NIS-direktivet

# NIS – att komma igång

Säkerhet för ett av våra viktigaste livsmedel – dricksvatten – är viktigt för samhället. I och med NIS-direktivet har informations- och IT-säkerhetsfrågor för VA-huvudmän uppmärksammats och Livsmedelsverket har fått i uppdrag att arbeta med tillsyn mot lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Innan tillsyn, föreskrifter och krav fullt ut är på plats kan aktörer i dricksvattensektorn som omfattas av NIS börja arbeta med informations- och IT-säkerhetsfrågor. Denna information ger några tips och förslag för att påbörja säkerhetsarbetet.

## Säkerhet i ett NIS-sammanhang

Primärt är det driftsäkerheten och förmågan att kontinuerligt och uthålligt tillhandhålla dricksvatten som NIS avser med hög säkerhet inom tjänsten *leverans och distribution av dricksvatten*.

Denna kontinuitet säkerställs genom att införa åtgärder för att förebygga störningar samt skapa en förmåga att hantera och lära sig av de störningar som, trots åtgärder, ändå uppstår. NIS inriktar sig på störningar som har sin orsak i att nätverksuppkopplad digital utrustning inte är tillgänglig eller inte fungerar korrekt – oavsett om det skett av misstag, naturfenomen eller genom angrepp.

Konfidentialitet är också en aspekt som är relevant inte minst för sådan information som i ett senare skede kan användas för att störa vattenleveransen. Exempelvis lösenord för fjärråtkomst, detaljerade kartor och systembeskrivningar.

## På kort sikt

Nedan beskrivs några åtgärder som kan ge stor effekt på driftssäkerheten. Listan är dels baserad på de anmälningsblanketter som Livsmedelsverket inom NIS-tillsynen fått in samt dels på standarder som ISO/IEC 27001, IEC 62443, Enisas guidelines för granskningar ( WP2018 O.2.2.3 Guidelines on assessing DSP and OES compliance), erfarenheter från penetrationstestning i allmänhet samt de större virusangreppen som drabbat samhället de senaste åren.

Som aktör kan ni använda denna lista för att komma igång med säkerhetsarbetet. Dock poängteras att detta *inte* innebär att det systematiska informationssäkerhetsarbetet som föreskrivs av MSB kan förbises. Det är heller *inte* en uttömmande lista utan en hjälp att komma igång med säkerhetsarbetet.

Riskområdena nedan är beskrivna utan inbördes prioritering.

Livsmedelsverket

## Separation av nätverk

Med separation av nätverk menas att de nätverk och de komponenter som styr vattenproduktionen och liknande verksamhet, t.ex. kontrollsystem för avlopp, ska vara åtskilda från övrig verksamhet. Med övrig verksamhet menas till exempel kontorsnätverk, annan kommunal verksamhet eller verksamhet som inte rör kontrollsystemen. Den högsta graden av åtskildhet är fysisk separation av samtliga komponenter inklusive nätverksutrustning och driftsmiljö. Ur ett driftssäkerhetsperspektiv är fysisk separation oftast att föredra framför logisk separation.

***Varför är detta viktigt?***

Traditionellt sett har industriella kontrollsystem varit isolerade; en högre grad av integration mellan olika verksamheters nätverk och system medför att kontrollsystem exponeras för risker som de inte är designade för att hantera. En drivande faktor till integration kan till exempel vara att effektivare utnyttja kommunala IT-resurser. I och med integrationen av kontrollsystemen blir riskerna svåra att analysera och hantera och risken ökar således med ökad mängd integrationer. Störningar (t.ex. virus, angrepp eller IT-haverier) i den allmänna IT-infrastrukturen påverkar även kontrollsystemens funktion i en integrerad miljö.

## Fjärråtkomst över internet

Om verksamheten tillåter åtkomst till styrsystem över internet via VPN eller dylikt så bör säkerheten för denna typ av åtkomst styras. Initialt bör det kontrolleras om det alls är relevant och om åtkomsten kan begränsas i exempelvis tid och antal. För fjärråtkomst är också säkerhet kring inloggning viktigt, två-faktors autentisering av något slag är grundläggande som säkerhetshöjande åtgärd för fjärrstyrning av industriella kontrollsystem.

***Varför är detta viktigt?***

Lösenord är på många sätt svaga då de ofta återanvänds på flera ställen – privata webtjänster, konton på jobbet mm  - och blir då lättare att stjäla. De är dessutom relativt enkla att genom upprepade försök knäcka. En fjärruppkoppling erbjuder inte heller samma möjlighet att kontrollera att den som loggar in faktiskt är den person eller maskin den utger sig för att vara – på en fysisk arbetsplats finns det ett skalskydd och kollegor som delvis fungerar som en kontrollmekanism vilket helt saknas vid fjärruppkoppling.

## Reglera åtkomst och rättigheter

Åtkomst till digitala system styrs i de flesta fall av användarnamn och lösenord. En stark styrning av åtkomsträttigheter, användarkonton och lösenordshantering säkerställer att det endast är behörig personal som har åtkomst till de digitala system som används för *leverans och distribution av dricksvatten.* Det innebär att även leverantörers eventuella åtkomst ska kontrolleras på samma sätt som anställdas åtkomst.

***Varför är detta viktigt?***

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 annars lätt att gamla behörigheter ligger kvar. Det är särskilt viktigt om åtkomst kan ske över internet.

## Inventering och hantering av utrustning och sårbarheter

Inventering av såväl anläggningens uppkopplade komponenter samt tekniska säkerhetsgranskningar av komponenternas sårbarheter kan ge en bättre inblick i den faktiska säkerhetsnivån. Tekniska säkerhetsgranskningar kan utföras genom till exempel sårbarhetsscanningar alternativt penetrationstester. Det är dock viktigt att känna till skillnaderna mellan vanlig IT-miljö och industriella kontrollsystem vid användandet av verktyg som till exempel scanningar. Om de industriella kontrollsystemen havererar på grund av oväntad nätverkstrafik kan konsekvenserna bli mycket stora. Tekniska säkerhetsgranskningar ska utföras med måtta och försiktighet i driftsmiljö, i synnerhet när det gäller kontrollsystem.

***Varför är detta viktigt?***

Med en uppdaterad överblick över vilken nätverksuppkopplad utrustning ett system innehåller och hur den tekniska nivån är avseende sårbarheter kan sådana svagheter hanteras - antingen genom uppdateringar eller andra kompenserande åtgärder. Vissa industriella kontrollsystem har inte möjlighet att uppdateras av olika skäl och då bör andra åtgärder vidtas, till exempel separation eller härdning. I praktiken är det dyrt och svårt att få en god riskbild för att kunna hantera tekniska sårbarheter om inte en sårbarhetsinventering utförs.

## Rapportering och hantering av IT-incidenter

Genom att bygga en fungerande verksamhet för de vardagliga incidenterna så blir också organisationen bättre rustad för att hantera allvarliga incidenter och attacker av olika slag. Incidentrapportering är kravställt i MSB föreskrifter och detta kommer att börja gälla 1 mars 2019.

## Att komma igång med systematiken

För att kunna genomföra säkerhetsarbetet systematiskt krävs resurser, ekonomiskt, personalmässigt och kompetensmässigt. Genom att samtidigt som ovanstående punkter bearbetas även införa regelbunden kontroll av identifierade åtgärder - som till exempel återkommande revision av konton och fjärråtkomst - så kan systematiken stegvis införas.

I förlängningen kan och ska detta byggas ut till ett komplett program med återkommande regelbundna aktiviteter, kontinuerlig uppföljning samt tydliga roller och ansvar baserat på vilka risker som identifieras under regelbundna riskanalyser.

## Informativa länkar

Lag 2018:1174: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174

Livsmedelsverket: www.livsmedelsverket.se/nis

MSB: https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/

Systematiskt arbete: www.informationssäkerhet.se

Har ni frågor? Kontakta oss på: **nistillsyn@slv.se**

Livsmedelsverket