Åtgärder för att förebygga skadeverkningar

Här ger Livsmedelsverket vägledning om hur kraven i lagstiftningen kan uppnås. Vägledningen är inte bindande och utesluter inte andra sätt att uppfylla kraven.

På den här sidan hittar du information om förebyggande åtgärder mot skadeverkningar på dricksvattenanläggningar enligt 4-6 §§ LIVSFS 2008:13.

Skydd efter behov

Dricksvattenförsörjning är en komplicerad verksamhet med många olika typer av anläggningar, installationer och anordningar från råvattenintag, via beredning och distributionsanläggning till kranen hos användaren. Driften av både vattenverket och dricksvattendistributionen sker oftast via dator. Många vattenverk fjärrstyrs dessutom från en driftcentral.

En uppgradering av skyddet av dricksvattenförsörjningen medför ökade kostnader. Därför är det viktigt att säkerhetsarbetet utförs systematiskt och att det finns en långsiktig plan för arbetet. Det är inte möjligt att uppnå ett hundraprocentigt skydd mot sabotage och skadegörelse, men målet måste vara att minska riskerna för sådana händelser så långt det är praktiskt möjligt och ekonomiskt försvarbart. Det är av största vikt att alltid fundera över syftet med de åtgärder som vidtas för att komma fram till de mest kostnadseffektiva lösningarna.

Livsmedelsföretagaren ska vidta de åtgärder som behövs för att förebygga skadeverkningar. Det anges i 4 - 6 §§ LIVSFS 2008:13. Formuleringen ger utrymme för tolkningar och en flexibilitet att anpassa säkerhetsnivån till de faktiska behov varje anläggning har. För att komma fram till vilka åtgärder som behöver vidtas är det nödvändigt att göra en systematisk genomgång av den nuvarande säkerhetsnivån, analysera vilka risker och eventuella hotbilder som kan finnas för olika delar av dricksvattenanläggningen, hitta de sårbarheter som kan finnas i systemet och ta fram en tidsplan för genomförande av åtgärder.

Begreppen obehörig/behörig och tillträde/åtkomst är centrala i LIVSFS 2008:13. Det gäller att definiera vilka som är behöriga att ha tillträde till olika delar av anläggningarna och åtkomst till olika sorters information och dokumentation. Därför är det också av avgörande betydelse att det finns rutiner för hur behörigheter delas ut, både internt och externt. Det kan till exempel vara rutiner för nyckel/kort/tag-hantering, rutiner för inloggning i datasystem, rutiner för tillträde till lokaler för externa besökare, entreprenörer och konsulter, rutiner för dokumenthantering och rutiner för att lämna ut handlingar.

Handböcker, rekommendationer, standarder och rapporter är exempel på hjälpmedel som behandlar säkerhetsarbete i allmänhet men även specifikt för dricksvattenförsörjning och hur informations- och IT-säkerhet hanteras.

Mer information

Fysiskt skydd

För att uppnå en bra säkerhet måste det först bestämmas vad som ska skyddas för att sedan kunna bestämma hur skyddet ska vara uppbyggt.

För att ta reda på vad som ska skyddas bör en inventering av alla typer av anläggningar, installationer och anordningar, som ingår i dricksvattenanläggningen göras. För att få underlag till beslut om på vilken nivå säkerhetsskyddet bör ligga, finns olika hjälpmedel, till exempel risk- och sårbarhetsanalys, kontinuitetsplanering och incidentrapportering.

Inventering

Exempel på anläggningar och anordningar som kan omfattas av inventeringen:

- Råvattenintag
- Grundvattenbrunnar
- Intagsledning/-ar
- Pumpar/pumpstationer

- Vattenverk
- De utrymmen (omslutningsytor) i vattenverket som särskilt måste skyddas, till exempel filtersalar med öppna vattenytor, kontaktbassänger eller reservoarer, kontrollrum med datorer med mera.
- Distributionsanläggning
- Pump-/tryckstegringsstationer
- Brand-/spolposter
- Hög-/lågreservoarer
- Mätar-/nedstigningsbrunnar

Risk- och sårbarhetsanalys

För att avgöra vilket skydd som är lämpligt för de olika objekten i dricksvattenanläggningen kan någon form av risk- och sårbarhetsanalys när det gäller säkerheten göras.

Analysen bör innehålla en uppskattning av sannolikheten för en oönskad händelse och vilka konsekvenser en sådan inträffad händelse kan få. Incidentrapportering, erfarenheter från branschen i övrigt och kontakter med kommunens säkerhetssamordnare och den lokala polismyndigheten kan vara till hjälp för att bedöma sannolikheten för olika händelser.

I många fall kan det dock vara svårt att bedöma sannolikheten för att en antagonistisk händelse kan inträffa. Då kan det vara lämpligare att fokusera på vilka konsekvenser olika händelser kan få för att komma fram till en bedömning av vilken säkerhetsnivå som behövs.

Man bör också tänka på att en händelse kan få olika konsekvenser för användarna/konsumenterna beroende på var i kedjan från täkt till kran den inträffar. Det är även mycket viktigt att ta hänsyn till var i processen dricksvattnet är mest sårbart, det vill säga där det finns öppen vattenyta och där vattnet inte står under tryck. Det sammanfaller oftast med den hygienzon där man har det mest omfattande hygienskyddet. Andra sårbarheter man bör ta hänsyn till är driftkritiska delar av anläggningen och stöldbegärlighet.

Exempel på oönskade händelser som kan tas upp i en risk- och sårbarhetsanalys är inbrott i reservoarer eller vattenverk, kemisk eller mikrobiologisk förorening av råvattnet, sabotage av IT-systemet, hot om förorening av dricksvatten som levereras till högriskabonnent (vissa myndighetsfunktioner, viss livsmedelsindustri med mera) och anlagd brand i vattenverket. Risk- och sårbarhetsanalysen är en hjälp i arbetet med att definiera vilka objekt eller objekttyper som behöver till exempel områdesskydd, kameraövervakning, utomhusbelysning, inbrottslarm och vilken typ av larm, vilken typ av låssystem m.m. Riskanalysen kan också ligga till grund för utarbetandet av åtgärder för att upptäcka och avhjälpa skadeverkningar.

Åtgärder för att upptäcka och avhjälpa skadeverkningar

Riskanalysen bör dokumenteras och revideras vid behov. En anledning att revidera riskanalysen kan t.ex. vara förändrad bebyggelse eller ökad rapportering av skadegörelse i ett område. Det finns många rekommendationer för hur risk- och sårbarhetsanalyser kan utföras, se till exempel Livsmedelsverkets handbok Risk- och sårbarhetsanalys. Myndigheten för samhällsskydd och beredskap, MSB, och säkerhetspolisen har också information om hur risk- och sårbarhetsanalyser kan utföras.

Kontinuitetsplanering

Kontinuitetsplanering (eller avbrottsplanering) kan vara ytterligare ett verktyg för att ta reda på vilka sårbarheter som finns i dricksvattenförsörjningen och hur prioritering av säkerhetsåtgärder kan göras. Kontinuitetsplanering fokuserar på tidskritiska funktioner/resurser för verksamheten. Vad som orsakar bortfallet av en resurs/funktion spelar i kontinuitetsplaneringen ingen roll.

Två viktiga frågor att ställa i arbete med kontinuitetsplanering är:

- Vad händer om en viktig funktion faller bort?
- Hur lång tid tar det innan vi kommer tillbaka till normal verksamhet efter att funktionen fallit bort? Kritiska resurser/funktioner i dricksvattenförsörjning kan t ex vara elförsörjning inklusive bränsletillgång, processkemikalier, personal/kompetens och kommunikationsmöjligheter. Mer information om kontinuitetsplanering finns på Myndighetens för samhällsskydd och beredskap (MSB) webbplats.

Val av skydd

Risk- och sårbarhetsanalys och eventuell kontinuitetsplanering är verktyg för att komma fram till en bedömning av vilken skyddsnivå olika delar av dricksvattenanläggningen bör ha. Mer information om skyddsklassificering och skyddsnivåer finns i Säkerhetshandbok för dricksvattenproducenter. Svenska stöldskyddsföreningen (SSF) har också riktlinjer för skydd samt detaljerad information om vilka tekniska krav man kan ställa på sina installationer t ex i SSF 200 Regler för mekaniskt inbrottsskydd.

Administrativt skydd

Nedan följer information om tillträdesrutiner och utbildning för personal som vistas i dricksvattenanläggningar.

Tillträdesrutiner

Om det mekaniska/fysiska skyddet ska fungera måste det också finns rutiner för vilka som har tillträde till de olika lokalerna eller anläggningarna. Rutiner måste också finnas för tillträde för andra än den ordinarie personalen, t.ex. entreprenörer inklusive städfirmor, externa besökare och studiebesök. Inhyrd eller extern personal som arbetar i lokalerna under längre tid eller vid upprepade tillfällen bör få muntlig och skriftlig information om vilka säkerhetsrutiner som gäller vid vistelse i lokalerna. När det gäller tillträde för teleoperatörer som har antenner på vattentorn rekommenderas att Svenskt Vattens riktlinjer följs. Dessa riktlinjer kan med fördel användas i alla sammanhang där annan än den ordinarie personalen behöver ha tillträde till dricksvattenanläggningen.

Dokumenterade rutiner för nyckel- och passerkortshantering bör finnas. Även hanteringen av nycklar till eventuella hänglås bör omfattas.

Utbildning och övningar

Det är den personal som dagligen arbetar med dricksvattenproduktionen och dricksvattendistributionen som är den viktigaste faktorn för att upprätthålla en hög säkerhetsnivå. Det är därför av största vikt att personalen är utbildad och informerad om de säkerhetsrutiner som finns och att de förstår varför rutinerna ska följas. Man bör genomföra regelbundna övningar av olika scenarier för att i en krissituation kunna fatta rätt beslut under tidspress.

Vattenverk

Vattenverk kan skilja sig åt mycket i storlek och konstruktion: från små grundvattenverk som besöks en eller några gånger i veckan och där vattnet i stort sett bara pumpas upp och levereras direkt till användare/konsument, till stora ytvattenverk som har dygnet-runt-bemanning med avancerad beredning, stora långsamfilter och öppna vattenytor. Säkerhetssystemen kommer därför av naturliga skäl att skilja sig åt.

Exempel på svaga punkter i alla byggnader är: dörrar, fönster, låsanordningar, ventilationstrummor, luftintag och manluckor till reservoarer. Stora vattenverk kan delas upp i olika omslutningsytor med förstärkt skydd, t.ex. rum med öppna vattenytor och kontrollrum med datorer. Även lågreservoarer i eller i anslutning till vattenverket som används för utjämning eller för att få tillräcklig kontakttid för klordesinfektionen bör ha förstärkt skydd. Ju senare i beredningen, desto större risk att förorenat dricksvatten kan nå användarna/konsumenterna.

Om det bedöms som nödvändigt att ha områdesskydd runt ett vattenverk kan det bestå av staket och grindar, eventuellt med någon form av passagekontroll. Staketet kan vara larmat och det kan finnas övervakningskameror på området. Belysning av vattenverksområdet kan verka avskräckande mot intrång.

Distributionsanläggning

Reservoarer, pumpstationer och liknande i distributionsanläggningen bör ur säkerhetssynpunkt behandlas på samma sätt som vattenverk för att förhindra tillträde för obehöriga. I reservoarer bör utrymmet med öppen vattenyta ha förstärkt skydd. Ventilationsrör och manluckor i hög- och lågreservoarer bör särskilt uppmärksammas.

Anordningar i distributionsanläggningen som kan utnyttjas för att suga eller trycka in förorenat vatten eller andra vätskor i distributionsanläggningen bör skyddas mot obehörig åtkomst. Olovligt uttag av dricksvatten ur brandposter orsakar ofta stora kvalitetsproblem och kan också innebära hälsomässig risk för användare/konsumenter. Detta kan betraktas som stöld och skadegörelse och det kan ibland innebära avsevärda kostnader för verksamhetsutövaren för att komma tillrätta med problemen.

Det är viktigt att identifiera de delar av distributionsanläggningen som är aktuella i detta sammanhang och tydligt definiera vem som ansvarar för dessa. På samma sätt som i resonemanget ovan om behörig/obehörig måste det tydliggöras vem som har behörig åtkomst till t ex brandposter. Rutiner för detta kan behöva tas fram. För att minska obehörigt nyttjande av dricksvatten från brandposter kan anvisade tappställen ordnas. Dessa bör förses med lämpligt återströmningsskydd. Om det bedöms som nödvändigt kan brandposter/spolposter förses med lämpliga låsanordningar. Det kan till exempel vara nödvändigt att låsa de brandposter där man har haft upprepade problem med obehörigt nyttjande eller brandposter i särskilt känsliga lägen. I den mån objekt som t.ex. brand- och spolposter inte längre används bör dessa tas bort. Även lock till mätarbrunnar och liknande kan behöva skyddsanordningar för att förhindra obehörig åtkomst.

Informations- och IT-säkerhet

Exempel på information som är känslig ur säkerhetssynpunkt är kartor och ritningar över råvattentäkter, vattenverk och distributionsanläggningar, men även teknisk driftinformation. För att hantera all information på ett säkert sätt är det angeläget att verksamhetsutövaren har en policy och rutiner för hur informationen hanteras, oavsett om den lagras digitalt eller i pappersform. Det är även här viktigt att beakta behörighetsfrågorna och ha rutiner för vilka som har tillgång till olika typer av information också inom organisationen.

En lämplig basnivå för informationssäkerhet kan vara att följa BITS (Basnivå för informationssäkerhet) som är MSB:s rekommendationer för de administrativa säkerhetsåtgärder som minst bör vidtas för att uppnå en acceptabel säkerhetsnivå för informationshantering i en organisation. BITS behandlar bl.a. säkerhetspolicy, organisation av informationssäkerhet, personalresurser och säkerhet, fysisk och miljörelaterad säkerhet, styrning av kommunikation och drift, styrning av åtkomst, anskaffning, utveckling och underhåll av informationssystem, hantering av informationssäkerhetsincidenter, kontinuitetsplanering och efterlevnad.

MSB har också ett verktyg för informationssäkerhetsanalys, BITS Plus, som kan användas för att avgöra på vilken nivå kraven på sekretess bör läggas och som dessutom ger förslag på säkerhetsåtgärder.

Både BITS och BITS Plus följer den tidigare standarden SS-ISO/IEC 17799, numera ISO/IEC 27001 ”Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet” och ISO/IEC 27002 ”Informationsteknik – Säkerhetstekniker – Riktlinjer för styrning av informationssäkerhet.”

IT-system i dricksvattenförsörjningen

Begreppet SCADA-system används här för vattenverkens styr- och reglersystem. SCADA står för Supervisory Control and Data Aquisition och är ett övergripande begrepp för processnära system.

Inom dricksvattenproduktionen används datorer för datainsamling, övervakning och styrning av olika driftsystem. Dessa tidigare rena styr- och reglersystem har blivit allt mer komplicerade, fått mer avancerade applikationer och integreras allt oftare i organisationens allmänna IT-system. Detta gör att SCADA-systemen blir allt mer sårbara för skadlig kod som kan komma via Internet, e-post och andra öppna kommunikationssystem. Drivkraften i utvecklingen av SCADA-systemen har främst varit funktion och inte IT-säkerhet.

En säkerhetsåtgärd är att, om möjligt, överhuvudtaget inte integrera SCADA-systemet i organisationens kontorsnätverk, utan ha ett separat processystem. Samma säkerhetsrutiner bör finnas för ett SCADA-system som för kontorsnätverket, t.ex. att rekommendationerna i BITS följs. Om SCADA-systemet är integrerat i det allmänna nätverket bör en kartläggning av SCADA-systemets uppbyggnad och kopplingar till det allmänna nätverket göras för att identifiera och minska riskerna.

Det är viktigt med tydliga regler för inloggning och för användarnas behörighet att utföra vissa operationer, t.ex. ändring av doseringar, larmvärden m.m. Det bör också finnas spårbarhet i systemet för att i efterhand kunna utvärdera ett händelseförlopp. System för fjärrstyrning och fjärrövervakning bör vara skyddade mot obehörig åtkomst.

Kommunens centrala IT-organisation kan eventuellt medverka vid uppbyggnaden av säkerheten även i SCADA-systemet.

Sekretess och offentlighet

Regler om sekretess

Regler om sekretess återfinns i offentlighets- och sekretesslagen (2009:400), OSL. För dricksvattenområdet finns en rad olika bestämmelser som kan bli aktuella, till exempel:

- Sekretess med hänsyn till rikets säkerhet (s.k. försvarssekretess; gäller för uppgifter som rör totalförsvaret; 15 kap 2 § OSL).
- Sekretess med hänsyn främst till intresset att förebygga eller beivra brott (gäller uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd med avseende på t.ex. byggnader, ritningar som innehåller uppgift om säkerhetsåtgärder; 18 kap 8 § OSL.).
- Sekretess med hänsyn till uppgifter i myndigheters risk- och sårbarhetsanalyser (gäller planering och förberedelser för att hantera fredstida krissituationer; 18 kap 13 § OSL).
- Sekretess med hänsyn främst till skyddet för enskilds ekonomiska förhållanden (planeringsfrågor samt frågor som rör enskilds affärs- eller driftsförhållanden, t.ex. förvärv, verksamhetsriktlinjer, prissättningskalkyler m.m.; 30 kap OSL).

Många av de uppgifter som förekommer vid planering och uppbyggnad av säkerheten på ett vattenverk eller i en distributionsanläggning kan omfattas av sekretessbestämmelserna i 18 kap OSL. Sådana uppgifter kan t.ex. vara en ritning över en byggnad, där placering av larm och övriga säkerhetsåtgärder framgår eller uppgifter om de säkerhetsrutiner som gäller i verksamheten. Viktigt att tänka på är att ritningar och andra uppgifter i någon mån måste innehålla uppgifter om säkerhetsåtgärder för att anses omfattas av OSL.

Med anledning av risk för spridning av känslig information är det lämpligt att kontrollmyndigheten överväger vilka handlingar som ska begäras in. Det kan i många fall vara tillräckligt att granska sådana handlingar på plats.

Skyddsobjekt

Mycket stora eller särskilt känsliga dricksvattenanläggningar kan förklaras som skyddsobjekt. Det är länsstyrelsen som efter ansökan från verksamhetsutövaren beslutar om att förklara en anläggning som skyddsobjekt. Att förklaras som skyddsobjekt bör kunna leda till bättre skydd av anläggningen. Exempelvis innebär ett beslut om skyddsobjekt att obehöriga inte har tillträde, att skyddsvakt får anlitas (skyddsvakt har utökade befogenheter i jämförelse med vanlig vakt) och att reglerna för kameraövervakning är enklare.

Senast uppdaterad 5 september 2019 Ansvarig grupp LK_Team Livsmedelshygien