempel risker där befintliga åtgärder inte bedöms tillräckliga eller risker som inte kommer att åtgärdas. Orsaker till att man väljer att inte införa en åtgärd kan till exempel vara resursbrist, mandatbrist, ekonomi eller något annat.

Nr	Risk	Orsak
1		
2		
3		
4		
5		

38. Lista upp till 5 säkerhetshöjande åtgärder som är under införande eller som har införts de senaste 3 åren.

Nr	Åtgärd
1	
2	
3	
4	
5	

Övriga kommentarer:

Livsmedelsverket

Tillsyn NIS via självskattning

Incidenthantering

Rapporteringspliktiga incidenter

Med rapporteringspliktiga incidenter avses de i MSB föreskrifter för vattensektorn:

”Leverantörer inom leverans och distribution av dricksvatten ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

1. har pågått i minst två timmar och som
    a) kan antas ha påverkat minst 2 000 personer,
    b) har påverkat akutsjukhus, eller
2. har påverkat styrning och övervakning av tjänsten. ”

39. Hur många incidenter som motsvarar den rapporteringspliktiga beskrivningen har inträffat de senaste:	
1 åren (2018)	
3 åren	
5 åren	

Övriga IT-relaterade incidenter

40. Hur många IT-incidenter har inträffat de senaste:	
1 åren (2018)	
3 åren	
5 åren	

Övriga kommentarer: